



**Australian Government**  
**Department of Home Affairs**



# **Reform of Australia's electronic surveillance framework**

**Discussion Paper**

© Commonwealth of Australia 2021

With the exception of the Commonwealth Coat of Arms, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International license at <https://creativecommons.org/licenses/by/4.0/legalcode>.



This means this license only applies to material as set out in this document.

The details of the relevant license conditions are available on the Creative Commons website at <https://creativecommons.org/> as is the full legal code for the CC BY 4.0 license at <https://creativecommons.org/licenses/by/4.0/legalcode>.

#### **Use of the Coat of Arms**

The terms under which the Coat of Arms can be used are detailed at the Department of the Prime Minister and Cabinet website—[www.pmc.gov.au/government/commonwealth-coat-arms](http://www.pmc.gov.au/government/commonwealth-coat-arms).

# CONTENTS

---

<b>Overview .....</b>	<b>1</b>
Australia’s legislation struggles to keep pace .....	3
Guiding principles for reform .....	6
Views of the public are essential .....	7
Before you comment .....	8
A guide to this discussion paper .....	9
<b>Part 1: Who can access information under the new framework? .....</b>	<b>11</b>
The new framework will continue to protect information and data .....	12
Access to information will be strictly controlled .....	16
<b>Part 2: What information can be accessed? .....</b>	<b>19</b>
Communications: What does this mean in 2021 and beyond?.....	21
Information about a communication is different to its content .....	23
Is there a real difference between ‘live’ and ‘stored’ communications anymore? .....	26
Australians no longer communicate exclusively using services provided by Australian carriers and carriage service providers.....	27
Regulation of surveillance devices focuses on types of device, not kinds of information.....	30
<b>Part 3: How can information be accessed? .....</b>	<b>32</b>
Is a warrant framework that emphasises impact on privacy over method of access the way forward? .....	33
<b>Part 4: When will information be accessed? .....</b>	<b>37</b>
Access will only be permitted in order to investigate or disrupt crimes and threats to national security .....	38
Access to private communications, content data and surveillance information .....	38
Access to information about communications .....	42
Access to information about a person’s location or movements .....	44
Warrants should be directed at a specific target or person in the first instance .....	46
What about third parties?.....	47
What about groups? .....	49

Powers should only be authorised where necessary and proportionate .....	51
Who should authorise the use of these powers? .....	53
Information must be appropriately protected and only shared with the appropriate authorities .....	55
Warrant requirements should only be relaxed in time-sensitive situations .....	57
<b>Part 5: Safeguards and oversight .....</b>	<b>61</b>
The use of intrusive powers will be strictly limited.....	62
Ensuring powers are exercised in line with the law .....	63
Reporting and record-keeping requirements .....	66
<b>Part 6: Working together: Industry and Government .....</b>	<b>69</b>
<b>Part 7: Interaction with existing and recent legislation and reviews .....</b>	<b>73</b>
<b>Part 8: Getting involved.....</b>	<b>77</b>
How to make a submission .....	78
<b>Part 9: Attachments .....</b>	<b>80</b>
Attachment A: Key electronic surveillance provisions.....	81
Attachment B: Comparison of Five Eyes electronic surveillance powers .....	90
Attachment C: List of questions.....	111
Attachment D: Agency powers under the current electronic surveillance framework..	115

# OVERVIEW

---



The internet and digital communications have forever changed the way we live, work and do business. Such technological advances have undoubtedly improved many aspects of our lives. However, they have also been embraced by criminals, terrorists and other nefarious actors. Our laws have struggled to keep pace, creating significant challenges for agencies that have a legitimate need to exercise electronic surveillance powers.

Law enforcement agencies, including integrity and anti-corruption bodies, and the Australian Security Intelligence Organisation (ASIO) at times require access to specific information and data<sup>1</sup> to protect the community from serious crimes and threats to Australia's national security. Without access to this information, law enforcement agencies could not prevent and prosecute the most serious criminal activities, such as child sexual abuse, organised crime and cybercrime. For ASIO, access to this information and data is critical to protect Australia from serious national security threats, such as terrorism or foreign interference with our democratic institutions.

The protection of, and access to, this information and data is governed by a range of legislation, including:

- the *Telecommunications (Interception and Access) Act 1979* (TIA Act)
- the *Surveillance Devices Act 2004* (SD Act)
- parts of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act)
- parts of the *Telecommunications Act 1997* (Telecommunications Act)
- discrete parts of other Commonwealth and state and territory laws.

These Acts protect several different kinds of information and data from unauthorised access, and only allow government agencies to lawfully access information and data in limited circumstances. The Acts also require companies that own telecommunications infrastructure and provide telecommunications services, to protect this information and to assist government agencies to gain access to it in certain circumstances. Information in relation to these obligations and powers is at **Attachment A**.

---

1 This paper uses the phrase '*access to information and data*' to refer to the use of electronic or technologically-assisted means to covertly listen to or read a person's conversations or messages, access a person's electronic information or observe a person's activities and movements – collectively, electronic surveillance powers. This includes activities such as intercepting phone calls, remotely accessing a person's computers or using a listening or tracking device. The terms '*information and data*' are used to refer to any kinds of information that could be obtained through these methods. There are various methods of accessing information (including electronic information and data) that do not involve electronic surveillance. For example, agencies may be able to access a computer on premises when executing a search warrant. Powers of that kind are not within the scope of this paper.

The current legislative framework was examined extensively by Mr Dennis Richardson AC in the *Comprehensive Review of the Legal Framework of the National Intelligence Community* (the Comprehensive Review).<sup>2</sup> The Comprehensive Review identified that the current laws are complex, inconsistent, outdated and inflexible. This puts at risk the effectiveness of protections for people’s information and data, and the proper governance of agencies who access this information. It also creates difficulties for agencies when investigating serious criminality and threats to national security. To address these risks, the Government intends to develop a new modernised and streamlined electronic surveillance legislative framework by 2023.

The reform project aims to repeal the TIA Act, SD Act and relevant parts of the ASIO Act, and replace the current patchwork of laws with a single, streamlined and technology-neutral Act.<sup>3</sup> Developing the new framework will be the most significant reform to Australia’s national security laws in more than four decades. The new framework will be developed in line with the principles and values that underscore our liberal democratic society. Therefore, it is critical the policy underpinning the new framework is informed by the views of affected stakeholders and the Australian public. Over the next 2 years, the Government will work closely with a range of stakeholders, including the communications industry and the public, to ensure that the new framework is clear, consistent and well adapted to the modern world and dynamic threat environment.

## Australia’s legislation struggles to keep pace

Australia’s legislation has struggled to keep pace with the rapid evolution of communications technology. Parts of the existing legislative framework reflect technological assumptions and definitions dating back to the 1960s. When the framework was designed, the Government owned telecommunications in Australia. Since then, the technological environment has evolved to the global telecommunications market we see today. The legislation was originally designed to protect the privacy of fixed line phone calls and telegrams. Over time, a patchwork of amendments has been necessary to uphold the same principles and address technological advances – including the use of computers, emails, texts, ‘over-the-top’ messaging applications and social media.

---

2 Mr Dennis Richardson AC, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (the Comprehensive Review), 2020.

3 This will also involve consideration of potential consequential amendments to support the new framework.






 <b>1979</b>	 <b>1990s</b>	 <b>2000s</b>	 <b>2010s</b>	 <b>2020s</b>
<ul style="list-style-type: none"> <li>• Telecommunications infrastructure owned by Government.</li> <li>• Legislation required to ensure protection of privacy of communications, such as phone calls and telegrams, and agencies could access evidence and intelligence to fulfil their functions.</li> </ul>	<ul style="list-style-type: none"> <li>• Deregulation and privatisation of Australia's telecommunications industry disrupts the interception framework.</li> <li>• The emergence of personal computers moves criminals into the digital age, for example use of the internet to facilitate criminal activity, and relevant evidence and intelligence stored as computer data.</li> </ul>	<ul style="list-style-type: none"> <li>• Widespread adoption of the internet, mobile phones, SMS, emails, and personal computing.</li> <li>• Portable technology enables greater anonymisation, and changes the way criminals communicate and store information, including use of burner phones.</li> </ul>	<ul style="list-style-type: none"> <li>• Rapid uptake of internet-based communications, including social media and over-the-top messaging services.</li> <li>• Ubiquitous end-to-end encryption limits intelligence and evidence agencies are able to collect.</li> </ul>	<ul style="list-style-type: none"> <li>• Continued diversification and globalisation of the communications ecosystem.</li> <li>• Dark web usage increases, hosting anonymous platforms for illegal activities, including the sharing of child sexual abuse images, and illicit drugs, firearms and malware markets.</li> </ul>
<ul style="list-style-type: none"> <li>• Current framework established with the <i>Telecommunications (Interception and Access Act) 1979</i> (TIA Act).</li> <li>• <i>Australian Security Intelligence Organisation Act 1979</i> (ASIO Act).</li> </ul>	<ul style="list-style-type: none"> <li>• <i>Telecommunications Act 1997</i> established new industry obligations and assistance measures.</li> <li>• ASIO given authority to remotely search computers through Computer Access Warrants.</li> </ul>	<ul style="list-style-type: none"> <li>• Tempo of reforms increase.</li> <li>• New warrants including named person and service based warrants respond to the plethora of devices being used by criminals to conceal their communications.</li> <li>• Development of a stored communications framework enables better access to SMS, emails and voice messages.</li> <li>• <i>Surveillance Devices Act 2004</i> (SD Act) enacted, regulating access to tracking and surveillance devices for agencies.</li> </ul>	<ul style="list-style-type: none"> <li>• Increasingly substantial and frequent amendments required to keep pace.</li> <li>• Mandatory data retention and industry assistance measures introduced to ensure companies that provide communication services and devices in Australia are able to assist agencies to obtain critical evidence and intelligence.</li> <li>• Computer Access Warrants expanded to law enforcement.</li> </ul>	<ul style="list-style-type: none"> <li>• New powers for the AFP and ACIC to combat dark web and anonymising technologies adds to the over 1,000 pages of existing electronic surveillance legislation and over 35 different types of warrants and authorisations.</li> <li>• Comprehensive Review recommends TIA Act, SD Act and parts of the ASIO Act are repealed and replaced with one single Act that is clearer, more coherent and better adapted to the modern world.</li> </ul>

Figure 1: The current electronic surveillance legislative framework is over 1,000 pages and has been subjected to hundreds of amendments over the past four decades. Despite these changes, much of its foundation is still based on outdated technology assumptions. The new Act to be created by these reforms will set a new foundation for the modern era.



To keep pace with technology and the criminals who seek to exploit it, the Government has amended the TIA Act more than 100 times, with most amendments occurring in the past 15 years. As a result, the powers currently in the TIA Act, SD Act and parts of the ASIO Act and Telecommunications Act span more than 1,000 pages of legislation and contain more than 35 different warrants and authorisations.

Equivalent powers with similar levels of privacy intrusion have inconsistent thresholds for their use. The powers are also increasingly challenged by the ever-evolving sophistication of modern crime and threats to national security. The gradual amendments to powers and associated privacy protections have created confusion and legal uncertainty, reducing the transparency of the framework. This is unsustainable.

The push to reform the electronic surveillance framework is not new. Since 2013, several parliamentary and independent reviews have recommended the legislation be rewritten to reflect contemporary society.<sup>4</sup>

The catalyst for this reform is the Comprehensive Review. Published on 4 December 2020, the Comprehensive Review found the existing patchwork of legislation is no longer fit for purpose. It recommended the creation of a new single framework to govern electronic surveillance powers.<sup>5</sup>

Submissions to the Comprehensive Review almost universally agreed wholesale reform is required.<sup>6</sup> The Comprehensive Review also noted that other like-minded countries, including the United Kingdom<sup>7</sup> and New Zealand,<sup>8</sup> have significantly shorter and simpler electronic surveillance frameworks. Information about the corresponding legislative frameworks of other Five Eyes countries is at **Attachment B**.

The Government response to the Comprehensive Review agreed in full, in part or in principle to 186 of the 190 unclassified recommendations, including the recommendations guiding the development of a new framework.<sup>9</sup>

---

4 Inquiries recommending amendment of the electronic surveillance framework include the following Parliamentary Joint Committee on Intelligence and Security (PJCS) reports: *Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press*; *Review of the mandatory data retention regime; Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*; *Advisory report on Telecommunications Legislation Amendment (International Production Orders) Bill 2020*; *Advisory report on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*; and *Report of the inquiry into potential reforms of Australia's national security legislation*.

5 The Comprehensive Review, Volume 2, recommendation 75.

6 The Comprehensive Review, Volume 2, page 244.

7 *Investigatory Powers Act 2016* (UK).

8 *Search and Surveillance Act 2012* (NZ).

9 Commonwealth of Australia, *Government response to the Comprehensive Review of the Legal Framework of the National Intelligence Community*, 2020.

## Guiding principles for reform

The objective of this reform is to develop a new single Act that:

- better protects individuals' information and data, including by reflecting what it means to communicate in the 21st century
- ensures that law enforcement agencies and ASIO have the powers they need to investigate serious crimes and threats to security
- is clear, transparent and usable for operational agencies and oversight bodies, as well as industry who need to comply with the obligations of the framework
- is modernised, streamlined and as technology-neutral as possible, by updating key concepts and clearly identifying the agencies that can seek access to this information
- contains appropriate thresholds and robust, effective and consistent controls, limits, safeguards and oversight of the use of these intrusive powers.

In developing the new framework, these objectives will be balanced against one another. The safeguards in the framework must reflect the importance of accountability, transparency, the rule of law, privacy and other applicable rights. These must be balanced against the need for law enforcement agencies and ASIO to have effective powers to investigate and disrupt serious threats. Equally, establishing more technology-neutral definitions, concepts and warrants will not come at the cost of clarity and legal certainty.

The framework will have some impact on industry. The need to protect the integrity and security of communications and networks will be front of mind. Industry assistance will continue to be required – for example, in intercepting communications and accessing telecommunications data. However, it is intended that streamlining the existing framework will ultimately lead to a reduced regulatory burden.

As previously mentioned, the reforms will also implement the Government's response to the recommendations of the Comprehensive Review and related parliamentary and independent reviews discussed in this paper. These include a number of Parliamentary Joint Committee on Intelligence and Security (PJCIS) reviews into existing and proposed legislation.

The new Act will set out clear principles for, limits on and expectations of agency powers. Key elements of the framework will be contained in the Act itself. The Act will be complemented by detailed and transparent policies, procedures or rules to deal with matters that are too specific to appear in legislation or are subject to frequent change.

## Views of the public are essential

The purpose of this paper is to seek early views on the principles that will guide the development of the proposed new legislative framework.

The paper provides an overview of how the Government proposes to reform the framework, with a particular focus on options for implementing key recommendations made by recent reviews. It will be complemented by public consultation throughout the development of the reforms, including the release of a public exposure draft of the legislation. This paper focuses primarily on powers that may be subject to change as part of the new Act. It does not consider all powers that exist under Australia's electronic surveillance framework in detail.

This will not be the last opportunity to provide input into this process. However, the feedback and submissions you provide in response to this paper will inform the key principles guiding the development of the draft legislation. Your views will help the Government develop draft legislation that reflects the interests, expectations and requirements of all stakeholders, including the Australian public.

The paper includes a number of targeted questions. The full list of questions is at **Attachment C**. It may be helpful to frame your submission around these questions. However, you may wish to address matters outside the scope of these questions.

There will also be opportunities to be heard on other national security reforms. **Part 7** of this paper outlines how the Government proposes to manage the interaction between other reforms and the development of a new electronic surveillance legislative framework. These reforms will be subject to targeted scrutiny and consultation processes.

## Before you comment

Not every aspect of the proposed new framework is discussed in detail in this paper. As such, this paper should be read alongside the [final report of the Comprehensive Review](#), particularly [Chapters 26 to 31 in Volume 2](#). The Comprehensive Review provides detailed analysis of key concepts discussed in this paper and further analysis of aspects of the reforms not touched on in this paper. The report also provides detailed commentary informing the recommendations discussed in this paper.

The following resources may also provide useful context for your submission:

- The existing legislative framework fact sheets in **Attachment A**.
- The table of corresponding legislative frameworks of other Five Eyes countries in **Attachment B**.
- The [Government response to the Comprehensive Review](#).
- The following Parliamentary Joint Committee on Intelligence and Security (PJCIS) inquiries and reviews:
  - [Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press](#)
  - [Review of the amendments made by the Telecommunications and Other Legislation Amendment \(Assistance and Access\) Bill 2018](#) (also subject to a recent [Independent National Security Legislation Monitor \(INSLM\) review](#))
  - [Review of the Surveillance Legislation Amendment \(Identify and Disrupt\) Bill 2020](#)
  - [Review of the Telecommunications Legislation Amendment \(International Production Orders\) Bill 2020](#)
  - [Review of the mandatory data retention regime](#)
  - [Review of the Intelligence Oversight and Other Legislation Amendment \(Integrity Measures\) Bill 2020](#)
  - [Review of the Foreign Intelligence Legislation Amendment Bill 2021](#)
  - [Review of the Security Legislation Amendment \(Critical Infrastructure\) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018](#)
  - [Review of Part 14 of the Telecommunications Act – Telecommunications Sector Security Reforms](#)
  - [Review of the Counter-Terrorism Legislation Amendment \(High Risk Terrorist Offenders\) Bill 2020](#).
- The Parliamentary Joint Committee on Law Enforcement (PJCLE) [inquiry into the impact of new and emerging information and communications technology](#)

# A guide to this discussion paper



## Part 1: Who can access information under the new framework?

The new framework will contain strict prohibitions and exceptions will be proposed under the new legislative framework. We seek your views on which law enforcement and intelligence agencies should have the ability to access data and personal information with strict safeguards and controls.



## Part 2: What information can be accessed?

The new framework will need to provide clarity to agencies, oversight bodies and the public about what kinds of data and personal information can be accessed. We seek your views on how the new framework might provide clearer definitions of key concepts in order to enhance privacy protections and endure technological advancements.



## Part 3: How can information be accessed?

The new framework will streamline the existing warrant framework to reduce the complexity of the process while improving transparency. We seek your views on the process to be used by agencies when seeking warrants and authorisations to use powers.



## Part 4: When will information be accessed?

The new framework will ensure that these powers are only authorised if necessary and proportionate. We seek your views on the situations in which powers should be used and for what purpose. We also seek your views on who can authorise the powers, under what circumstances and how the information can be further disclosed.



### **Part 5: Safeguards and oversight**

The new framework will maintain strict safeguards and robust oversight mechanisms, including more consistent and streamlined reporting and record-keeping requirements. We seek your views on what kinds of requirements agencies should be subject to and how oversight agencies could enhance information sharing.



### **Part 6: Working together: Industry and Government**

The communications industry plays an integral role in assisting with law enforcement and national security investigations. We seek your views on how the new framework could enhance the way agencies work with the communications industry and reduce the burden on industry by streamlining and consolidating obligations.



### **Part 7: Interaction with existing and recent legislation and reviews**

Electronic surveillance reform is a significant project. In the meantime, the Government will progress targeted amendments to resolve urgent gaps. These reviews will be considered as part of this reform.



### **Part 8: Getting involved**

This section outlines how the public, academia, industry and issue groups can contribute their experiences, learnings and challenges to inform this once-in-a-generation reform.

# **PART 1:** **WHO CAN ACCESS** **INFORMATION UNDER** **THE NEW FRAMEWORK?**

---



# The new framework will continue to protect information and data

Electronic surveillance powers are intrusive and can reveal sensitive information about an individual or organisation. As a general rule, covertly listening to a person's private conversations, observing a person's private activities or obtaining a person's private information or data should not be permitted.<sup>10</sup>

## Current State

There are a number of existing prohibitions and offences that apply to unlawful covert access to information and data. The Comprehensive Review did not make any recommendations about these prohibitions and did not consider that there were any gaps in the protection they provide. However, some of the TIA Act prohibitions rely on outdated definitions and will become increasingly difficult to apply to new technologies. There are also significant inconsistencies in the prohibitions across state and territory laws that apply to the use of surveillance devices.

### Telecommunications systems and computer networks

Offences concerning access to information and data on telecommunications systems and computer networks are in the following Acts.

- **TIA Act:** contains prohibitions relating to 'interception' and access to 'stored communications'. Section 7 of the TIA Act prohibits people from obtaining the content of a communication while it is being transmitted across a telecommunications network, e.g. a telephone call – this is called 'interception'. Section 108 of the TIA Act makes it an offence for people to access the *content* of a communication while a 'carrier' (such as Telstra) or a 'carriage service provider' (such as amaysim) holds it, e.g. a text message – this is called access to 'stored communications'.
- **Telecommunications Act:** contains offences that broadly prohibit persons involved in providing telecommunications services from disclosing and using information or documents that relate to communications or carriage services supplied to a person or the personal particulars of a person – this includes 'telecommunications data' or 'metadata'.<sup>11</sup>

---

<sup>10</sup> Article 17 of the International Covenant on Civil and Political Rights further provides that no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

<sup>11</sup> Telecommunications Act, section 276.



- ***Criminal Code Act 1995*** (the Criminal Code): contains a range of criminal offences for unlawfully accessing or interfering with a telecommunications system or accessing data in a computer without authorisation.<sup>12</sup>

Taken together, these offences and prohibitions prevent people, including government agencies, from accessing a person's communications and information on a person's computer or other device. Electronic surveillance powers provide an exception to these prohibitions, discussed further below.

However, elements of these prohibitions – in particular, the prohibitions on interception and access to stored communications – rely on outdated assumptions and terms.<sup>13</sup> Applying these outdated assumptions to modern technologies results in complexity and ambiguity. This creates a risk that the law may not properly protect the privacy of people's information.

These outdated assumptions and terms are discussed in more detail in **Part 2**.

## **Surveillance devices**

Commonwealth legislation does not currently prohibit the use of surveillance devices. This is governed by state and territory legislation. Each state and territory has legislation that prohibits people from using certain surveillance devices in certain circumstances. The prohibitions are different in each state or territory and variously apply to use of devices to:

- observe or visually record a private activity – called an 'optical device'
- record or listen to private conversations – called a 'listening device'
- determine the geographical location of a person or thing – called a 'tracking device'
- record or monitor the input and output of information to and from a computer – called a 'data surveillance device'.

Not all states and territories prohibit the use of all of these devices. Further, the prohibitions on use of these devices differ across the states and territories. For example, some states and territories only prohibit use of a listening device to listen to a private conversation to which the person is not a party. These differences mean the privacy protections for individuals vary between jurisdictions. This can also create difficulties where investigations cross state and territory borders.

---

<sup>12</sup> *Criminal Code Act 1995* Schedule 1 (the Criminal Code), Parts 10.6 and 10.7.

<sup>13</sup> See discussion in the Comprehensive Review, Volume 2, at paragraphs [26.106]–[26.114].

## Case study

For example, a number of people invested in various investment schemes presented by a company at information seminars conducted in various states. The Australian Securities and Investments Commission (ASIC) was provided with recordings of these seminars because the company allegedly made false and misleading statements about the schemes. However, the status of each of the recordings – including whether they had been lawfully made and whether they could be admitted as evidence – was subject to the location of where the recordings were made. Recordings made in jurisdictions which permitted such recordings supported the complaints and provided evidence of the false and misleading statements made. Recordings made in jurisdictions where such recordings were prohibited could not be relied upon as evidence. In addition, those who had recorded the seminars could be liable for prosecution in certain jurisdictions.

## Potential Future State

In developing the new framework, the Government will consider the appropriateness of existing prohibitions and whether any additional protections are necessary. This includes:

- The criminal offences concerning interference with telecommunications systems and accessing data on computers in the Criminal Code.
- The offences that relate to telecommunications data in the Telecommunications Act. It may be necessary to revise these offences depending on how the framework deals with telecommunications data more broadly.
- The prohibitions relating to interception and access to stored communications. It may be useful to combine these prohibitions into a new consolidated prohibition and offence. This may not retain the distinction between interception and stored communications. The prohibition and offence may be in the new framework itself. Alternatively, it may be included elsewhere, such as in Part 10.6 of the Criminal Code relating to interference with telecommunications systems.

In 2014, the Australian Law Reform Commission recommended the Commonwealth enact legislation to replace state and territory surveillance device laws.<sup>14</sup> The Comprehensive Review noted that adopting the Commission's recommendation would substantially increase the complexity of the reform process.<sup>15</sup>

---

14 Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report No. 123, Australian Law Reform Commission, 2016, recommendation 141.

15 The Comprehensive Review, Volume 2, pages 265–266, footnote 613.

The Commonwealth has powers under section 51 of the *Australian Constitution* that could enable the Commonwealth to enact a more comprehensive regime prohibiting the use of surveillance devices.<sup>16</sup> However, any Commonwealth prohibition on surveillance devices could render state and territory surveillance device legislation inoperative.

A Commonwealth surveillance device prohibition could create consistency across all jurisdictions. For example, this could assist in targeting improper or harmful use of devices in domestic violence cases, where inconsistencies in state and territory legislation may create gaps in investigating and prosecuting these offences. However, any prohibition would also need to ensure that everyday activities are not unduly restricted.

In light of this, the Commonwealth will work with states and territories to ensure the new framework is harmonised with state and territory legislation to provide appropriate protections against observing activities, listening to conversations and tracking a person's movements through the unauthorised use of surveillance devices.

## Questions

1. Do the existing prohibitions and offences against unlawful access to information and data adequately protect privacy in the modern day?
  - a. If so, which aspects are working well?
  - b. If not, which aspects are not working well and how could the new prohibition and/or offences be crafted to ensure that information and data is adequately protected?
2. Do the existing prohibitions and offences against unlawful access to information and data adequately allow the pursuit of other objectives, e.g. cyber security of networks, online safety or scam protection/reduction?

---

<sup>16</sup> The most relevant is section 51(v) which relates to the 'communications' power. In addition, the Australian Law Reform Commission's report on *Serious Invasions of Privacy in the Digital Error* (June 2014) identified that a Commonwealth surveillance device prohibition would likely be supported by the external affairs power in s 51(xxix).

# Access to information will be strictly controlled

Covert access to an Australian's information and data is generally prohibited. However, limited access to this information is sometimes needed for some government agencies to perform their functions. Law enforcement agencies and ASIO require electronic surveillance powers to investigate serious crime and respond to national security threats.<sup>17</sup>

There are, and must continue to be, exceptions to these prohibitions so these agencies can use these powers where necessary and proportionate to protect the community from serious harm. These exceptions will be subject to strict limitations and robust safeguards. Accountability and transparency measures will include reporting and record-keeping requirements, proportionality tests and independent oversight by bodies with appropriate experience, scope and powers.

There are also some circumstances in which it is necessary and appropriate for certain persons and bodies outside Government to be able to access a person's information and data without that person's knowledge or permission. For example, under the TIA Act the companies that own and operate telecommunications systems may intercept communications in order to run and maintain those systems. The new framework will need to include some limited exceptions of this kind.

## Current State

There are currently 21 Commonwealth, state and territory agencies that can obtain warrants and authorisations to use electronic surveillance for certain purposes under the TIA Act, SD Act or ASIO Act. These agencies include law enforcement agencies, anti-corruption and integrity bodies, and ASIO. Not all of these agencies have access to *all* electronic surveillance powers. Currently, a slightly larger number of agencies can access stored communications than can intercept communications or use computer access or surveillance devices.

A summary of which agencies can access particular electronic surveillance powers is set out at **Attachment D**.

It is also possible for some other organisations to lawfully access telecommunications data under sections 280 and 313(3) of the Telecommunications Act. Concerns have been raised that the current effect of these sections may go beyond what was intended by Parliament and could be used to circumvent restrictions in the TIA Act on which agencies can access telecommunications data.

---

<sup>17</sup> Law enforcement agencies includes anti-corruption and integrity bodies, which make up a large proportion of the agencies with access to powers under the current framework.

## Potential Future State

Agencies will only be able to use electronic surveillance powers where those powers are needed to perform their functions. The reform does not propose to remove any existing powers under the TIA Act, SD Act and ASIO Act from any agencies. In line with the Government's response to recommendation 15 of the PJCIS review of the mandatory data retention scheme,<sup>18</sup> the Government will consider which bodies should have access to telecommunications data or metadata under Telecommunications Act sections 280(1)(b) and 313(3).

However, other agencies seeking particular electronic surveillance powers may be provided with additional powers where a clear and compelling case is made by that agency. In line with recommendations of the Comprehensive Review and other reviews,<sup>19</sup> the Government will consider providing:

- the Australian Transaction Reports and Analysis Centre (AUSTRAC) with the power to access telecommunications data for the purposes of fulfilling its dual financial intelligence and regulatory roles to prevent money laundering and terrorism financing
- the Australian Taxation Office (ATO) with the power to access telecommunications data for the purpose of protecting public revenue from serious financial crimes
- state and territory corrective services with the power to access telecommunications data, for the purposes of monitoring criminal offenders
- the Australian Border Force with the power to use tracking devices to investigate border-related measures
- the Australian Criminal Intelligence Commission (ACIC) with the power to use its electronic surveillance powers for a slightly wider range of investigations.

Each of these additional powers has been recommended by either the Comprehensive Review or a parliamentary committee.<sup>20</sup>

---

18 PJCIS, Review of the mandatory data retention scheme of the *Telecommunications (Interception and Access) Act 1979* (Data Retention review), Commonwealth of Australia, Canberra, 2020, Recommendation 15.

19 This includes the PJCLE's *Inquiry into financial related crime, the Treasury Black Economy Taskforce's Final Report*, and the Inspector-General of Taxation's *Review into the Australian Taxation Office's fraud control management*.

20 See Comprehensive Review report, Volume 2, recommendations 77–79 and 88 and the PJCLE's 2015 report from its *Inquiry into financial related crime*, recommendation 3.

## Case study

In most cases granting access to these additional powers will complement existing investigative powers. For example, with respect to the ATO, access to telecommunications data would support or, in some cases, potentially replace expensive, resource-intensive and intrusive physical surveillance operations. ATO experience demonstrates that telecommunications data would also be a critical tool in excluding non-involved individuals from lines of inquiry, or in establishing a relationship between an original person of interest being investigated (for example, for tax fraud) and a larger group of individuals committing serious criminal offences (such as large-scale fraud against the Commonwealth).

When deciding whether any additional agency (other than those listed above) should have access to particular powers in the new framework, the Government will consider the following questions.

- Does the agency typically deal with the investigation, prevention or enforcement of crimes that merit access to such information?
- Does the agency need access to electronic surveillance powers to effectively perform its functions and, if so, which powers in particular?
- Are there other effective mechanisms the agency could use to obtain the information it needs?
- Does the agency have appropriate expertise and privacy safeguards, including secure systems, facilities and processes in place to deal with information received through electronic surveillance?
- Does the agency have appropriate processes in place to allow it to comply with the law (for example, does it have processes in place to meet record-keeping and reporting requirements)?
- Is it in the public interest for the agency to have these powers, considering the severity of any public harm that may result in the absence of the powers?
- Are there any other factors in favour of, or against, giving the agency these powers?
- Are there appropriate oversight mechanisms in place?

## Questions

3. Are there any additional agencies that should have powers to access particular information and data to perform their functions? If so, which agencies and why?
4. Do you agree with the proposed considerations for determining whether additional agencies should be permitted to access peoples' information and data? Are there any additional considerations that have not been outlined above?

# PART 2: WHAT INFORMATION CAN BE ACCESSED?

---



Electronic surveillance powers are increasingly vital investigative tools for law enforcement agencies and ASIO. The legislation underpinning these powers needs to be easily understood to enhance transparency. This will also improve the framework's application by agencies and industry and provide clarity for oversight bodies.

The Comprehensive Review noted that the existing framework is long, complicated and difficult to understand. The framework is also underpinned by a range of outdated assumptions. Applying these assumptions to modern technology compounds the lack of clarity.<sup>21</sup>

In line with the Comprehensive Review's recommendation, the core definitions in the new framework will aim to:

- provide clarity to agencies, oversight bodies and the public about the scope of agencies' powers
- ensure there are no gaps in the types of information that agencies may access or obtain under warrants and authorisations
- be capable of applying to new technologies over time.<sup>22</sup>

Key concepts underpinning the new framework must provide clarity about what information is protected and what information agencies can obtain. The core concepts and definitions relating to the powers will help determine what kinds of information can be accessed, and in what form it can be accessed, under each warrant and authorisation. In developing the new framework, the Government will reconsider a number of core concepts, such as:

- the definition of a 'communication'
- the distinction between 'content' and 'non-content' information
- the distinction between 'live' and 'stored' communications
- the kinds of providers that hold relevant information and data
- the kinds of information that may be obtained through surveillance and tracking devices.

---

21 For more detail, see discussion in the Comprehensive Review, Volume 2, at paragraphs [26.106]–[26.126].

22 The Comprehensive Review, Volume 2, recommendation 109.



# Communications: What does this mean in 2021 and beyond?

## Current State

The definition of ‘communication’ is fundamental to the operation of the TIA Act. The provisions of the TIA Act apply to intercepting or accessing ‘communications’, and the powers given to agencies to access ‘communications’. However, the definition of ‘communications’ is unclear and its application to modern technologies is complex and artificial.

The TIA Act defines communications as including (but not being limited to) a ‘conversation and a message’. This can be in the form of speech, music or other sounds, data, text, visual images, signals or any other form or combination of forms. This definition was introduced in 1989 and has not been amended since. The definition reflects the era in which it was drafted. As the Comprehensive Review noted, at that time, conversations and messages between people were the main type of information carried across the telecommunications network.<sup>23</sup> In contrast, there is now a wider range of information and data passing over the telecommunications network, such as machine-to-machine signals between servers, routers and modems that enable the network to route communications to their intended destination.

Whether the TIA Act prohibits access to something depends on whether that thing is a ‘communication’. However, it is becoming increasingly difficult to determine which kinds of information can be classed as ‘communications’. Determining whether a particular new kind of information or interaction is a ‘communication’ can be complex. For example, it is unclear whether those machine-to-machine signals form part of a ‘conversation’ or ‘message’, and therefore whether they are a ‘communication’ within the meaning of the TIA Act.

Whether something is a communication therefore has significant consequences for whether that information is protected. As a result, there may be gaps in the limits, controls and safeguards that apply to this information, even where it is passing over the telecommunications network.

While this definition can still be applied to modern communications technology, it will become even harder to apply as technology develops. This creates difficulties for agencies in using existing powers and for oversight bodies in overseeing use of the powers. It also reduces transparency, as the legal protections and the powers available to agencies cannot be readily understood by reading the legislation.

---

23 The Comprehensive Review, Volume 2, paragraph [26.112].

## Potential Future State

The reform aims to replace the outdated concept of ‘communications’ with a term and definition that reflects the range of information and data transmitted electronically. The definition will be as technology-neutral as possible so that it can apply to future information and communications technologies. This will ensure the full range of information and data transmitted electronically is protected from unauthorised access.

In developing this definition and other key concepts, the Government will consider how to best capture the following kinds of information.

- Electronic conversations and messages between people, whether they are travelling between devices or stored by a telecommunications provider or on a person’s device or personal network. This includes phone calls, emails, instant messages, video conversations and conversations via over-the-top messaging applications. It may also include draft emails and instant messages that sit on a carrier or carriage service provider’s server but which have not been sent.
- A person’s activities on the internet. This includes web-browsing history, URLs visited by a person and a person’s use of non-messaging applications on their smart phone.
- Electronic documents, files, images or other content created by a person, regardless of whether they are transmitted to another person. This includes text documents or images a person saves on their computer or uploads to a cloud storage service such as Dropbox or Google Drive.
- Interactions between a person and a machine. This includes instant messages between a person and an automated system, such as a customer service chat-bot.
- Interactions/signalling information between a machine and another machine. This includes interactions between devices on the Internet of Things – for example, data generated by connected or autonomous vehicles, or smart home security systems.<sup>24</sup>
- Emerging technologies, such as machine learning and information derived from quantum computing.

Modernising the definition of communication will likely result in more information being protected and better controls on access to that information. Under the new framework, government agencies will only be able to access this broader range of information under a warrant or authorisation, and this access will be subject to robust oversight and safeguards.

---

<sup>24</sup> The ‘Internet of Things’ refers to the interconnection via the internet of computing devices embedded in everyday objects, enabling them to send and receive data. Examples include AI voice assistants such as Amazon Echo and Google Home, smart home security systems and appliances with internet connectivity.

There are several examples that may be considered when designing a new technology-neutral definition of communications. For example, the definition of communications in the Telecommunications Act,<sup>25</sup> and international examples from New Zealand<sup>26</sup> and the United Kingdom,<sup>27</sup> provide useful starting points when considering how the existing definition in the TIA Act could be expanded.

The interaction between the new definition and other legislation that relies upon that terminology will need to be considered. Industry will require clarity as to the scope of the new definition and will be closely consulted as part of its development.

## Questions

5. Are there other kinds of information that should be captured by the new definition of ‘communication’? If so, what are they?
6. Are there other key concepts in the existing framework that require updating to improve clarity? If so, what are they?
7. How could the framework best account for emerging technologies, such as artificial intelligence and information derived from quantum computing?

# Information about a communication is different to its content

## Current State

Under the TIA Act, the way in which agencies can obtain information depends on whether that information is the ‘content’ of a communication or ‘non-content’ information.

Broadly speaking, ‘content’ information is the substance or meaning of a communication – for example, the words said in a phone call or written in the body of an email. ‘Non-content’ information is information *about* a communication – for example, the time at which a phone call was made, the duration of the phone call and the participants in the call.

---

<sup>25</sup> Telecommunications Act, section 7.

<sup>26</sup> *Intelligence and Security Act 2017* (NZ), section 47.

<sup>27</sup> *Investigatory Powers Act 2016* (UK), section 261.

Typically, agencies require a warrant to obtain the ‘content’ of a communication, while they can obtain ‘non-content’ information through the TIA Act and Telecommunications Act. Under the TIA Act, a request for this type of information is usually authorised by a senior officer within the agency (internal authorisation). This is because ‘non-content’ information is perceived to be less private than ‘content’ information.<sup>28</sup> This distinction is highly significant for agencies and oversight bodies.

The distinction is also important for industry. The TIA Act provides that communications service providers must maintain certain datasets about the services they provide and communications made on those services – this is called the ‘mandatory data retention regime’. Among other information, providers must keep the name of the subscriber of a service; the source, destination, date, time, duration and type of a communication on the service; and the location of equipment used in connection with a communication. The TIA Act includes a description of the kinds of information that must be kept.<sup>29</sup>

The TIA Act also specifies information that providers do not need to keep. Importantly, under the Act providers do not need to keep ‘information that is the contents or substance of a communication’ – that is, ‘content’ information.<sup>30</sup> For this reason, under a stored communications warrant, agencies can only access information that the provider has stored of its own volition, or as required by a preservation notice.<sup>31</sup>

There is currently no definition for ‘contents or substance’.

The distinction between ‘content’ and ‘non-content’ is not clear-cut in the existing framework. For example, it is unclear whether a URL is content or non-content information. On one hand, a URL could be seen as non-content, in that it is a ‘delivery instruction’, like the address of a communication. On the other hand, accessing a URL may also reveal the content a person viewed on a website. This lack of clarity creates a risk that providers may inadvertently keep and disclose content information to agencies without a warrant in response to a request for ‘non-content’ information.

## Potential Future State

In its review of the mandatory data retention regime, the PJCIS recommended the term ‘content or substance of a communication’ be defined.<sup>32</sup> Defining the terms ‘content’ and ‘non-content’ will provide certainty for agencies and providers and will improve privacy protections by reducing the risk that ‘content’ information will be inadvertently disclosed without a warrant.

---

28 Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, paragraph 9.

29 TIA Act, section 187AA.

30 TIA Act, paragraph 187A(4)(a).

31 TIA Act, Chapter 3.

32 Data Retention review, recommendation 2.

In line with the recommendations of the PJCIS, the Government will consider how ‘content’ information could be defined. The wording used to define ‘content’ and ‘non-content’ information will depend on the approach taken to defining ‘communications’ in the new framework. The definition will be developed in consultation with a range of agencies, industry bodies, oversight agencies and civil society organisations.

An example of a modern definition of ‘content of a communication’ adopted by the UK is:

- *Content*, in relation to a communication and a telecommunications operator, telecommunications service or telecommunication system, means any element of the communication, or any data attached to or logically associated with the communication, which reveals anything of what might reasonably be considered to be the meaning (if any) of the communication, but –
  - a) any meaning arising from the fact of the communication or from any data relating to the transmission of the communication is to be disregarded, and
  - b) anything which is systems data is not content.<sup>33</sup>

In developing the framework, the Government will consider whether it is necessary to revise the scope of non-content information. The Government will also consider whether there is benefit in distinguishing between different kinds of non-content information and how that information is treated. For example, the UK has different authorisation levels for two different categories of non-content data – ‘entity data’ and ‘events data’.

- ‘Entity data’ is information relating to ‘entities’ such as persons, groups, mobile phones, computers or other communication devices. This includes information identifying the subscriber of a phone number or the holder of an email account, billing information for an account, or information about a device used by a subscriber or account holder.
- ‘Events data’ is information about particular things happening over a telecommunications system at a particular time. This includes information about the sender and/or recipient of a communication, numbers called by a person, internet connection records, the time and duration of a call or internet connection, the size of data downloaded or uploaded, or the location of a phone when a call is made or received.

---

33 *Investigatory Powers Act 2016* (UK), section 261. Section 263 of that Act defines ‘systems data’ to mean: ‘any data that enables or facilitates, or identifies or describes anything connected with enabling or facilitating, the functioning of any of the following:  
(a) a postal service;  
(b) a telecommunication system (including any apparatus forming part of the system);  
(c) any telecommunications service provided by means of a telecommunication system;  
(d) a relevant system (including any apparatus forming part of the system);  
(e) any service provided by means of a relevant system.’

## Questions

8. What kinds of information should be defined as ‘content’ information? What kinds of information should be defined as ‘non-content’ information?
9. Would adopting a definition of ‘content’ similar to the UK be appropriate, or have any other countries adopted definitions that achieve the desired outcome?
10. Are there benefits in distinguishing between different kinds of non-content information? Are there particular kinds of non-content information that are more or less sensitive than others?

## Is there a real difference between ‘live’ and ‘stored’ communications anymore?

### Current State

The TIA Act draws a distinction between:

- intercepting ‘live’ communications (for example, a phone call in the course of transmission), and
- accessing ‘stored’ communications held by a carrier or carriage service provider (for example, a voicemail or an email stored on a provider’s servers).

This distinction affects the protections applying to information and how agencies can access that information. For law enforcement agencies, the threshold for intercepting live communications is higher than the threshold for accessing stored communications. Other requirements in the TIA Act, such as the purposes for which communications can be used and shared, also differ based on whether the information was intercepted when live or accessed when stored.

The provisions concerning stored communications were added to the TIA Act in 2006. This distinction reflects the view at that time that stored communications, such as a voicemail or email, would generally be more ‘considered’ and less spontaneous than a live communication such as a phone call.<sup>34</sup> On this basis, the distinction assumes that accessing stored communications is less intrusive than intercepting live communications.

Under section 109 of the TIA Act, ASIO may obtain an interception warrant for both live and stored communications.

---

<sup>34</sup> The Comprehensive Review, Volume 2, paragraphs [26.110]–[26.111].

## Potential Future State

The Comprehensive Review considered this distinction to be less significant than it may once have been.<sup>35</sup> Many conversations once held over the phone are now conducted by text messaging or other communications applications. As the way in which people communicate has shifted significantly, this distinction has little current relevance or use.

In practice, the distinction also leads to inconsistent protections for the same information. Many communications can either be intercepted while live or accessed while stored. For example, a text message could be intercepted while being transmitted or accessed after it is delivered and while it is stored on a provider's systems or person's device. This means the protections applicable to a particular communication will change significantly when the communication ceases to be transmitted and goes from being 'live' to being 'stored', despite there being no change in the content (or privacy sensitivity) of the communication.

### Questions

11. Should the distinction between 'live' and 'stored' communications be maintained in the new framework?
12. Do each of these kinds of information involve the same intrusion into privacy? Or should the impact of each be considered differently?

## Australians no longer communicate exclusively using services provided by Australian carriers and carriage service providers

### Current State

All stored communications warrants, most interception warrants and all telecommunications data authorisations are given to a 'carrier' or a 'carriage service provider' under Australian law. The provider then intercepts or accesses the communication or data and provides it to the requesting agency.

---

<sup>35</sup> For more detail, see discussion in the Comprehensive Review, Volume 2, at paragraphs [26.108]–[26.111].

A carrier is an entity that owns telecommunications infrastructure or facilities used to deliver 'carriage services' to the public. Carriage services are services for carrying communications, including things like phone or internet services. Carriers include companies such as Telstra, Vodafone and NBN Co. A carriage service provider is an entity that delivers carriage services over carriers' infrastructure or facilities, such as amaysim and ALDImobile.

Both carriers and carriage service providers have obligations under the existing framework. These include maintaining interception capability plans and keeping certain types of data. This is to ensure providers can assist requesting agencies whenever assistance is required.

However, the definition of 'carriage service provider' is broad.<sup>36</sup> It can sometimes be difficult to determine whether a provider is a 'carriage service provider'. This means it is not always clear whether a provider must comply with interception and stored communications warrants or retain or disclose telecommunications data.

Furthermore, there are now a range of global entities involved in the communications process that are not traditional carriers or carriage service providers. For example, data centre operators<sup>37</sup> and equipment manufacturers play an important role in the telecommunications supply chain but are probably not carriers or carriage service providers. Providers of 'over-the-top' messaging applications, such as Facebook and Fastmail, also play key roles in the communications process. The Government will consider whether over-the-top providers are adequately captured under existing arrangements or whether further changes are required under the new framework.

The new framework will require greater certainty as to which entities are carriage service providers for the purposes of the TIA Act. This is significant because the prohibition on accessing stored communications only applies to information held by carriers or carriage service providers. Further, stored communications warrants, interception warrants and telecommunications data authorisations only apply to carriers or carriage service providers.

In contrast, the obligations in the industry assistance framework in Part 15 of the Telecommunications Act (discussed in **Part 6**) apply to 'designated communications providers'. This term captures a much wider range of companies, organisations and individuals who contribute to the communications supply chain in Australia. This includes telecommunications operators, providers of electronic services, developers of software and manufacturers of devices.

---

36 'Carriage service provider' is defined in section 87 of the Telecommunications Act to include a person who supplies, or proposes to supply, a 'listed carriage service' to the public using a 'network unit' owned by one or more carriers or a network unit in relation to which a 'nominated carrier declaration' is in force. 'Carriage service' means a service for carrying communications by means of guided and/or unguided electromagnetic energy.

37 A data centre is a centralised facility that houses computing and networking equipment. Data centres are a core component of modern telecommunications infrastructure, as telecommunications companies increasingly use data centres to store data. However, data centre operators are not carriers or carriage service providers.



The international production order framework in Schedule 1 to the TIA Act applies to a range of foreign entities, including several kinds of providers that are not carriers or carriage service providers. Under this framework, where Australia has a ‘designated international agreement’ with a foreign country (such as the prospective Clarifying Lawful Overseas Use of Data (CLOUD) Act Agreement between Australia and the USA) Australian law enforcement agencies and ASIO can obtain orders seeking communications and related data from foreign providers. This includes providers of ‘message application services’ (like Facebook and WhatsApp), ‘video call application services’ (like Skype) and ‘storage/backup services’ (like Dropbox).

## Potential Future State

The new framework will aim to provide greater clarity about which kinds of communications service providers must execute, or assist with the execution of, electronic surveillance warrants, authorisations or assistance orders. In developing the framework, the Government will consider what kinds of entities involved in the communications supply chain, in addition to traditional carriers and carriage service providers, must meet these obligations. Changes may be needed if existing or potential future providers the community would expect to be subject to these obligations are not captured. The question of which obligations should apply to which providers is further discussed in **Part 6**.

Any change to the range of providers that must provide communications or technical assistance to agencies should avoid placing unnecessary additional burdens on Australian industry. Any change would also need to consider jurisdictional limitations. For example, providers based in the USA may be prevented by US law from complying with a request for communications unless it is issued under the CLOUD Act Agreement.

### Question

13. What type of Australian communications providers should have obligations to protect and retain information, and comply with warrants, authorisations and assistance orders under the new framework?

# Regulation of surveillance devices focuses on types of device, not kinds of information

## Current State

The SD Act regulates some law enforcement agency use of surveillance devices. For state and territory agencies, this is sometimes regulated by their state or territory legislation. ASIO's use of surveillance devices is governed by Subdivision D of Division 2 of Part III of the ASIO Act. Broadly, the SD Act and the ASIO Act regulate the use of surveillance devices by reference to kinds of devices, rather than kinds of information. Warrants under these Acts allow the use of specified *kinds of devices* but do not consider the *kinds of information* that can be obtained using these devices. The definitions of these devices in the Acts focus on device capability. For example:

- a device capable of being used to visually record or observe an activity (optical surveillance device)
- a device capable of being used to overhear, record, monitor or listen to sounds, signals or a conversation, or words spoken to or by any person in conversation (listening device)
- a device capable of being used to track a person or an object (tracking device in the ASIO Act) or a device capable of being used to determine or monitor the location of a person or an object or the status of an object (tracking device in the SD Act).<sup>38</sup>

The SD Act also regulates 'data surveillance devices', which are devices that can record or monitor the input of information into, or the output of information from, an electronic device for storing or processing information.

Both the SD Act<sup>39</sup> and the ASIO Act<sup>40</sup> allow tracking devices to be used under internal authorisation where the use of the device does not involve entry onto premises or interference with the interior of a vehicle without the owner's permission. This differs from the approach taken in some state and territory legislation, which requires a court order.<sup>41</sup> In addition, both the ASIO Act and the SD Act allow use of surveillance devices without a warrant in certain circumstances.<sup>42</sup> For example, a federal law enforcement officer may use an optical surveillance device where use of the device does not involve entry onto premises or interference with any vehicle or thing without permission.<sup>43</sup>

---

38 ASIO Act, section 22; SD Act, section 6.

39 SD Act, section 39.

40 ASIO Act s26G, s26J.

41 For example, under section 14 of the *Surveillance Devices Act 1999* (Vic), a Supreme Court judge may issue a warrant for the use of any surveillance device. A magistrate may issue a surveillance device warrant that authorises the use of a tracking device only.

42 ASIO Act, sections 26C and 26D; SD Act, Part 4.

43 SD Act, section 37.

The ability to use surveillance devices without a requirement to obtain a warrant provides agencies with greater flexibility to collect information in limited circumstances, where that collection will typically have a lesser impact on privacy. For example:

- use of cameras in public places, with legal certainty that information they collect will not be rendered inadmissible if they inadvertently record a privacy activity, and
- record conversations to which an officer or human source is a part and therefore is not a private conversation in relation to that person.

## Potential Future State

In developing the new framework, the Government will consider whether the framework should keep the current approach to regulating the use of kinds of surveillance devices, or instead regulate the type of information that can be obtained. In doing so, the Government will consider whether it is necessary to redefine the kinds of information that can be captured by surveillance devices.

As discussed in **Part 4**, the new framework may include different thresholds for use of devices that provide information about private activities and communications and for devices that only provide information about a person's movements. As such, the Government will consider how to define and distinguish between the kind of information obtained by listening and optical devices and the kind of information obtained by tracking devices.

It is important to note that devices can often be used to obtain different types of information. For example, the kinds of information obtained by a data surveillance device can overlap with the kinds of information that may be considered a 'communication', outlined above. It is the Government's intention that the new framework is clear about the types of information agencies are able to obtain under each warrant and authorisation.

The Government will work closely with states and territories to ensure that these concepts and definitions are considered alongside state and territory surveillance and tracking device legislation.

### Question

14. What are your thoughts on the above proposed approach? In particular, how do you think the information captured by surveillance and tracking devices could be explained or defined?

# PART 3: HOW CAN INFORMATION BE ACCESSED?

---



# Is a warrant framework that emphasises impact on privacy over method of access the way forward?

As the communications environment has become more complex, so too have the legal frameworks for accessing communications.

Without a new approach, the variety of warrants and authorisations will continue to increase as agencies are forced to develop new methods in response to technological developments. This will increase the complexity of the framework, raise the risk of inconsistencies and capability gaps, and create inefficiencies, and may result in compliance issues.

The new framework will adopt a more technology-neutral, streamlined and flexible approach to governing law enforcement agencies' and ASIO's use of electronic surveillance. However, efficiency will not come at the cost of transparency or privacy protections. The new framework will encourage an emphasis on what information agencies are trying to collect, the intrusiveness and the matter being investigated, instead of the current focus on how they intend to collect it.

## Current State

At present, agencies may obtain certain types of information under more than 35 different warrants and authorisations. These warrants broadly enable agencies to undertake specific activities such as:

- intercepting communications passing over a telecommunications network (e.g. listening to a live telephone conversation)
- accessing a computer or a network of computers (e.g. accessing information on a person's mobile phone or laptop)
- using an optical, listening or data surveillance device (e.g. video surveillance and recording devices)
- accessing stored communications (e.g. accessing a person's text messages stored by a carrier)
- using a tracking device (e.g. monitoring a person's physical location).

In many cases there is considerable overlap between the types of information agencies can access under these warrants. For example, interception, stored communications, data surveillance devices and computer access powers all enable access to private communications and information. The Comprehensive Review described this as 'functional equivalency'. It noted that although these powers operate in different ways, they all have a similar privacy impact.

The Comprehensive Review considered whether electronic surveillance powers in the current framework are similar in nature or intrusiveness – that is, whether they are ‘functionally equivalent’. In doing so, it considered the objectives of the powers, broadly categorising these as covertly accessing private information, covertly tracking movements or covertly obtaining records or information about communications.

The number of warrants and their overlapping nature is partly due to the current framework’s focus on the technology or method an agency uses to obtain information, as opposed to the type of information or outcome.

For example, rather than authorising access to a particular type of information, such as communications content, a warrant will generally authorise use of a particular method, such as telecommunications interception, in an effort to obtain this information.

A problem with this approach is that the current framework is based on outdated views of how people communicate and interact. The existing framework was formed in the 1960s and 1970s, when electronic communications mainly consisted of telephone calls and telegrams. Since then, Australia has seen the widespread adoption of mobile telecommunications, the internet, personal computing and mobile internet access.

While frequent amendments have been made to the legislation in response to technological changes, the changing ways people communicate as technology advances will become more difficult to address through such amendments.

A warrant framework focused mainly on the method used to obtain information lacks the flexibility needed to keep pace with rapid technological advances. It requires frequent and substantial amendments to ensure agencies’ powers keep pace with changes in technology and the methods used by those being investigated.

## **Potential Future State**

A simpler warrant framework will improve the accessibility and utility of the framework and support compliance with legislative responsibilities.

One way to achieve this would be to shift the emphasis from a method-based framework to a more outcome-based framework. For example, an issuing authority could authorise an agency to access certain types of information (e.g. the content of a target’s electronic communications) without limiting the methods used. This would also allow a greater emphasis on the privacy impact of obtaining access to that information and on the offences or threats being investigated.

While the aim is for the legislation to remain as technology-neutral as possible, the method of access will be a key consideration for the issuing authority when assessing the privacy impact of the warrant and its necessity and proportionality. For example, as part of the warrant application, an agency will likely be required to satisfy the issuing authority that the proposed methods of access are the least intrusive means available that would be effective in the circumstances. This may involve the agency justifying those methods over less intrusive alternatives.

To achieve this, the new warrant framework will likely change a number of existing warrants. For example, instead of separate warrants for individual methods of access (e.g. telecommunications interception, accessing stored communications, computer access or use of a data surveillance device), the new framework could contain more consolidated outcomes-based warrants. In doing so, the new Act could allow agencies to obtain one warrant for access to electronic communications and one warrant for access to surveillance information in relation to a particular offence or security threat.

Certain matters could be specified in the warrant application so the issuing authority can make an informed assessment of the necessity and proportionality of the proposed actions. For example, agencies might need to specify whether they will obtain access to the information with assistance from a communications provider or through their own technical capabilities. Agencies would also be required to detail (to the extent possible) the particular technical methods they propose to use to access the information (e.g. interception or computer access).

Subordinate legislation or rules could be used to support a streamlined, outcomes-based warrant framework to deal with detailed matters that are likely to change frequently (e.g. due to rapid technological change). They could also be used to provide further information on technical matters (such as methods of access) and administrative detail associated with executing the methods/activities.

Shifting to an information type-focused and technology-neutral framework would have several benefits, including:

- putting privacy at the centre of the framework by requiring issuing authorities to consider the level of intrusion and the type and volume of information being accessed
- reducing the complexity of the framework and providing greater transparency around what information can be accessed by agencies
- creating a simpler, more accessible framework by reducing the overlap between multiple warrants in the existing framework

- preventing capability gaps for law enforcement agencies and ASIO by creating greater flexibility and limiting the need for frequent amendments to account for new technologies or methods.<sup>44</sup>

It will be important for a simpler warrant framework to ensure sufficient transparency about the types of activities agencies can undertake. This could be done, for example, by setting out in legislation the powers that can be exercised under warrant and including general descriptions of the ways agencies access information. This is important for parliament and the public to review and understand agencies' powers.

## Questions

15. How could the current warrant framework be simplified to reflect the functional equivalency of many of the existing warrants while ensuring appropriate privacy protections are maintained?
16. What other options could be pursued to simplify the warrant framework for agencies and oversight bodies, while also enabling the framework to withstand rapid technological change?

---

44 See for example The Comprehensive Review, Volume 2, paragraphs [27.12] and [27.13].



# PART 4: WHEN WILL INFORMATION BE ACCESSED?

---



# Access will only be permitted in order to investigate or disrupt crimes and threats to national security

As technology has developed, it has become more difficult for agencies to identify criminals and the devices they use to facilitate criminality. This has resulted in a patchwork of legislative amendments providing agencies with powers to protect the community from emerging threats. For this reason, the existing warrant framework contains a range of warrants to enable agencies to identify a person of interest, collect evidence on a person or third parties, disrupt serious criminal activity and collect intelligence on people or groups – all with a range of differing legislative thresholds.

The new Act will harmonise the existing warrant framework to provide more consistent safeguards on the authorisation and use of electronic surveillance powers, and to ensure protections in relation to privacy apply equally across the framework. Consideration will also be given to strengthening authorisation requirements for all applications to explicitly require an issuing authority to consider necessity and proportionality before authorising access to information or data. In addition, the Government will consider how thresholds for access to electronic information align with equivalent thresholds for access to information in the physical world – for example, where similar information could be obtained through electronic surveillance, or under a search warrant by obtaining physical documents in a filing cabinet.

## Access to private communications, content data and surveillance information

### Current State

Under the current framework, agencies need separate warrants to intercept communications, access stored communications, access computers or use surveillance devices to access information. Other powers, such as accessing telecommunications data or using some tracking devices, may be authorised internally. As outlined in **Part 3**, these powers provide a number of different means of covertly accessing private information.

Despite the overlap between powers and their similar levels of intrusiveness, they are not subject to a consistent approach in terms of thresholds, purposes, safeguards or accountability. For example, law enforcement agencies can generally only use interception powers for an investigation of an offence carrying a maximum penalty of imprisonment of 7 years or more – such as murder, kidnapping or child sexual abuse – with a range of exceptions to this threshold. In comparison, a computer access warrant, which can enable access to the same type of information (private communications), only requires that agencies be investigating an offence carrying a maximum penalty of imprisonment of 3 years or more – for example, stalking or using a carriage service to menace.<sup>45</sup>

Similarly, in order to obtain a warrant to intercept communications, ASIO must show that a person is engaged in, or likely to be engaged in, activities prejudicial to security, and interception will assist ASIO in obtaining intelligence relating to security. In contrast, to obtain a computer access warrant ASIO must show that access to a computer will substantially assist the collection of intelligence in respect of a matter that is important in relation to security.

## Potential Future State

As a general principle, the Comprehensive Review found that where powers are functionally equivalent, they should be subject to the same limits, controls and safeguards.<sup>46</sup> The new framework will aim to harmonise the existing thresholds for functionally equivalent powers. The Government will consider new thresholds primarily targeting the person who is the subject of an investigation. However, the new framework should also allow agencies to use powers against objects, third parties and groups where appropriate by satisfying additional thresholds.

In line with the Comprehensive Review's recommendations, the Government will consider expanding the scope of agency powers to access, use and retain information for the purpose of developing, testing, maintaining and evaluating electronic surveillance and cyber capabilities and technologies.<sup>47</sup>

---

45 Exceptions for these offence thresholds exist for specific offences – for example, offences that may be challenging to investigate without the use of electronic surveillance powers, such as cyber-enabled criminal activity and cybercrime.

46 The Comprehensive Review, Volume 2, paragraph [28.54].

47 The Comprehensive Review, Volume 2, recommendations 106–108.

## ASIO

The Government will consider introducing consistent thresholds for the use of ASIO's powers to intercept telecommunications, access stored communications, access computers and use optical and listening devices. This would allow the Attorney-General to issue a warrant for access to private communications, data and surveillance information if satisfied that:

- a person is engaged in, or is reasonably suspected of being engaged in or of being likely to engage in, activities relevant to security, and
- the exercise of powers under the warrant in respect of the person is likely to substantially assist ASIO in obtaining intelligence in respect of a matter that is important in relation to security.

The proposed new threshold would ensure that ASIO's electronic surveillance warrants are 'person-based', by requiring ASIO to satisfy the Attorney-General that there are reasonable grounds to suspect that the person is engaged in, or is likely to engage in, activities relevant to security, such as ideologically motivated violence or espionage. The threshold would also require ASIO to satisfy the higher threshold (which presently applies to computer access warrants), that the exercise of powers would 'substantially assist' in obtaining intelligence in relation to a matter that is important in relation to security.

## Law enforcement

Equally, the Government will consider streamlining the thresholds that apply to law enforcement agencies' use of these powers, to allow an issuing authority to authorise access to private communications and surveillance information if satisfied that:

- a person has committed, or is reasonably suspected of committing or of being likely to commit, an offence that is punishable by a maximum penalty of at least 5 years' imprisonment, or additional offences as outlined below, and
- the exercise of powers under the warrant in respect of the person is likely to substantially assist the agency in the investigation of the offence.<sup>48</sup>

As recommended by the Comprehensive Review, the Government will consider additional categories of offences that may not meet the recommended 5 year offence threshold but cannot be effectively investigated without covert access to communications content<sup>49</sup> – for example, cybercrimes such as hacking or infecting a computer with ransomware, spyware, worms, Trojans or viruses. It is likely any exceptions will be specified in the new Act, and these exceptions will generally be limited to offences with a threshold of at least 3 years' imprisonment.

---

48 The Comprehensive Review considered the 5 year threshold struck the right balance between ensuring that electronic surveillance powers were available to investigate serious offences, and only using these intrusive powers where proportionate to the law enforcement objective to be achieved (The Comprehensive Review, Volume 2, paragraph [28.103]).

49 The Comprehensive Review, Volume 2, recommendation 89.

It may also be necessary to allow the use of electronic surveillance powers for a small number of offences that carry a maximum penalty of less than 3 years. This will likely only be permitted where the nature of the offence means there is no practical way of collecting information without using electronic surveillance powers. These are generally cybercrime or cyber-enabled offences, such as:

- section 478.1 of the Criminal Code – unauthorised access to, or modification of, restricted data (maximum penalty of 2 years’ imprisonment)
- section 478.2 of the Criminal Code – unauthorised impairment of data held on a computer disk etc. (maximum penalty of 2 years’ imprisonment).

These thresholds are meant to strike an appropriate balance between ensuring agencies can access information to investigate serious offences or collect important intelligence, and limiting the use of intrusive powers to times when it is necessary and proportionate to the gravity of the matter under investigation.

In addition, and in line with the Comprehensive Review, the new framework may retain a separate threshold for tracking information for law enforcement<sup>50</sup> – that is, information about a person’s movements that may reveal a pattern of life or associations but lacks the more detailed information that may be obtained from other surveillance methods (i.e. video or audio surveillance). This may include telecommunications metadata used to track the movements of a telecommunications service. This is outlined further below under the heading Access to information about a person’s location or movements. This would not preclude tracking information from being obtained under a broader warrant for surveillance information.

The Government will also consider whether there should be a separate threshold for ASIO’s access to tracking information.

## Question

17. Is it appropriate to harmonise legislative thresholds (as outlined above) for covert access to private communications, content data and surveillance information where existing warrants are functionally equivalent?

---

50 The Comprehensive Review, Volume 2, recommendation 92.

# Access to information about communications

## Current State

Limited access to types of information about communications (for example, the time at which a phone call was made, the duration of the phone call and the participants in the call) is generally internally authorised under Chapter 4 of the TIA Act. Service providers must retain this information under Part 5-1A of the TIA Act. A range of agencies may also access information about communications outside the TIA Act under sections 280 and 313(3) of the Telecommunications Act.

Thresholds for access to information about communications must ensure access is proportionate to the gravity of the matter under investigation and only impacts upon the privacy of individuals where necessary for law enforcement and security purposes. However, the thresholds associated with access to information about communications should also reflect the relative intrusiveness of this information compared to other investigative powers.

Currently, Part 4-1 of the TIA Act allows officers from 20 listed law enforcement agencies to authorise the disclosure of telecommunications data if a number of grounds are met, including that access is necessary, justifiable and proportionate. An authorised officer is the head or deputy head of the agency, or a person acting in one of those positions, or who holds or is acting in a management office or management position and is relevantly authorised under the TIA Act.

The current framework distinguishes between existing (information that came into existence before the authorisation is received) and prospective (information that comes into existence during a specified period for which the authorisation is in force) telecommunications data. In order to access existing data, authorising officers must be satisfied that the disclosure is reasonably necessary for enforcing the criminal law.<sup>51</sup> In order to access prospective telecommunications data, they must also be satisfied that the disclosure is reasonably necessary for the investigation of an offence punishable by at least 3 years' imprisonment.<sup>52</sup>

In the case of ASIO, access to existing or prospective telecommunications data may be internally authorised where it is in connection with the performance of ASIO's functions.<sup>53</sup> However, access to prospective data may only be authorised by a senior officer (at the SES Band 2 level or above).

---

51 TIA Act, section 178.

52 TIA Act, section 180.

53 TIA Act, sections 175 and 176.

A warrant is required, and additional protections apply, if the agency is seeking to access a journalist's telecommunications data for the purpose of identifying the journalist's source.<sup>54</sup> In issuing such a warrant, the issuing authority must be satisfied that:

- the public interest in the issuing of the warrant outweighs the public interest in protecting the confidentiality of the identity of the source
- in the case of a law enforcement agency – the warrant is reasonably necessary for a particular purpose, such as enforcement of the criminal law, and
- in the case of ASIO – that ASIO's functions would extend to obtaining telecommunications data for the purpose of identifying the source, for example because doing so would be relevant to the protection of Australia or Australians from espionage, foreign interference or politically motivated violence.

When an agency seeks a warrant to access a journalist's telecommunications data for the purpose of identifying the journalist's source, a Public Interest Advocate can make a submission to the issuing authority. This submission can deal with a range of matters, including whether the public interest in issuing the warrant outweighs the public interest in protecting the identity of the source.<sup>55</sup>

## Potential Future State

The new framework will implement the Government's response to the PJCIS review of the mandatory data retention regime. In implementing this response, the Government will consider whether the existing thresholds and authorisation requirements for law enforcement agencies and ASIO to access telecommunications data remain appropriate. The government will also consider requiring these agencies to satisfy a proportionality test before access to telecommunications data is authorised.

The new framework will retain the current data retention period of 2 years.<sup>56</sup> Consideration will also be given to the entities that will be required to retain this data as discussed in **Part 2** of this paper. In developing the new framework, the Government will also consider the national guidelines being developed to support access to telecommunications data, and additional reporting and record-keeping requirements to bolster transparency (discussed in **Part 5**). In addition, the Government will carefully consider legislative and regulatory measures to address concerns surrounding the safeguards, oversight and record-keeping requirements associated with access to telecommunications data outside of the mandatory data retention scheme.

---

54 TIA Act, Division 4C of Part 4-1.

55 TIA Act, sections 180L and 180X.

56 TIA Act, Division 1 of Part 5-1A.

Consistent with the Government's response to the PJCIS inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press, the Government will consider how to strengthen the safeguards that apply when agencies seek telecommunications data in relation to a journalist in the new framework. This may include expanding the existing role of Public Interest Advocates and strengthening reporting and record-keeping requirements.

## Question

18. Are there any other changes that should be made to the framework for accessing this type of data?

# Access to information about a person's location or movements

## Current State

A tracking device provides information about a person's movements that may reveal a person's pattern of life or associations. It can also be used to provide information about the movement or status of specific objects, such as vehicles or cargo. In this paper, this is referred to as tracking information. At a federal level, tracking devices are regulated under the ASIO Act for ASIO and the SD Act for law enforcement agencies. Some states and territories also legislate for the use of tracking devices.

Deployable geolocation tracking devices do not provide access to the content of communications. Despite this, the use of such devices is subject to the same framework that applies to more intrusive surveillance via optical devices, listening devices and data surveillance devices (all of which can be used to access the content of a person's conversations).

## Potential Future State

As noted by the Comprehensive Review,<sup>57</sup> tracking information may have less impact on privacy than other surveillance information, particularly where that information is devoid of the greater substance and context derived from access to a person's communications. Optical or listening devices may be used to observe a person's activities or conversations inside their home, or in other circumstances where a person may have a reasonable expectation of privacy. In contrast, a person's movements are typically observable to others and less private in nature.

---

<sup>57</sup> The Comprehensive Review, Volume 2, page 317.



In line with the Comprehensive Review, the Government will consider regulating access to tracking information separately from other surveillance information.<sup>58</sup> At present, law enforcement agencies may use a tracking device in relation to an offence punishable by a maximum penalty of 3 years' imprisonment. This threshold could be retained in the new framework in relation to tracking information. Importantly, if access to tracking information were regulated separately, agencies would not be prevented from seeking authorisation for access to tracking information under a warrant that also authorises access to other surveillance information.

The Government will consider whether it is necessary to make any changes to enable ASIO to access tracking information separately from other surveillance information.

Other minor changes will be considered in relation to the threshold and purpose for which law enforcement agencies and ASIO access tracking information, including:

- more consistent and rigorous controls on access to tracking information, including changes to require the powers to be exercised against a person in the first instance
- limited exceptions to allow agencies to obtain tracking information in relation to an object or premises where necessary.<sup>59</sup>

Agencies still need the ability to internally authorise the use of certain tracking devices where using the device does not involve entry onto premises without permission, or interference with the interior of a vehicle without permission of the owner. The Government will consider how this can be retained in the new framework.

## Question

19. What are your views on the proposed thresholds in relation to access to information about a person's location or movements?

---

58 The Comprehensive Review, Volume 2, recommendation 92.

59 The Comprehensive Review, Volume 2, recommendations 81 and 93–95.

# Warrants should be directed at a specific target or person in the first instance

## Current State

In general, agencies can currently only use electronic surveillance powers where those powers target a particular person who is under investigation. However, this is not always the case. Some warrants can be used to identify a person or target whose identity is unknown but who is suspected of being involved in criminal activity or activities relevant to security. For example, under the SD Act, a surveillance device warrant can be issued in relation to an object or premises. Such warrants are often used by law enforcement to identify an unknown criminal.

Under the ASIO Act and the SD Act, computer access warrants target computers rather than persons. This reflects the origin of the computer access warrant framework, which was a response to challenges faced in executing traditional search warrants over information stored on computers or networks. These warrants let agencies 'search' particular computers or networks for information or data relevant to their investigations. The computer-based approach can also assist agencies when they can identify a computer or device used to disseminate child sexual abuse material or ransomware, or engage in matters relevant to security, but cannot determine who is using the computer.

While warrants that do not target an identified person are critical tools for investigations, they may impact upon the privacy of people not directly engaged in criminal or security-relevant activities. For example, under a computer access warrant agencies could access the data of other individuals who use the targeted computer.

## Potential Future State

Due to their intrusive nature, the Comprehensive Review recommended electronic surveillance powers be directed, in the first instance, at the person who is the subject of the investigation. In other words, where possible these powers should be 'person-based'.<sup>60</sup> In line with this, the Government will consider requiring agencies to demonstrate a reasonable nexus between electronic surveillance activities and the person under investigation. This could be achieved by ensuring that legislative thresholds for the use of electronic surveillance powers target a person in the first instance.

---

60 The Comprehensive Review, Volume 2, recommendation 81.

However, this is not always possible.<sup>61</sup> The Government will therefore consider providing limited exceptions to a person-based warrant in relation to third parties, groups, unidentified persons and foreign intelligence. As person-based, third party and group warrants may not be sufficient to address all cases, an object or premises-based warrant may also be retained.

The Government will further consider how the new framework could best integrate the ability of law enforcement to obtain warrants to collect intelligence, disrupt offending and collect evidence. In this regard, the Government intends to incorporate the existing powers introduced by the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (SLAID Act) to allow the Australian Federal Police (AFP) and the ACIC to obtain intelligence in relation to criminal networks and for the purposes of disrupting or preventing offending.

## Question

20. What are your views on the proposed framework requiring warrants and authorisations to target a person in the first instance (with exceptions for objects and premises where required)?

# What about third parties?

## Current State

The TIA Act, SD Act and ASIO Act currently allow agencies to obtain information and data in relation to third parties. This means that intrusive powers may be used in relation to persons who are not themselves the target of an investigation. In some cases, people who are the subject of law enforcement and security investigations go to considerable lengths, and have considerable expertise, in concealing their communications. This is particularly the case where agencies are investigating sophisticated groups and individuals, such as organised crime syndicates, foreign spies and their agents, and some violent extremist groups. In these cases, collecting information from a third party who is known to be in contact with the person under investigation may be the only way for an agency to determine how the subject is communicating and to obtain evidence of a serious crime or intelligence about a security threat. For example, where an agency cannot identify the telecommunications service of a person of interest, it may intercept the communications of a known third party who is communicating with the target.

---

<sup>61</sup> See for example The Comprehensive Review, Volume 2, paragraphs [28.30] and [28.42].

The Comprehensive Review noted that existing third party provisions are not sufficiently confined or consistent. For example, under the current framework, law enforcement agencies may obtain a warrant to use a surveillance device in relation to a third party without satisfying any additional threshold. In contrast, ASIO cannot obtain a surveillance device against a third party at all (with the exception of certain tracking devices). To intercept third party communications, both law enforcement agencies and ASIO must satisfy additional thresholds by demonstrating either that all other practicable methods of identifying the communications service used by the subject have been exhausted, or that intercepting communications under an ordinary warrant would not otherwise be possible. In contrast, they may obtain a warrant to covertly access a computer in relation to a third party to obtain the same information without satisfying any additional test.

## Potential Future State

In line with the Comprehensive Review,<sup>62</sup> the Government will consider standardising the thresholds and purposes for which third party powers can be used by both law enforcement agencies and ASIO. In practice, this may amount to two substantive changes.

First, the new framework could provide both law enforcement agencies and ASIO with the ability to obtain third party warrants to access information traditionally obtained through the surveillance devices, interception and computer access powers (i.e. private communications and data, and surveillance information).

Second, under the new framework agencies may be required to satisfy an additional threshold to obtain a third party warrant. For example, they may need to satisfy the issuing authority that, in addition to the test for an ordinary warrant, obtaining information directly under a warrant would be impractical or ineffective. This would not mean agencies must have actually tried all other methods before getting a third party warrant. Instead, the agency would need to demonstrate these other methods would be impractical or ineffective.

For example, the agency may not be able to identify the services used by the target, or may have information the target does not use identified services (e.g. their home phone or internet) for criminal or security-relevant purposes. This additional threshold currently applies to some, but not all, third party warrants. Consistent application across all third party warrants in the new framework would ensure agencies must satisfy a higher threshold in every case. The threshold for third parties warrants in the new framework will aim to balance privacy concerns with the need for agencies to have appropriate powers to investigate criminal or security-relevant conduct.

---

62 The Comprehensive Review, Volume 2, recommendation 82.

## Question

21. Is the proposed additional warrant threshold for third parties appropriate?

## What about groups?

### Current State

Due to the anonymous and borderless nature of the internet, it is becoming increasingly difficult, if not impossible, for agencies to connect online activities to specific individuals. Sophisticated cyber actors often operate in groups to undertake their activities, such as hacking and ransomware groups, and child sexual abuse rings, with different group members responsible for different parts of their operations—including offline activities such as procuring servers and infrastructure, as well as online activities such as hacking, sharing abuse material, and marketing. Agencies can identify and begin investigating these groups' collective activities. However agencies presently face significant challenges when it comes time to apply for warrants—because of the requirement to be able to attribute specific actions to a specific person, when applying for existing person-based warrants. For example, where sophisticated cyber actors operate in groups dispersed all over the globe to undertake their activities, or where child sexual abuse rings use dark web forums to disseminate and share material.

Under the current framework, there are some limited instances in which law enforcement agencies and ASIO can obtain warrants targeting groups. For example, law enforcement agencies can obtain a surveillance device or computer access warrant to target a group. However, interception warrants can only be issued in relation to an individual. Similarly, ASIO can obtain computer access warrants to access computers used by a group. ASIO can also obtain interception warrants in relation to services that are being used for purposes prejudicial to security—which can allow ASIO to target groups in limited circumstances. However, unlike law enforcement agencies, ASIO's surveillance device warrants can only be issued in relation to an individual.

## Potential Future State

In line with the Comprehensive Review,<sup>63</sup> the Government will consider introducing dedicated group warrant regimes for both law enforcement agencies and ASIO, which will apply consistently across all warrant types. Group warrants would only be available where the issuing authority is satisfied a warrant in relation to individual members of the group would be impractical or ineffective.<sup>64</sup> Higher thresholds for group warrants would ensure proportionality is considered in applying for, and issuing, these potentially more intrusive warrants.

This does not mean an agency could obtain a group warrant simply because it would be more efficient. Nor does it mean a group warrant could only be issued where it would be impossible to obtain a warrant in relation to individuals. Instead, the intention is to ensure that a group warrant would not be available where the identities of all group members are known and could be specified in person-based warrants.<sup>65</sup>

The group should be identified by reference to members' shared characteristics and group activities that justify the use of the surveillance warrant. Where an agency requires a service provider's assistance to execute the warrant (such as to intercept communications), the agency will be required to identify the services, devices or communications that should be accessed, so that providers are able to action the request. An agency may be able to obtain a group warrant in relation to users of an encrypted messaging platform similar to the ANOM app, where all users of the platform use it for criminal purposes but the anonymising nature of the platform makes it impossible to identify individual users.

The new framework will include the powers introduced by the SLAID Act for the AFP and ACIC to combat serious crime online. This includes the ability to use computer access against online criminal networks for the purposes of obtaining intelligence, and to disrupt or frustrate criminal offending facilitated by a computer. The reform will consider the extent to which it is necessary to retain separate warrants for these powers and how the thresholds for these powers may be streamlined to be consistent with the new group warrant framework.

### Question

22. Is the proposed additional threshold for group warrants appropriate?

63 The Comprehensive Review, Volume 2, recommendation 83.

64 The Comprehensive Review, Volume 2, recommendation 82.

65 The Comprehensive Review, Volume 2, paragraph [28.39].

# Powers should only be authorised where necessary and proportionate

Given the intrusive nature of electronic surveillance, the use of these powers should only be authorised if it is necessary and proportionate. Importantly, this does not mean electronic surveillance will only be available where unavoidable. Instead, the requirement that the use of powers be necessary and proportionate would mean the exercise of these powers must be aimed at a legitimate and lawful objective and the intrusion on rights and privacy must not outweigh the benefits of that objective.

## Current State

The TIA Act and the SD Act have different tests for issuing a warrant, but the principles of necessity and proportionality are reflected in the existing warrant thresholds for electronic surveillance. For example, both the TIA Act and SD Act require that issuing authorities must consider matters such as the impact on privacy, the gravity of the threat of offence and the availability of other investigative methods. These factors require the agency and the issuing authority consider whether the use of these powers is necessary and proportionate in the circumstances.

Similarly, the Minister for Home Affairs has issued Guidelines under the ASIO Act that require ASIO to ensure that any means it uses to obtain information is proportionate to the gravity of the threat posed and the likelihood of its occurrence, to undertake its inquiries and investigations with as little intrusion into privacy as is reasonably required, and where possible to use the least intrusive techniques for collecting information before using more intrusive techniques.

However, the current legislation does not include a clear requirement that powers only be used where necessary and proportionate. The Comprehensive Review noted that the new framework should introduce a more consistent and explicit necessity and proportionality test.<sup>66</sup>

---

66 The Comprehensive Review, Volume 2, recommendation 80.

## Potential Future State

The Government will consider how best to incorporate a clear, express requirement in the new framework to ensure electronic surveillance powers are only used where necessary and proportionate. Agencies may be required to satisfy an issuing authority that the use of a particular power would be necessary and proportionate to particular matters, which may be specified in the legislation, such as:

- the gravity of the matter under investigation – is the crime or security matter, and the resulting likely harm, serious enough to justify the use of the power?
- the intrusion on privacy – how much will the use of the power intrude on the privacy of the target or any other person?
- the likelihood the surveillance will achieve the warrant objective – will the use of the power actually provide the information that the agency is seeking?
- the likely relevance and usefulness of the information – is the information likely to further the agency’s investigation, including preventing further criminal activity or threats to security?
- whether there are less intrusive means of achieving the purpose of the warrant – could the agency use some other less intrusive power to obtain the information it is seeking?
- what other intrusive powers have been, or are being, used in relation to the target?

### Question

23. What are your views on the above proposed approach? Are there any other matters that should be considered by an issuing authority when considering necessity and proportionality?



# Who should authorise the use of these powers?

## Current State

At present, law enforcement agencies must apply to an independent issuing authority to authorise the use of electronic surveillance.<sup>67</sup> Broadly, under the existing framework warrants for electronic surveillance are issued by eligible judges and nominated Administrative Appeals Tribunal (AAT) members. The Attorney-General issues ASIO warrants.

There are some inconsistencies in the framework around which judges and AAT members may issue particular warrants under the TIA Act and the SD Act. For example, certain warrants can only be issued by nominated federal judges and certain senior AAT members. However, stored communication warrants under the TIA Act can be issued by state and territory magistrates.<sup>68</sup> Further, the AAT members who can issue SD Act warrants and interception warrants are different from those who can issue stored communications warrants. Similarly, the TIA Act provides that magistrates can issue stored communications warrants but not interception warrants.

## Potential Future State

The Comprehensive Review did not make specific recommendations about who should issue law enforcement warrants. The new framework will continue to require that law enforcement warrants be authorised by an appropriate independent authority. The Government will consider the appropriate issuing authority for each power. In doing this, the Government will consider matters such as the role of AAT members and whether some law enforcement powers should only be authorised by judges of a particular seniority.<sup>69</sup>

---

67 This section deals with the authorities responsible for issuing warrants. The paper deals separately with circumstances in which powers can be exercised without a warrant. For example, the circumstances in which tracking devices can be used without a warrant are considered above in relation to access to information about a person's location or movements.

68 Following the renaming of the Federal Magistrates Court as the Federal Circuit Court and the reclassification of federal magistrates as judges in 2013, there are no federal magistrates. This means the reference to magistrates in the TIA Act only refers to magistrates in state and territory courts.

69 For example, recommendation 9 of the PJCIS Advisory report on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 recommended that some powers in that Bill should only be authorised by a Federal Court judge or a state or territory Supreme Court judge.

In line with the Comprehensive Review's recommendations, the Attorney-General will continue to authorise ASIO's activities under the new framework.<sup>70</sup> Further, the Comprehensive Review recommended ASIO warrants should not be subject to additional judicial or other independent authorisation<sup>71</sup> (with the exception of ASIO's international production orders, as discussed below).

The new framework will retain separate authorisation requirements to allow Australian law enforcement agencies and ASIO to obtain orders for electronic data held by US carriage service providers (international production orders). This is necessary due to the requirements of the US CLOUD Act, which underpins the proposed agreement between Australia and the US to enable the issuing of these orders. To meet the requirements of this agreement, Australian legislation must meet certain criteria, including that orders must be authorised by persons characterised as a court, judge, magistrate, or other independent authority.

The new framework will ensure that only appropriately senior independent officers can issue warrants for access to journalists' and media organisations' data. This is consistent with the Government's response to the PJCIS inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press.<sup>72</sup> In addition, the Government will consider an expanded role for Public Interest Advocates, extending beyond warrants for journalists' telecommunications data. This role would apply to warrants in relation to the investigation of an unauthorised disclosure of government information or a Commonwealth secrecy offence where the warrant relates to a person working in a professional capacity as a journalist or a media organisation.<sup>73</sup>

## Question

24. Should magistrates, judges and/or AAT members continue to issue warrants for law enforcement agencies seeking access to this information?

---

70 The Comprehensive Review, Volume 2, paragraphs [18.126]–[18.128].

71 The Comprehensive Review, Volume 2, recommendation 30.

72 PJCIS, Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press (Press Freedoms inquiry), Commonwealth of Australia, Canberra, 2020, recommendation 2.

73 Press Freedoms inquiry, recommendation 2.

# Information must be appropriately protected and only shared with the appropriate authorities

The ability to use and share electronically accessed information must be strictly controlled. The new framework will prohibit the improper use and dissemination of information obtained, accessed or received under the framework. There will be exceptions to this prohibition for using and disclosing information for particular purposes in line with an agency's functions.

## Current State

Provisions in the TIA Act and SD Act criminalise the unauthorised disclosure of information and provide protection against its unauthorised use and disclosure. Both Acts contain provisions setting out when use and sharing of this information is permitted. These provisions are prescriptive, complicated and somewhat inconsistent.

The Comprehensive Review noted that the TIA Act contains more than 54 provisions relating to use, disclosure and other dealings with information obtained under the Act. The purposes for which information can be used and disclosed differ based on agency, type of information and the means by which the information was obtained.<sup>74</sup> In comparison, the use and disclosure provisions in the SD Act are simpler, as they apply to a defined category of 'protected information'.<sup>75</sup>

Some of these provisions prevent the effective use and disclosure of this information. For example, some parts of the TIA Act provide that information can only be shared with a small number of agencies, meaning agencies may not be able to pass information to an authority that can use it to prevent criminal activity or address national security threats.<sup>76</sup> Further, the Comprehensive Review noted that due to the phrasing of some provisions under the TIA Act, it is not clear whether agencies may disclose lawfully intercepted information to other law enforcement agencies in certain circumstances. For example, there is uncertainty around whether agencies may share information where the information indicates a person is likely to commit a relevant offence, or whether this information may only be disclosed once a person has already committed the offence.<sup>77</sup>

---

74 TIA Act, sections 63–76A, 89, 92A, 133(2)–146, 180C–180F, 181–182B, 186F and 299.

75 SD Act, sections 44–48 and 65B.

76 TIA Act, Parts 2-6 and 3-4.

77 TIA Act, subsection 68(b).

## Case study

An example of limitations in current information sharing provisions can be seen through the operation of section 45 of the SD Act. The execution of surveillance device warrants and computer access warrants by the AFP has previously uncovered evidence of state-based offences. However, section 45 of the SD Act prevents the AFP from sharing this information with state law enforcement partners unless the information relates to a Commonwealth offence or a state offence with a federal aspect.

Evidence uncovered by the AFP has included information about historical murders, information where a person ‘boasted’ about having seriously assaulted their partner and multiple instances of communication about historical serious assaults. These are all state-based offences that lack a federal aspect. As such, the AFP has been unable to share this information with state law enforcement partners, by operation of section 45 of the SD Act.

As well as limiting the use and disclosure of information, the TIA Act, SD Act and ASIO Act also require agencies to destroy this information where it is no longer likely to be relevant to the permitted purposes for which it could be used. In addition, Ministerial Guidelines issued under the ASIO Act require ASIO to take reasonable steps to dispose of personal information in certain circumstances. The Comprehensive Review noted that the destruction provisions in these Acts are complex, prescriptive and inconsistent. There are also inconsistencies in the information that must be destroyed and the reporting required following destruction. For example, law enforcement agencies are required to destroy originals and copies of information obtained under stored communications warrants but are not required to destroy copies of intercepted information.<sup>78</sup> In contrast, ASIO is required to destroy records and copies of intercepted information.<sup>79</sup> The timing of destruction is also inconsistent between the TIA Act and the SD Act.<sup>80</sup>

## Potential Future State

In line with the Comprehensive Review, the Government will consider how to implement simple, principles-based rules limiting how information can be used and shared.<sup>81</sup> This will allow disclosure of information to the authority best able to use it and include limitations on use and sharing based on the purpose and nature of the information.

---

78 See TIA Act, sections 5 (definition of restricted record), 79 and 150.

79 TIA Act, section 14.

80 See The Comprehensive Review, Volume 2, paragraphs [30.148]–[30.151].

81 The Comprehensive Review, Volume 2, recommendation 120.

The framework will contain clear offences for unauthorised disclosures. The Government will consider how to retain and consolidate the effect of existing secrecy offences in the TIA and SD Act in the new legislation, retaining the distinction between ‘entrusted persons’ and ‘outsiders’. However, this approach would not limit the persons or authorities with whom information can be shared, as long as the disclosure is for a permitted purpose. As recommended by the Comprehensive Review, the permitted purposes may be tiered, with a primary permitted purpose for use or disclosure, a defined range of secondary purposes and a defined range of miscellaneous purposes.<sup>82</sup>

A primary permitted purpose would allow agencies to use and disclose information to other agencies for the same reason they collected it. Permitted secondary purposes would allow information to be used and disclosed for sufficiently serious matters, such as, but not necessarily limited to, the investigation or prosecution of a serious criminal offence, the performance of ASIO’s functions and the prevention of a serious risk to life, health, safety or substantial damage to property. It will also be necessary for information to be used and disclosed for oversight purposes by the Inspector-General of Intelligence and Security (IGIS) and the Commonwealth Ombudsman.<sup>83</sup>

Destruction provisions will also be considered to balance agencies’ operational needs and continued performance of their functions, appropriate oversight and the privacy of individuals. These provisions will need to take into account obligations on agencies to retain certain information under other legislation, including the *Archives Act 1983*.

## Questions

25. What are your thoughts on the proposed principles-based, tiered approach to use and disclosure?
26. When should agencies be required to destroy information obtained under a warrant?

## Warrant requirements should only be relaxed in time-sensitive situations

The requirement for agencies to obtain written, independently authorised warrants is an important check on use of intrusive powers. However, in an emergency law enforcement agencies and ASIO may need to act urgently to collect information critical to an investigation or in order to prevent serious harm. In these circumstances, there may not be time for an agency to go through the usual processes for getting a warrant.

82 The Comprehensive Review, Volume 2, recommendations 121–123.

83 For a list of secondary and miscellaneous purposes, see The Comprehensive Review, Volume 2, pages 403–412.

## Current State

Emergency authorisation processes allow agencies to use powers more rapidly, in rare circumstances where time is of the utmost essence. Part of law enforcement agencies' and ASIO's work is to respond to immediate and critical threats, such as terrorist attacks. In these situations, the immediate use of electronic surveillance powers can be necessary to allow agencies to understand and respond to the threat. For example, the time needed to obtain a warrant through the ordinary process, involving a written application to an issuing authority, who in turn issues the warrant in writing, may delay agencies' ability to prevent a serious risk to life. It is important that agencies are able to obtain permission to use these powers more rapidly in such cases, to respond to and prevent imminent threats.

There may be other urgent or time-critical circumstances where the time taken to apply for and obtain a warrant in writing from an external authority would seriously jeopardise an investigation into criminal activities or national security threats. The types of evidence and intelligence that can be obtained under electronic surveillance powers are often transient—in the sense that there is no second opportunity if an agency misses the opportunity to record a critical meeting, or to intercept a critical conversation. The ability for agencies to obtain permission to exercise powers more rapidly in such cases can ensure that critical evidence or intelligence will not be lost.

These are exceptional circumstances. In the vast majority of cases, agencies apply for and obtain warrants in the usual manner. However, it is important that the legal framework provides agencies with the flexibility to act in time-critical cases.

There are a number of different provisions in the current framework enabling law enforcement agencies and ASIO to obtain warrants and authorisations in time-sensitive or emergency situations. These provisions are not consistent and vary between activities and agencies. For example, some emergency authorisation provisions allow agencies to seek a warrant orally (in person or over the phone) where there is not enough time to compile a written application and obtain a written warrant. Other emergency authorisation provisions allow agencies to use such powers under internal authorisation from a senior agency official.

## Case study

ASIO's emergency authorisation provisions in the TIA Act, and in relation to its computer access and surveillance devices powers in the ASIO Act, in particular, are poorly-adapted for use in emergencies and time sensitive cases. ASIO is required to have already prepared and forwarded a written request to the Attorney-General for a warrant, before the Director-General's power to issue an emergency warrant is enlivened. As the Comprehensive Review noted, while this has not prevented ASIO from obtaining warrants in urgent situations, aspects of the framework cause delay without any oversight or accountability benefit. For example, the requirement for ASIO to prepare and forward a complete, written request for a warrant to the Attorney-General's Office in an emergency, when it knows that the Attorney-General is not there and is not able to review the request, does not enhance the Attorney-General's control over the process or improve oversight.

Agencies only use these powers in rare circumstances. For example, law enforcement agencies only made one emergency authorisation under the SD Act between 2015 and 2020.<sup>84</sup> Similarly, only around one per cent of applications for telecommunications interception warrants were made orally in this period.<sup>85</sup>

## Potential Future State

The Government will consider how to implement a revised and consolidated emergency authorisation framework. Consistent with the Comprehensive Review,<sup>86</sup> this would contain a tiered authorisation framework for issuing warrants in emergency and time-sensitive circumstances, accompanied by stringent record-keeping, notification and reporting obligations. This includes a requirement to obtain a written warrant or authorisation after the fact.

Warrants would still need to be issued in writing wherever possible. Where this is not possible, a separate tiered authorisation framework would allow law enforcement agencies and ASIO to use powers without a written warrant. For example, where it is not possible for ASIO to obtain a warrant in writing from the Attorney-General, the new framework could enable the Attorney-General to issue the warrant orally where the Director-General of ASIO believes on reasonable grounds that a delay in obtaining authorisation would defeat the purpose of obtaining the authorisation.

---

84 See SD Act Annual Reports for 2015–16 through 2019–20.

85 See TIA Act Annual Reports for 2015–16 through 2019–20.

86 The Comprehensive Review, Volume 2, recommendation 97.

Where the Attorney-General is unavailable, or where making an oral application would pose an unacceptable risk to operational security, the new framework could allow the Director-General to authorise a warrant, with appropriate safeguards including subsequent written approval from the Attorney-General.

A similar tiered approach may be taken for law enforcement agencies. The new Act would require law enforcement warrants to be issued in writing wherever possible. In limited circumstances, where a delay would defeat the purpose of obtaining the warrant, an issuing authority (usually a judge) may authorise a warrant orally. In extremely limited circumstances, a law enforcement officer may be able to provide internal authorisation to:

- prevent or lessen imminent threats to life, or of serious harm or serious damage to property
- locate and investigate suspected kidnappings
- locate missing persons
- recover a child subject to a child recovery order.

Reporting and oversight requirements for the use of powers under the new framework are discussed further in **Part 5**.

Whether a situation is time-critical or an emergency will vary according to the nature of the investigation. As such, the Government does not propose to exhaustively define what amounts to an emergency. Attempting to provide an exhaustive definition may unintentionally narrow the scope in which the emergency authorisation framework may be used and have negative consequences. Instead, the tiered framework would focus on whether the purpose of the warrant would be defeated by the delay involved in obtaining written authorisation. Internal authorisation of law enforcement powers would only be permitted where the circumstances are so urgent as to require the immediate use of the power, and where it is not practicable to apply for a warrant.

More generally, the framework will take a technology-neutral approach to the way in which agencies can make applications. While the framework will require applications and warrants to be in writing where possible, this does not mean applications must be made in person with hardcopy documents. Instead, the framework will allow applications to be made, and warrants to be issued, by any appropriate method. This could include a physical meeting with hardcopy documents, or a video conference with digital documents sent by email. The appropriate method in a given case will be a matter of discretion between the agency and the issuing authority.

## Question

27. What are your thoughts on the proposed approach to emergency authorisations?



# PART 5: SAFEGUARDS AND OVERSIGHT

---



# The use of intrusive powers will be strictly limited

While it is important that agencies have electronic surveillance powers to perform their functions, there must be strict limitations on when and how they use those powers. These safeguards come in different forms and should be present at all stages of the process. Safeguards are usually designed to balance the scope, privacy intrusion and breadth of a particular warrant.

## Current State

There are a range of existing legislative safeguards. Broadly, these include:

- requirements to obtain a warrant or authorisation with appropriately strict thresholds
- conditions placed on the activities authorised under a warrant
- independent issuing authorities
- independent advocates providing submissions concerning warrant applications in some circumstances
- limitations on how agencies can use and disclose information
- requirements to destroy information.

While these safeguards all serve important functions, they apply inconsistently to the various electronic surveillance powers. Further details about the inconsistencies with current safeguards have been discussed throughout **Part 3** and **Part 4**.

## Potential Future State

All of these important safeguards will be retained in the new framework. To the extent possible, safeguards will be strengthened and consolidated to enhance consistency and transparency. For example, consideration will be given to:

- harmonising warrant thresholds
- maintaining and strengthening existing safeguards to protect journalists' sources where appropriate, including broadening the role of independent Public Interest Advocates in relation to warrants concerning journalists in line with the PJCIS recommendations from its press freedoms inquiry
- the need for any additional safeguards for other professions (such as lawyers or medical practitioners)
- consolidating and simplifying the provisions that govern how agencies use and disclose information
- updating requirements to destroy information to ensure these reflect modern-day data storage and transfer technologies.

Further details about the approach to revising these safeguards are set out in **Part 3** and **Part 4**.

## Questions

28. Are there any additional safeguards that should be considered in the new framework?
29. Is there a need for statutory protections for legally privileged information (and possible other sensitive information, such as health information)?

## Ensuring powers are exercised in line with the law

Robust independent oversight is necessary to ensure agencies use electronic surveillance powers lawfully and with propriety. The IGIS and the Commonwealth Ombudsman will continue to oversee the use of electronic surveillance by ASIO (and other intelligence agencies) and law enforcement agencies respectively. Ensuring these bodies have the right scope of oversight and sufficient powers to perform these functions is critical for developing public confidence in the new framework. The INSLM also plays a critical role in conducting reviews of electronic surveillance-related legislation to ensure it contains appropriate protections for individual rights, remains proportionate to national security threats and is necessary.

These independent oversight arrangements are complemented by robust parliamentary oversight arrangements, particularly the PJCIS and the PJCLE. It is expected the INSLM and parliamentary committees will continue to play an important role in the oversight of the new framework.

## Current State

The IGIS oversees the activities of ASIO and other intelligence agencies<sup>87</sup> for legality, propriety and compliance with human rights. The IGIS also oversees the activities of the ACIC and the AFP as they relate to those agencies' use of network activity warrants. The IGIS does this through inspections, inquiries and investigations into complaints. Should the IGIS choose to conduct an inquiry into the actions of ASIO or another intelligence agency, the IGIS has significant, wide-ranging powers to compel the giving of evidence under oath or affirmation, to require the production of documents and to access premises. These powers are primarily set out in the *Inspector-General of Intelligence and Security Act 1986*. The Comprehensive Review was supportive of the IGIS' broad scope of oversight and range of powers.

Oversight of law enforcement agencies' use of electronic surveillance is shared across the Commonwealth Ombudsman and a range of state and territory oversight bodies. The Commonwealth Ombudsman's powers are set out in several pieces of legislation, including the TIA Act and the *Ombudsman Act 1976*. The Commonwealth Ombudsman conducts regular inspections to review Commonwealth, state and territory law enforcement agencies' compliance with the legislation in relation to the SD Act and those agencies' access to stored communications and telecommunications data under the TIA Act. The Commonwealth Ombudsman only oversees Commonwealth law enforcement agencies' use of interception under the TIA Act.

Significantly, the Commonwealth Ombudsman does not have power to oversee all aspects of Commonwealth law enforcement agencies' compliance with the law relating to interception powers. Instead, the Commonwealth Ombudsman only oversees those agencies' compliance with record-keeping and reporting obligations. This is considerably narrower than the IGIS' oversight of ASIO's use of interception powers. It is also more limited than the Commonwealth Ombudsman's oversight of law enforcement agencies' use of other electronic surveillance powers.

State and territory oversight bodies oversee state and territory agencies' use of interception powers under the TIA Act and of surveillance device powers. These oversight bodies also oversee state and territory law enforcement agencies' activities more broadly. To support this broader oversight, the Commonwealth Ombudsman may share information with state and territory oversight bodies from the Ombudsman's inspections of state and territory agencies in relation to electronic surveillance powers.

---

87 The Australian Security Intelligence (ASIS), the Australian Geospatial-Intelligence Organisation (AGO), the Defence Intelligence Organisation (DIO), the Australian Signals Directorate (ASD) and the Office of National Intelligence (ONI).

## Potential Future State

The IGIS will continue to oversee ASIO and other intelligence agencies' use of electronic surveillance and will retain its broad scope, wide discretion and significant powers.

The Comprehensive Review further recommended that IGIS oversight be expanded to include the intelligence functions of the ACIC and AUSTRAC but not the AFP or the Department of Home Affairs.<sup>88</sup> The Government is implementing this recommendation through the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020.

In line with the Comprehensive Review's recommendations, the Government is considering the scope and role of the Commonwealth Ombudsman, including whether the Commonwealth Ombudsman should assume greater responsibility for law enforcement agencies.<sup>89</sup> This would involve the Commonwealth Ombudsman overseeing all Commonwealth, state and territory law enforcement agencies' use of electronic surveillance powers under the new framework.

The Government will further consider the Commonwealth Ombudsman's ability to exchange information with state and territory oversight bodies, to ensure those bodies can maintain effective oversight of state and territory law enforcement agencies' broader activities as necessary.

The specific design of the oversight framework will depend on the form of the new powers. Consistent with the Comprehensive Review's recommendations, the design of the framework will involve extensive consultation with the IGIS and the Commonwealth Ombudsman to ensure that oversight issues can be addressed up front.<sup>90</sup> The framework will also be underpinned by the oversight principles recommended by the Comprehensive Review and any associated guidelines issued by the Attorney-General.<sup>91</sup>

## Questions

30. What are the expectations of the public, including industry, in relation to oversight of these powers, and how can a new oversight framework be designed to meet those expectations?
31. What, if any, changes are required to the scope, role and powers of the Commonwealth Ombudsman to ensure effective oversight of law enforcement agencies' use of powers in the new framework?

88 The Comprehensive Review, Volume 3, recommendation 168.

89 The Comprehensive Review, Volume 2, recommendations 129–131.

90 The Comprehensive Review, Volume 3, recommendation 170.

91 The Comprehensive Review, Volume 3, recommendation 171.

# Reporting and record-keeping requirements

## Current State

To support effective oversight and review of these powers, agencies that use electronic surveillance powers must keep a range of records and fulfil various reporting requirements in relation to the use of those powers. These requirements facilitate transparency in the use of these powers.

### Record-keeping

Law enforcement agencies, in particular, must keep detailed records about their use of powers. This includes keeping any warrants or authorisations they receive, along with details about each warrant. For example, agencies must typically keep records with details about how information obtained through the use of these powers has been used and communicated.

ASIO is required to keep records in accordance with the *Archives Act 1983* and specific provisions in the ASIO Act and TIA Act. In addition, the IGIS oversees ASIO record-keeping.

### Reporting requirements

Annual reporting is one public disclosure method used by agencies to support transparency in relation to the use of electronic surveillance. Law enforcement agencies provide detailed annual reports with statistics about their use of particular powers, including details of their expenditure on electronic surveillance. Similarly, ASIO provides annual reports to the Minister for Home Affairs in accordance with the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) and the ASIO Act.

There are a range of other reporting requirements that also contribute to transparency around the use of these powers. These include:

- The Department of Home Affairs maintaining registers of warrants, with details of all warrants obtained. These registers must be provided to the Minister for Home Affairs every 3 months.
- Law enforcement agencies providing a report to the Minister about each warrant or authorisation issued to the agency under the SD Act.
- ASIO providing a report to the Attorney-General about the extent to which the interception of communications under each warrant assisted ASIO in carrying out its functions.

- ASIO reporting statistics about the use of its powers to the Minister for Home Affairs.
  - An unclassified version of this report is public, but statistics about use of electronic surveillance powers are not included.

## Limitations

While the TIA Act, SD Act and ASIO Act contain a range of reporting requirements, not all of these requirements facilitate meaningful transparency. For example, the Comprehensive Review considered that details of expenditure on electronic surveillance do not meaningfully improve transparency, as it is not possible to make a useful comparison between different agencies and jurisdictions. Similarly, the Review noted that the requirement to provide warrant registers and to report on SD Act warrants to the Minister for Home Affairs serves no useful function, as the Minister cannot, and should not, direct law enforcement agencies on the conduct of their investigations.<sup>92</sup>

## Potential Future State

The Government will consider how reporting and record-keeping requirements can be revised and streamlined to ensure they support effective and meaningful transparency, accountability and oversight. Obligations will not necessarily be removed just because they are administratively burdensome. Consideration will be given to:

- the extent to which agencies should be required to notify or report to the appropriate oversight body on their use of powers to support effective oversight
- what oversight bodies should be required to report to the relevant Minister or parliament on – for example, the activities of oversight bodies to assess agency compliance, or whether agencies have been compliant with their obligations
- the level of public reporting on compliance and annual reports on use of the powers that should be retained to assist meaningful transparency and accountability.

---

<sup>92</sup> The Comprehensive Review, Volume 2, [31.41].

Reporting that does not assist meaningful transparency (such as reporting on annual expenditure on electronic surveillance or reporting on warrant registers) may be removed. Additional reporting obligations could be added to address any gaps in transparency. For example, the Comprehensive Review recommended including additional information in public reports on the use of electronic surveillance information by integrity agencies, such as how many people have been the subject of electronic surveillance and how often an issuing authority has requested additional information or amendments to the terms of a warrant.<sup>93</sup>

## Questions

32. How could the new framework streamline the existing record-keeping and reporting obligations to ensure effective and meaningful oversight?
33. Are there any additional reporting or record-keeping requirements agencies should have to improve transparency, accountability and oversight?

---

93 The Comprehensive Review, Volume 2, page 440.

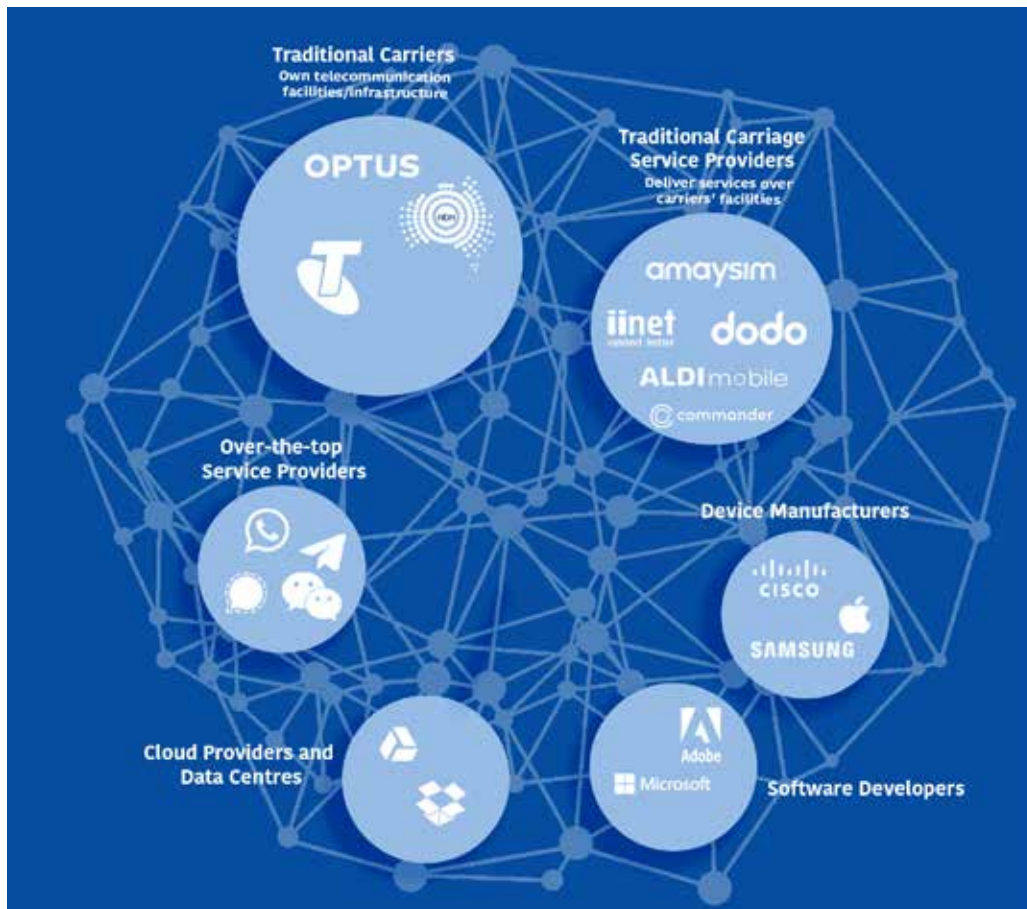


# **PART 6:** **WORKING TOGETHER:** **INDUSTRY AND GOVERNMENT**

---



The communications industry plays an important role in assisting Australian authorities with effective law enforcement and security investigations. The transition to a more globalised communications environment has seen exponential growth in the number and type of industry partners. These range from traditional carriers and carriage service providers to over-the-top providers, device manufacturers, software developers, cloud providers and data centres. With the evolution of communications technology the distinctions between these categories of services and providers is becoming increasingly blurred.



Industry is subject to a range of legal obligations to ensure the privacy of users and to assist government. These include obligations to protect the confidentiality of communications,<sup>94</sup> build and maintain telecommunications interception capabilities,<sup>95</sup> retain particular telecommunication data sets<sup>96</sup> and provide government agencies with assistance to overcome technology barriers to investigations.<sup>97</sup>

94 Telecommunications Act, Part 13.

95 TIA Act, Part 5-4.

96 TIA Act, Part 5-1A.

97 Telecommunications Act, Part 15.

Government is committed to working and consulting with industry to ensure obligations are reasonable and proportionate. Developing a new legal framework presents an opportunity to consider how the burden on industry can be reduced by streamlining and consolidating these obligations.

To a large degree, reforms to industry assistance obligations will depend on the outcome of a number of significant legislative reviews, including the PJCIS's review into the:

- *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (which will include consideration of the INSLM's review completed in June 2020) (currently under way)
- mandatory data retention regime
- Part 14 of the Telecommunications Act – Telecommunications Sector Security Reforms.

The Government's response to these reviews will be incorporated into the new framework. Government will consult on the implementation of these responses throughout the development of the new framework to ensure that the framework is fit for purpose.

Other potential areas for reform include:

- **Interception capability plans (ICPs):** Carriers and nominated carriage service providers are required to provide Government with annual ICPs detailing their ability to intercept communications transmitted over their network. However, ICPs frequently do not require significant updates. Under the new framework, the annual review process could be replaced with a standing obligation for carriers and carriage service providers to maintain a plan, updated as required. This could be, accompanied by a risk-based approach by the Government to selectively review plans. Such an approach would reduce the regulatory burden on industry and provide efficiencies for the Government.
- **Attribution-based interception:** Attribution-based interception would allow interception to be targeted based on a wider and more flexible range of 'attributes' or identifiers than current service- and device-based warrants. It would also allow a provider to 'filter' out intercepted material that is of limited investigative value (such as video and audio streaming services). Due to the costs involved, the Comprehensive Review recommended against industry being required to develop a general attribution-based capability. However, it did recommend the Attorney-General be given the power to require a particular company to develop and maintain such a capability where the benefits would justify the cost. Such an approach would reduce data storage implications and costs for agencies accepting large amounts of this data under a warrant.

## Questions

34. How workable is the current framework for providers, including the ability to comply with Government requests?
35. How could the new framework reduce the burden on industry while also ensuring agencies are able to effectively execute warrants to obtain electronic surveillance information?
36. How could the new framework be designed to ensure that agencies and industry are able to work together in a more streamlined way?

# **PART 7:** INTERACTION WITH EXISTING AND RECENT LEGISLATION AND REVIEWS

---



To ensure the privacy of Australians and help law enforcement agencies and ASIO to perform their duties, the Government is progressing legislative amendments to address gaps in the legal framework along with longer-term reforms to the electronic surveillance legal framework.

Such reforms are subject to the normal rigorous policy and legislative development process, including both public and parliamentary scrutiny. In particular, the PJCIS has completed, or is in the process of completing, inquiries into a number of matters that touch directly on the electronic surveillance framework. These include:

- [Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press](#)
- [Review of the amendments made by the Telecommunications and Other Legislation Amendment \(Assistance and Access\) Bill 2018](#) (also subject to a recent [INSLM review](#))
- [Review of the Surveillance Legislation Amendment \(Identify and Disrupt\) Bill 2020](#)
- [Telecommunications Legislation Amendment \(International Production Orders\) Bill 2020](#)
- [Review of the mandatory data retention regime](#)
- [Review of the Intelligence Oversight and Other Legislation Amendment \(Integrity Measures\) Bill 2020](#)
- [Review of the Foreign Intelligence Legislation Amendment Bill 2021](#)
- [Review of the Security Legislation Amendment \(Critical Infrastructure\) Bill 2020](#) and [Statutory Review of the Security of Critical Infrastructure Act 2018](#)
- [Review of Part 14 of the Telecommunications Act – Telecommunications Sector Security Reforms](#)
- [Review of the Counter-Terrorism Legislation Amendment \(High Risk Terrorist Offenders\) Bill 2020](#).

The PJCLE has also completed an [inquiry into the impact of new and emerging information and communications technology](#).

The current reform project will not revisit the outcome of such inquiries. Rather, developing the new electronic surveillance framework will allow the Government to work closely with affected stakeholders to appropriately implement the Government's response to those reviews, while ensuring they are consistent with the principles and thresholds outlined in this paper.

For the same reason, Government responses to inquiry recommendations that require changes to electronic surveillance laws will generally be implemented as part of the new framework. For example, some key recommendations from these reviews that will be implemented in the new framework include:

- clearly defining the term ‘content or substance of a communication’<sup>98</sup>
- placing obligations on agencies to quarantine the contents or substance of a communication and web-browsing history if the information has been supplied by a service provider in error along with the provision of telecommunications data<sup>99</sup>
- clarifying the scope and definition of data generated by ‘Internet of Things’ devices to be retained by providers<sup>100</sup>
- amending the reporting, record-keeping, retention period, authorisation and revocation provisions relating to authorisations to disclose telecommunications data<sup>101</sup>
- reducing the range of officers of criminal law enforcement agencies who may be designated as ‘authorised officers’ for the purposes of authorising the disclosure of telecommunications data<sup>102</sup>
- expanding the role of the Public Interest Advocate to include mandatory consideration by Public Interest Advocates of any warrant applications under the new framework that relate to a person working in a professional capacity as a journalist or a media organisation, where the warrant is related to the investigation of an unauthorised disclosure of government information or a Commonwealth secrecy offence<sup>103</sup>
- expanding the record-keeping and reporting requirements relating to the role of the Public Interest Advocate and warrants obtained in relation to journalists or media organisations.<sup>104</sup>

The list above is not exhaustive. It is likely new legislation will be developed and new reviews conducted during the course of the reform process. Such initiatives will run parallel to the broader reform effort and will be subject to their own scrutiny and consultation processes.

---

98 Data Retention review, recommendation 2.

99 Data Retention review, recommendation 3.

100 Data Retention review, recommendation 5.

101 Data Retention review, recommendations 6, 7, 9 and 10.

102 Data Retention review, recommendation 11.

103 Press Freedoms inquiry, recommendation 2.

104 Press Freedoms inquiry, recommendations 3, 4 and 5.

## Questions

37. Do you have views on how the framework could best implement the recommendations of these reviews? In particular:
- a. What data generated by 'Internet of Things' and other devices should or should not be retained by providers?
  - b. Are there additional records that agencies should be required to keep or matters that agencies should be required to report on in relation to data retention and to warrants obtained in relation to journalists or media organisations? How can any new reporting requirements be balanced against the need to ensure sensitive law enforcement or security investigations and capabilities are not compromised or revealed?
  - c. Is it appropriate that the Public Interest Advocate framework be expanded only in relation to journalists and media organisations?
  - d. What would be the impact on reducing the number of officers who may be designated as 'authorised officers' for the purposes of authorising the disclosure of telecommunications data?



# PART 8: GETTING INVOLVED

---



Electronic surveillance laws affect all Australians. The Government needs to hear from the community, businesses, industry organisations and advocacy groups to ensure the new framework protects privacy and is proportionate and fit for purpose in the current and emerging threat environment. This paper is the first of many opportunities to be heard.

The Department of Home Affairs (the Department) will conduct a number of rounds of public consultation, both virtual and face-to-face (where permitted), to ensure the new framework benefits from the shared experiences, learnings and challenges of all stakeholders. The consultation process will be comprehensive, genuine and iterative, commencing with this paper and culminating in close consultation on draft legislation.

Through this consultation, the Government hopes to build public confidence in the evidence base for change, understanding of the existing complexities of these laws, and instil transparency at the heart of the new framework.

## How to make a submission

The Department of Home Affairs invites written submissions based on the questions posed in this discussion paper.

Submissions should be made online at [www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers](http://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers) or via post.

Hardcopy submissions can be posted to:

Electronic Surveillance Reform Branch  
Department of Home Affairs  
PO Box 25  
BELCONNEN ACT 2616

The Department will consider hardcopy submissions received by post. However, these submissions will not be published on the website.

Submissions should be received by the Department by 5.00 PM AEDT, Friday 11 February 2022.

## Privacy collection notice

The Department is bound by the Australian Privacy Principles (APPs) in the *Privacy Act 1988* (Cth) (the Privacy Act). The APPs regulate how we collect, use, store and disclose personal information, and how you may seek access to, or correction of, the personal information that we hold about you.

Providing personal information in your submission is voluntary. Please refrain from including personal information of any third parties. The Department may publish your submission (including your name), unless you request that your submission remain anonymous or confidential, or we consider (for any reason) that it should not be made public. If you do not tell us that your submission is to remain anonymous or confidential, you acknowledge that by providing your submission it may be accessible to people outside Australia and that you are aware that:

- any overseas recipient(s) will not be accountable under the Privacy Act for any acts or practices of the overseas recipient in relation to the information that would breach the APPs (s); and
- you will not be able to seek redress under the Privacy Act if an overseas recipient handles your personal information in breach of the Privacy Act.

The Department may redact parts of published submissions, as appropriate. For example, submissions may be redacted to remove defamatory or sensitive material. Submissions containing offensive language or inappropriate content will not be responded to and may be destroyed.

Information you provide in your submission, including personal information, may be disclosed to the Commonwealth; state and territory governments and their departments and agencies; and third parties who provide services to the Department, for the purposes of informing and supporting the work of the Electronic Surveillance Reform Branch. This information may also be used to communicate with you about your submission and the consultation process.

For more information about the Department's personal information handling practices, including how you can seek access to, or correction of, personal information that the Department holds about you, or how to make a complaint if you believe that the Department has handled your personal information in a way that breaches our obligations in the APPs, please refer to the Department's privacy policy, which you can access [here](#).

Please refer to our Privacy Policy or consultation privacy notice on our submission webpage to find out more.

# PART 9: ATTACHMENTS

---



# Attachment A: Key electronic surveillance provisions

Telecommunications Act 1997 – key electronic surveillance provisions	
Relevant electronic surveillance purposes	<p>The electronic surveillance provisions of the Act:</p> <ul style="list-style-type: none"> <li>• create a framework for telecommunications industry participants to <b>protect information</b> relating to the contents of a communication, services they are providing to individuals, and personal details of customers – Part 13</li> <li>• create a framework for telecommunications industry to understand their <b>obligations for national interest matters</b>, providing help as is reasonably necessary under a no profit, no loss condition – Part 14</li> <li>• create a framework for <b>industry to assist law enforcement and national security agencies</b>, including to facilitate the exercise of agencies' powers under the <i>Telecommunications (Interception and Access) Act 1979</i> (TIA Act) – Parts 14 and 15</li> </ul>
Protecting information or documents	
Key concepts	<ul style="list-style-type: none"> <li>• <b>Carriers</b> are holders of a carrier licence, which is a type of licence required before certain infrastructure can be used to carry communications – section 7 and Part 3</li> <li>• <b>Carriage Service Providers</b> are industry participants who use a carrier's network to provide telecommunications services to the public – section 87</li> <li>• <b>Content Service Provider</b> is a person that uses or proposes to use a listed carriage service to provide a content service, for example, a broadcasting service, an on-line entertainment service or any other online service – section 97</li> </ul>
Protection of communications	<ul style="list-style-type: none"> <li>• It is an offence for certain participants in the telecommunications industry (including carriers and carriage service providers) to use or disclose information that relates to: <ul style="list-style-type: none"> <li>– the contents of a person's communications</li> <li>– carriage services supplied by carriers and carriage service providers</li> <li>– the affairs or personal particulars of persons – sections 276-278</li> </ul> </li> <li>• There are a range of <b>permitted purposes</b> for use and disclosure of this information which are exceptions to the offence. For example, use or disclosure is not prohibited if it is by an employee of a carrier in the performance of the person's duties. Disclosure is also not prohibited where it is required or authorised under a warrant or under law – sections 279-293 <ul style="list-style-type: none"> <li>– If information is lawfully disclosed to a person for one of these purposes, there are <b>offences for secondary use or disclosure</b>. For example, if information is disclosed to a person by an employee of a carrier for a purpose related to the performance of the employee's functions, the person must not disclose or use the information or document except for that purpose – sections 296-303</li> </ul> </li> </ul>
Obligation to assist agencies	<ul style="list-style-type: none"> <li>• <b>Carriers and carriage service providers must give Commonwealth, state and territory agencies such help as is reasonably necessary</b> for a range of specified purposes, including enforcing the criminal law of Australia and foreign countries, management of natural disasters, protecting public revenue, investigating or prosecuting war crimes and safeguarding national security – subsection 313(3)</li> </ul>
Reporting and record-keeping	<ul style="list-style-type: none"> <li>• Carriers and carriage service providers are required to <b>retain information</b> about disclosures of information, including telecommunications data disclosed in compliance with an authorisation under the TIA Act. Carriers and providers must also provide <b>annual reports</b> to the Australian Communications and Media Authority on disclosures – sections 305-307</li> </ul>

## Industry assistance

Key concepts	<ul style="list-style-type: none"> <li>• <b>Designated communications providers</b> include a wide range of companies, businesses, organisations or individuals that contribute to the communications supply chain in Australia – section 317C</li> </ul>
Industry assistance	<ul style="list-style-type: none"> <li>• The head, or delegated senior executive, of the Australian Security Intelligence Organisation (ASIO), the Australian Signals Directorate (ASD), the Australian Secret Intelligence Service (ASIS), the Australian Federal Police (AFP), the Australian Criminal Intelligence Commission (ACIC) or a state or territory police force may give a <b>technical assistance request (TAR)</b> to a designated communications provider, requesting they do specified things to assist the agency. This ensures providers are immune to civil liability when they are obligated to or are voluntarily assisting agencies – section 317G</li> <li>• The head, or delegated senior executive, of ASIO, AFP, ACIC and a state or territory police force (with approval from the AFP Commissioner) may give a <b>technical assistance notice (TAN)</b> to a designated communications provider, requiring them to do specified things to assist the agency. This establishes a legal obligation for assistance, where the assistance falls within a providers' existing business functions – section 317L</li> <li>• The Attorney-General, with the agreement of the Minister for Communications, may issue a <b>technical capability notice (TCN)</b> requiring that a provider build a capability to assist law enforcement and national security agencies. These may be requested by ASIO, AFP, ACIC or a State or Territory police force – section 317T             <ul style="list-style-type: none"> <li>– Assistance may only be sought in relation to the <b>relevant object of the issuing agency</b>. ASIO may only seek assistance in relation to their functions in safeguarding national security.</li> <li>– Law enforcement agencies may only seek assistance in relation to enforcing the criminal law for serious offences in Australia and overseas. A serious offence means an offence with a maximum penalty of at least 3 years' imprisonment.</li> </ul> </li> </ul>
Safeguards	<ul style="list-style-type: none"> <li>• These requests and notices may not introduce a systemic weakness or vulnerability to the carriage service – section 317ZG</li> <li>• A proposed request for assistance must be <b>reasonable, proportionate, practicable and technically feasible</b> – sections 317JAA, 317P and 317V</li> <li>• Agencies are expressly required to <b>consult with a provider</b> before requiring their assistance – section 317PA and 317W</li> <li>• Technical assistance requests, technical assistance notices and technical capability notices <b>cannot permit or compel providers to do an act or thing for which an officer of an agency would be required to obtain a warrant or authorisation permitting such an action</b> – section 317ZH</li> </ul>
Reporting and record-keeping	<ul style="list-style-type: none"> <li>• The <b>Inspector-General of Intelligence and Security must be notified</b> within seven days that a request for assistance has been made by ASIO – sections 317HAB, 317MAB and 317TAB</li> <li>• The <b>Commonwealth Ombudsman must be notified</b> within seven days that a request for assistance has been made by law enforcement agencies – sections 317HAB, 317MAB and 317TAB</li> <li>• Agencies are required to provide a report to the Minister for Home Affairs on any TARs, TANs and TCNs given in a financial year and the offences for which they were given, for inclusion in the TIA Act Annual Report – section 317ZS</li> </ul>

Division 2 of Part III of the *Australian Security Intelligence Organisation Act 1979* – key electronic surveillance provisions

Purpose	<ul style="list-style-type: none"> <li>The electronic surveillance provisions of the Act regulate the Australian Security Intelligence Organisation's (ASIO's) <b>powers to use surveillance devices and access computers</b>.</li> </ul>
Key concepts	<ul style="list-style-type: none"> <li><b>Surveillance device</b> means any of the following (or a device that is any combination of the following): <ul style="list-style-type: none"> <li><b>listening device</b> – meaning a device capable of being used to overhear, record, monitor or listen to a conversation or words spoken to or by any person in conversation (but not devices like a hearing aid)</li> <li><b>optical surveillance device</b> – meaning a device capable of being used to record visually or observe an activity (but not devices like spectacles or contact lenses)</li> <li><b>tracking device</b> – meaning a device capable of being used to determine or monitor the location of a person or an object or the status of an object – section 22</li> </ul> </li> </ul>
Offences	<ul style="list-style-type: none"> <li>The Act <b>provides a legal framework to authorise ASIO to undertake electronic surveillance activities that would otherwise be unlawful</b>. <ul style="list-style-type: none"> <li>State and territory legislation also regulates the use of surveillance devices. Prohibitions in relation to the use of surveillance devices differ in each state and territory.</li> </ul> </li> <li>The <i>Criminal Code Act 1995</i> contains a range of computer offences, including offences for unauthorised access, modification or impairment to data held in or electronic communication to or from a computer.</li> </ul>
Warrants	<p><i>Surveillance device warrants</i></p> <ul style="list-style-type: none"> <li>On application by the Director-General of Security, the Attorney-General may issue a <b>surveillance device warrant</b>. The threshold depends on whether the warrant relates to a person, premises or an object. For example, the Attorney-General may only issue a warrant in relation to a person if satisfied that the person is engaged in activities prejudicial to security and the use of a surveillance device is likely to assist ASIO in carrying out its function of obtaining intelligence in relation to security – section 26 <ul style="list-style-type: none"> <li>A surveillance device warrant <b>authorises the installation, use and maintenance of a device</b>, as well as related activities such as entry onto premises, retrieval of the device, and any other thing reasonably incidental to these activities – section 26B</li> </ul> </li> </ul> <p><i>Computer access warrants</i></p> <ul style="list-style-type: none"> <li>On application by the Director-General of Security, the Attorney-General may issue a <b>computer access warrant</b>. The Attorney-General may only issue a warrant if satisfied that there are reasonable grounds for believing that access to data in a computer will substantially assist the collection of intelligence in respect of a matter that is important in relation to security – section 25A <ul style="list-style-type: none"> <li>A computer access warrant can authorise activities such as using a computer, telecommunications facility, electronic equipment or a data storage device for the purpose of obtaining access to data held in the computer. A warrant can also authorise related activities necessary for the purpose of the warrant such as entering premises – section 25A</li> </ul> </li> </ul>

Internal authorisations	<ul style="list-style-type: none"> <li>• The Director-General can issue computer access warrants and surveillance device warrants in limited <b>emergency circumstances</b> – section 29</li> <li>• The Act itself authorises ASIO to use a <b>listening device</b> in limited circumstances, including to listen to or record words spoken by or to an ASIO employee or affiliate – section 26C</li> <li>• The Act itself authorises ASIO to use an <b>optical device</b> if the installation or retrieval of the device does not involve entry onto premises or interference with the interior of a vehicle without permission – section 26D</li> <li>• ASIO can use a <b>tracking device under an internal authorisation</b> if the authorising office is satisfied that there are reasonable grounds for believing that the use of the tracking device will, or is likely to, substantially assist the collection of intelligence in respect of a matter that is important in relation to security. An internal authorisation cannot authorise entry onto premises or interference with the interior of a vehicle without permission from the owner, remote installation of tracking devices, or use of a tracking device to listen or record words or communications. ASIO can also use a tracking device without a warrant if the person being tracked consents – sections 26E and 26G-26R</li> </ul>
Using information	<ul style="list-style-type: none"> <li>• The ASIO Act contains <b>offences for unauthorised dealing</b> with information acquired or prepared by ASIO in connection with its functions or related to the performance by ASIO of its functions – sections 18-18C</li> <li>• There are a range of <b>permitted purposes</b> for using and communicating such information, including communicating information relating to the commission of a serious crime to a relevant Commonwealth or State authority – sections 18, 18D, 19 and 19A</li> </ul>
Reporting and record-keeping	<ul style="list-style-type: none"> <li>• ASIO must destroy information obtained under a warrant if the Director-General of Security is satisfied that the information is not required for the purposes of ASIO's functions or powers – section 31</li> <li>• The Director-General of Security must report to the Attorney-General on various matters, including the extent to which action taken under warrant or a tracking device authorisation has assisted ASIO in carrying out its functions – sections 34-34AAB</li> <li>• The Director-General of Security must give an annual report to the Minister for Home Affairs setting out a range of matters including the number of warrant requests made. The Minister must table the report in Parliament, subject to deletions necessary to avoid prejudice to security, the defence of the Commonwealth, the conduct of the Commonwealth's international affairs or the privacy of individuals – section 94</li> </ul>
Oversight	<ul style="list-style-type: none"> <li>• The Inspector-General of Intelligence and Security's functions and powers concerning oversight of the legality and propriety of ASIO's activities are largely set out in the <i>Inspector-General of Intelligence and Security Act 1986</i>.</li> <li>• ASIO is required to comply with guidelines issued by the Minister for Home Affairs relating to the performance of ASIO's functions and powers – section 8A</li> <li>• The ASIO Act provides that: <ul style="list-style-type: none"> <li>– ASIO's functions do not include the investigation of lawful advocacy, protest or dissent – Section 17A</li> <li>– The Director-General of Security must take all reasonable steps to ensure that the work of ASIO is limited to what is necessary for the purposes of the discharge of its functions, and that ASIO is kept free from any influences or considerations not relevant to its functions and that nothing is done that might lend colour to any suggestion that it is concerned to further or protect the interests of any particular section of the community, or with any matters other than the discharge of its functions – section 20</li> </ul> </li> </ul>



## Surveillance Devices Act 2004 – key provisions

Purpose	<ul style="list-style-type: none"> <li>The Act provides a regime for primarily Commonwealth law enforcement agencies' <b>to use surveillance devices and access computers</b>. state and territory agencies may use the regime in limited circumstances.</li> </ul>
Key concepts	<ul style="list-style-type: none"> <li><b>Computer</b> means all or part of one or more computers, computer systems or computer networks – section 6</li> <li><b>Law enforcement agencies</b> are the Australian Federal Police (AFP), Australian Commission for Law Enforcement Integrity, Australian Criminal Intelligence Commission, and various state and territory law enforcement agencies – section 6A</li> <li><b>Relevant offences</b> are generally offences against Commonwealth laws and offences against state laws that have a federal aspect, that are punishable by a maximum term of 3 years' imprisonment or more – sections 6 and 7</li> <li><b>Surveillance device</b> means any of the following (or a device that is any combination of the following): <ul style="list-style-type: none"> <li><b>data surveillance device</b> – meaning a device or program capable of being used to record or monitor the input of information into, or the output of information from, an electronic device for storing or processing information</li> <li><b>listening device</b> – meaning a device capable of being used to overhear, record, monitor or listen to a conversation or words spoken to or by any person in conversation (but not devices like a hearing aid)</li> <li><b>optical surveillance device</b> – meaning a device capable of being used to record visually or observe an activity (but not devices like spectacles or contact lenses)</li> <li><b>tracking device</b> – meaning a device capable of being used to determine or monitor the location of a person or an object or the status of an object – section 6</li> </ul> </li> </ul>
Offences	<ul style="list-style-type: none"> <li>The Act does <b>not prohibit electronic surveillance activities</b>.</li> <li>State and territory legislation prohibits the use of surveillance devices. The prohibitions differ in each state and territory.</li> <li>The <i>Criminal Code Act 1995</i> includes offences for unauthorised access, modification or impairment to data held in or electronic communication to or from a computer.</li> </ul>
Warrants	<p><i>Surveillance device warrants</i></p> <ul style="list-style-type: none"> <li>On application by a law enforcement agency, a Judge or Administrative Appeals Tribunal (AAT) member <b>may issue a surveillance device warrant</b> in relation to the investigation of a relevant offence, recovering a child subject to a recovery order, an international assistance investigation, an integrity operation, or a person subject to a control order. The thresholds and relevant considerations differ depending on what the warrant relates to. For example, if the warrant relates to the investigation of a relevant offence, the Judge or AAT member must be satisfied there are reasonable grounds for suspecting that the use of a surveillance device is necessary in the course of the investigation, having regard to matters such as the gravity of the offence being investigated – sections 14 and 16 <ul style="list-style-type: none"> <li>A surveillance device warrant <b>authorises the installation, use and maintenance of a device</b>, as well as related activities such as entry onto premises, retrieval of the device, or breaking open something to install the device etc. – section 18</li> <li>Law enforcement agencies can apply to an eligible Judge or nominated AAT member for a warrant to <b>retrieve a surveillance device</b> that was lawfully installed – section 22</li> </ul> </li> </ul>

	<p><i>Computer access warrants</i></p> <ul style="list-style-type: none"> <li>• On application by a law enforcement agency, a Judge or AAT member may issue a <b>computer access</b> warrant in relation to the investigation of a relevant offence, recovering a child subject to a recovery order, an international assistance investigation, an integrity operation, or a person subject to a control order. The threshold and relevant considerations differ depending on what the warrant relates to. For example, if the warrant relates to the investigation of a relevant offence, the Judge or AAT member must be satisfied there are reasonable grounds for suspecting that the use of a surveillance device is necessary in the course of the investigation of a relevant offence, having regard to matters such as the gravity of the offence being investigated – sections 27A and 27C       <ul style="list-style-type: none"> <li>– A computer access warrant can authorise activities such as using a computer, telecommunications facility, electronic equipment or a data storage device for the purpose of obtaining access to data held in the computer. A warrant can also authorise related activities, such as entering premises, or adding, copying, deleting or altering data in the computer – section 27E</li> </ul> </li> </ul> <p><i>Data disruption warrants</i></p> <ul style="list-style-type: none"> <li>• On application by the AFP or ACIC, a judged or nominated AAT member may issue a data disruption warrant to authorise disruption of data for the purposes of frustrating the commission of a relevant offence. A Judge or nominated AAT member may issue a data disruption warrant if satisfied that there are reasonable grounds for the suspicion founding the application for the warrant and the disruption of data authorised by the warrant is reasonably necessary and proportionate, having regard to the offences (there are also a range of additional factors the issuing authority must have regard to) – section 27KC       <ul style="list-style-type: none"> <li>– A data disruption warrant can authorise the AFP or ACIC to add, copy, alter and delete data to allow access to, and disruption of data for the purposes of frustrating criminal offences</li> </ul> </li> </ul> <p><i>Network activity warrants</i></p> <ul style="list-style-type: none"> <li>• On application by the AFP or ACIC, a Judge or nominated AAT member may issue a <b>network activity warrant</b> to authorise the collection of intelligence that relate to a criminal network of individuals. A Judge or nominated AAT member may issue a network activity warrant if satisfied that there are reasonable grounds for the suspicion founding the application of the warrant and the issue of the warrant is justified and proportionate, having regard to the kinds of offences in relation which information will be obtained under the warrant (there are also a range of additional factors the issuing authority must have regard to) – section 27KM       <ul style="list-style-type: none"> <li>– A network activity warrant can authorise the AFP and ACIC to access data held in computers used by the criminal network operating online to understand the scope of their activities and the identities of their members. Information collected under network activity warrants cannot be used in evidence in respect of the relevant offence.</li> </ul> </li> </ul>
Internal authorisations	<ul style="list-style-type: none"> <li>• Law enforcement agencies can use surveillance devices or access a computer without a warrant (but with internal authorisation by specified senior officials) in limited circumstances:       <ul style="list-style-type: none"> <li>– Law enforcement agencies can use <b>optical or tracking devices without a warrant</b> for certain purposes if the installation or retrieval of the device does not involve entry onto premises or interference with the interior of a vehicle without permission. Agencies can use a <b>listening device without a warrant</b> in limited circumstances, including listening to or recording words spoken by or to a law enforcement officer – sections 37, 38 and 39</li> </ul> </li> </ul>
Emergency authorisations	<ul style="list-style-type: none"> <li>• In limited <b>emergency circumstances</b> (for example, where there is a serious risk to a person or property), specified senior officers in a law enforcement agency may authorise the use of a surveillance device, access to a computer or data disruption warrant. Safeguards on these powers include a requirement to apply for approval of the authorisation by a Judge or AAT member within 48 hours – sections 28-36</li> </ul>

Dealing with protected information	<ul style="list-style-type: none"> <li>• It is an <b>offence to use, record, communicate or publish protected information</b>, meaning information obtained under a warrant issued under the Act and information about such warrants – sections 45 and 45B</li> <li>• Information can be communicated, used or recorded for certain <b>permitted purposes</b>, including where there is a reasonable belief that the use or communication is necessary to help prevent or reduce the risk of serious violence to a person or substantial damage to property – sections 45, 45A and 45B</li> <li>• <b>Protected information must be kept in a secure place and must be destroyed</b> as soon as practicable or within 5 years after it was created, unless the agency certifies that the information is likely to be required for specified purposes – section 46</li> </ul>
Reporting and record-keeping	<ul style="list-style-type: none"> <li>• Agencies must <b>retain documents</b> connected with warrants and authorisations (including a copy of each warrant and each application) and must keep a <b>register of warrants and authorisations</b> – sections 51, 52 and 53</li> <li>• Agencies have obligations to report to the Minister for Home Affairs and the Commonwealth Ombudsman on certain matters relating to the use of powers. Details about the use of powers must be included in an annual report to the Minister, which is tabled in Parliament – sections 49 and 50</li> </ul>
Oversight	<ul style="list-style-type: none"> <li>• The <b>Commonwealth Ombudsman has oversight</b> of agencies' use of these powers, except network activity warrants, and is required to inspect agencies' records accordingly. The Ombudsman has a range of powers, including the power to require officers to answer questions. The Ombudsman reports to the Minister on inspections, and may report on breaches of the Act – sections 60 and 61</li> <li>• The <b>Inspector-General of Intelligence and Security (IGIS) has oversight</b> of agencies' use of network activity warrants and may inspect agencies' records accordingly. The IGIS has a range of powers to require officers to give information or produce documents within a reasonable period. The IGIS must provide reports as a result of its inquiries to the Minister – section 22 of the <i>Inspector-General of Intelligence and Security Act 1986</i></li> </ul>

### Telecommunications (Interception and Access) Act 1979 – key provisions

Purpose	<ul style="list-style-type: none"> <li>• The Act regulates law enforcement agencies' and the Australian Security Intelligence Organisation's (ASIO's) <b>powers to access communications</b> (whether passing over a telecommunications network or held by a communications service provider) and <b>information about those communications</b>.</li> </ul>
Key concepts	<ul style="list-style-type: none"> <li>• <b>Communication</b> is defined to include conversations and messages, whether in the form of speech, music or other sounds, data, text, visual images, signals, or any other form or combination of forms – section 5</li> <li>• <b>Interception agencies</b> are the Australian Federal Police, Australian Commission for Law Enforcement Integrity, Australian Criminal Intelligence Commission, and various state and territory law enforcement agencies – section 5</li> <li>• <b>Criminal law enforcement agencies</b> include all interception agencies as well as the Australian Border Force, Australian Securities and Investments Commission and the Australian Competition and Consumer Commission – section 110A</li> <li>• <b>Enforcement agencies</b> include all criminal law enforcement agencies and any other declared bodies (of which there are currently none) – section 176A</li> <li>• <b>Interception of a communication</b> means listening to or recording a communication passing over a telecommunications system without the knowledge of the person making the communication – section 6</li> <li>• <b>Stored communications</b> are communications that are not passing over a telecommunications system, are held on a carrier's equipment, and that can only be accessed by a party to the communication or with the assistance of a carrier – section 5</li> </ul>

Offences	<ul style="list-style-type: none"> <li>• It is an <b>offence to intercept a communication</b> passing over a telecommunication system – sections 7 and 105</li> <li>• It is an <b>offence to access a stored communication</b> without the knowledge of the sender or intended recipient of the stored communication – section 108</li> <li>• There are prescribed <b>exceptions</b> to these offences, most notably for interception of communications and access to stored communications under a warrant – subsections 7(2)-(10) and 108(2)-(4)</li> </ul>
Law enforcement warrants	<ul style="list-style-type: none"> <li>• On application by an interception agency, a Judge or Administrative Appeals Tribunal (AAT) member can issue an <b>interception warrant</b> permitting the interception of communications. The Judge or AAT member must be satisfied of various things, including that information likely to be obtained by intercepting the communication would be likely to assist in the investigation of an offence constituting certain conduct with a maximum penalty of 7 years' imprisonment or more (and some other specified offences) – sections 39, 46 and 46A <ul style="list-style-type: none"> <li>– Typically, interception activities under a warrant must be undertaken by a carrier – section 47</li> </ul> </li> <li>• On application by a criminal law enforcement agency, a Judge, magistrate or AAT member can issue a <b>stored communications warrant</b> permitting access to stored communications. The Judge, magistrate or AAT member must be satisfied of various things, including that information obtained by accessing those communications would be likely to assist in an investigation into an offence with a maximum penalty of 3 years' imprisonment or more – sections 110 and 116</li> <li>• Authorised senior officers in enforcement agencies can authorise <b>disclosure of historical telecommunications data</b>, meaning data that exists at the time the authorisation is made. An officer can only authorise disclosure of the information if satisfied that it is reasonably necessary for the enforcement of the criminal law, enforcement of a law imposing a pecuniary penalty, protection of public revenue, or the location of a missing person – sections 178, 178A, 179</li> <li>• Authorised senior officers in enforcement agencies can authorise <b>disclosure of prospective telecommunications data</b>, meaning data that comes into existence during a specified period after the authorisation is made. An officer can only authorise disclosure if satisfied that it is reasonably necessary for an investigation into an offence with a maximum penalty of 3 years' imprisonment or more (and some other specified offences) – section 180</li> </ul>
ASIO warrants	<ul style="list-style-type: none"> <li>• The Attorney-General can issue an <b>interception warrant</b> permitting authorised ASIO employees or affiliates to intercept a communication. The Attorney-General must be satisfied of various things, including that the interception of communications will, or is likely to, assist ASIO in carrying out its function of obtaining intelligence relating to security – sections 9 and 9A</li> <li>• An interception warrant also permits ASIO to access <b>stored communications</b> – subsections 9(1A) and 9A(1C)</li> <li>• The <b>Attorney-General</b> can also issue a warrant to permit authorised ASIO employees or affiliates to intercept communications or access stored communications for the collection of foreign intelligence – sections 11A to 11C</li> <li>• The Director-General of Security, the Deputy Director-General of Security or an authorised ASIO employee or affiliate can authorise the <b>disclosure of historical telecommunications data</b>. The person can only make an authorisation if satisfied that the disclosure would be in connection with the performance by ASIO of its functions – section 175</li> <li>• The Director-General of Security, the Deputy Director-General of Security or an authorised senior ASIO employee or affiliate can authorise <b>disclosure of prospective telecommunications data</b>. The person can only make an authorisation if satisfied that the disclosure would be in connection with the performance by ASIO of its functions – section 176</li> </ul>

International Production Orders	<ul style="list-style-type: none"> <li>• Australian agencies can serve domestic warrants for electronic data directly to communications service providers located in foreign countries with whom the Government has signed a cross-border access to data agreement through the international production orders scheme – Schedule 1</li> </ul>
Dealing with information	<ul style="list-style-type: none"> <li>• There are <b>offences for using, disclosing or dealing with information</b> obtained under a warrant or authorisation, or information about a warrant or authorisation – sections 63, 105, 133 and 181A-182B</li> <li>• There are a range of <b>permitted purposes for dealing with information</b>, including in connection with the investigation of certain offences – sections 63AA-76A, 134-146, 181A(6), 181B(3), 182(2)-(4A) and 182B</li> </ul>
Reporting and record-keeping	<ul style="list-style-type: none"> <li>• Agencies have <b>obligations to keep certain documents</b> in connection with warrants issued, as well as destruction requirements – sections 80-81AA, 151, 185 and 186A</li> <li>• The Department of Home Affairs must keep a <b>General Register and a Special Register of Warrants</b> – sections 81A-81D</li> <li>• Agencies have <b>obligations to report to the Minister for Home Affairs</b> about the use of their powers, and this information is published in an annual report – sections 93-104, 159-164 and 186</li> </ul>
Oversight	<ul style="list-style-type: none"> <li>• The Commonwealth Ombudsman <b>oversees the use of law enforcement agencies' powers</b>, and conducts inspections of their records. The Ombudsman reports to the Minister for Home Affairs on inspections, and may report on breaches of the Act – Chapter 4A</li> <li>• The Inspector-General of Intelligence and Security's functions and powers concerning oversight of the <b>legality and propriety of ASIO's activities</b> (including under the TIA Act) are largely set out in the <i>Inspector-General of Intelligence and Security Act 1986</i></li> </ul>
Working with industry	<ul style="list-style-type: none"> <li>• There are various <b>industry obligations</b>, including to nominate delivery points from which an agency can access intercepted communications, maintain interception capabilities, and submit interception capability plans annually – Parts 5-2 to 5-6</li> <li>• Service providers have <b>obligations to keep certain types of information</b> for a period of 2 years in order to assist agencies with their investigations. This includes subscriber information, the source of a communication, the destination of a communication, the time a communication was made, the type of service used, and the location of the equipment used – Part 5-1A</li> </ul>

# Attachment B: Comparison of Five Eyes electronic surveillance powers<sup>105</sup>

## Interception and access to stored communications

	Australia	Canada	New Zealand	United Kingdom	United States
Prohibition	<p><i>Telecommunications (Interception and Access) Act 1979</i> (TIA Act) – s7 and 108</p> <ul style="list-style-type: none"> <li>A person shall not intercept, authorise, or enable another person to intercept a communication passing over a telecommunications system.</li> <li>A person commits an offence if they access a stored communication, or authorise or assist another person to access a stored communication without the knowledge of the intended recipient or the sender of the stored communication.</li> </ul> <p><i>Criminal Code Act 1995 – Part 10.6</i></p> <ul style="list-style-type: none"> <li>Range of criminal offences for unlawfully accessing or interfering with a telecommunications system.</li> </ul>	<p><i>Criminal Code Act – s184(1)</i></p> <ul style="list-style-type: none"> <li>Every person who, by means of any electro-magnetic, acoustic, mechanical or other device, knowingly intercepts a private communication is guilty of an indictable offence.</li> </ul>	<p><i>Crimes Act 1961 – s216B</i></p> <ul style="list-style-type: none"> <li>It is an offence to intentionally intercept any private communication by means of an interception device.</li> </ul> <p><i>Bill of Rights Act 1990 – s21</i></p> <ul style="list-style-type: none"> <li>Everyone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise.</li> </ul>	<p><i>Investigatory Powers Act 2016 – s3</i></p> <ul style="list-style-type: none"> <li>A person commits an offence if the person intentionally intercepts a communication in the course of its transmission by means of:                             <ul style="list-style-type: none"> <li>a public or private telecommunication system, or a public postal service,</li> <li>the interception is carried out in the United Kingdom, and</li> <li>the person does not have lawful authority to carry out the interception.</li> </ul> </li> <li>A person commits an offence where they knowingly or recklessly obtain communications data from a telecommunications operator or a postal operator without lawful authority.</li> <li>Intercepted content may not be selected for examination if any criteria used for the selection are referable to an individual known to be in the British Islands and the purpose of using those criteria is to identify the content of communications sent by, or intended for, that individual.</li> </ul>	<p><i>Electronic Communications Privacy Act of 1986</i> (ECPA), 18 U.S.C. §§ 2510-2523</p> <p>Title I of the ECPA (the Wiretap Act) – s2511:</p> <ul style="list-style-type: none"> <li>Offences for intentional actual or attempted interception, use or disclosure of any wire, oral, or electronic communication is an offence.</li> </ul> <p>Title II of the ECPA (Stored Communications Act) – s2701:</p> <ul style="list-style-type: none"> <li>Offences for intentional access to a facility through which an electronic communication service is provided and thereby obtain, alter or prevents authorised access to a wire or electronic communication is an offence.</li> </ul>

<sup>105</sup> The powers are grouped by reference to the electronic surveillance warrants currently available to Australian agencies. Some jurisdictions do not have directly referable powers. This comparison identifies powers in each jurisdiction that permit agencies to do activities broadly equivalent to those permitted by Australian warrants. It is important to note that comparable powers across these jurisdictions are performed by a range of agencies with different scopes and functions to agencies using powers in Australia.

Warrant(s)	Australia	Canada	New Zealand	United Kingdom	United States
<p><b>Interception Warrant (the Australian Security Intelligence Organisation (ASIO))</b> TIA Act- s9, 9A</p> <ul style="list-style-type: none"> <li>• interception of communications made to or from a service, including access to stored communications.</li> <li>• interception of communications that are being made to or from any telecommunications service that a specified person is using, including access to stored communications.</li> </ul> <p><b>Interception Warrant</b> TIA Act- s46, 46A</p> <p>Interception of communications made to or from a specified service.</p> <ul style="list-style-type: none"> <li>• interception of communications that are being made to or from any telecommunications service that a specified person is using.</li> </ul> <p><b>Stored Communications Warrant</b> TIA Act- s17</p> <ul style="list-style-type: none"> <li>• Permits access to communications stored by a carrier.</li> </ul>	<p><b>Interception Authorisation</b> <i>Criminal Code Act – s186</i></p> <ul style="list-style-type: none"> <li>• Interception by means of an electro-magnetic, acoustic, mechanical or other device.</li> <li>• Includes authority to install, maintain or remove the device.</li> </ul> <p><b>Interception Warrant</b> <i>Canadian Security Intelligence Service Act – s21</i></p> <ul style="list-style-type: none"> <li>• Intercept any communication or obtain any information, record, document or thing and for that purpose: <ul style="list-style-type: none"> <li>– enter any place or open or obtain access to any thing,</li> <li>– search for, remove or return, or examine, take extracts or make copies of or record the information, document or thing, or</li> <li>– install, maintain or remove any thing.</li> </ul> </li> <li>• Retain information collected or incidentally collected in the carrying out of the authorised activities.</li> </ul> <p><b>Measures to reduce threats to security of Canada</b> <i>Canadian Security Intelligence Service Act – s21</i></p> <ul style="list-style-type: none"> <li>• Alter, remove, replace, destroy, disrupt or degrade a communication or means of communication.</li> <li>• Alter, remove, replace, destroy, degrade, provide or interfere with anything or part of a thing, including records, documents and goods.</li> <li>• Fabricating or disseminating any information, record or document.</li> </ul>	<p><b>Surveillance Device Warrant</b> <i>Search and Surveillance Act 2012 – s49</i></p> <ul style="list-style-type: none"> <li>• Use of an interception device to intercept a private communication.</li> <li>• Use of a tracking device.</li> <li>• Observation of private activity in private premises, and any recording of that observation, by means of a visual surveillance device.</li> <li>• Use of a surveillance device that involves trespass to land or trespass to goods.</li> <li>• Observation of private activity in the curtilage of private premises.</li> <li>• Any recording of that observation by means of a visual surveillance device.</li> </ul> <p><b>Type 1 Intelligence Warrants</b> <i>Intelligence and Security Act 2017 – ss58-59, 67</i></p> <ul style="list-style-type: none"> <li>• Carry out otherwise unlawful activities for the purpose of collecting information about, or to do any other thing directly in relation to, any person who is— <ul style="list-style-type: none"> <li>– a New Zealand citizen or permanent resident of New Zealand, or</li> <li>– a class of person that includes citizens or permanent residents of New Zealand.</li> </ul> </li> <li>• Includes intercepting any private communications or classes of private communications.</li> </ul>	<p><b>Interception and Examination Warrant</b> <i>Investigatory Powers Act 2016 – s15</i></p> <ul style="list-style-type: none"> <li>• Interception of communications during transmission by means of a postal service or telecommunication system.</li> <li>• Obtaining of secondary data from communications transmitted by means of a postal service or telecommunication system and described in the warrant.</li> <li>• Selection of relevant content for examination.</li> </ul> <p><b>General Warrant</b> <i>Intelligence Services Act 1994 – s5</i></p> <ul style="list-style-type: none"> <li>• Taking of any such action as specified in the warrant in respect of any property or in respect of wireless telegraphy.</li> </ul>	<p><b>Order for interception of wire, oral, or electronic communication</b> <i>Wiretap Act – s2516</i></p> <ul style="list-style-type: none"> <li>• Interception by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of an offense, or investigative or law enforcement officers of: <ul style="list-style-type: none"> <li>– wire communications – the transfer of communication that include the human voice transmitted over a device,</li> <li>– oral communications – are generally face-to-face communications for which the speakers have a reasonable expectation of privacy, or</li> <li>– electronic communications – any transfer of data of any nature over a device that does not include the human voice, therefore containing things like written words and pictures.</li> </ul> </li> </ul> <p><b>Required disclosure of wire or electronic communications</b> <i>Stored Communications Act – s2703</i></p> <ul style="list-style-type: none"> <li>• Disclosure by communication service providers of non-content data, and stored wire and electronic communications.</li> </ul>	

	Australia	Canada	New Zealand	United Kingdom	United States
Distinction between interception and stored communications	Yes	No	No	No	Yes
Definition of communication	<p>TIA Act- s5</p> <ul style="list-style-type: none"> <li>• <i>Communication</i> includes conversation and a message, and any part of a conversation or message, whether in the form of speech, music or other sounds; data; text; visual images, whether or not animated; or signals; or in any other form or in any combination of forms.</li> <li>• <i>Stored communication</i> means a communication that is not passing over a telecommunications system, and is held on equipment that is operated by, and is in the possession of a carrier and 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.</li> </ul>	<p><b>Interception Authorisation</b> <i>Criminal Code Act – s183</i></p> <ul style="list-style-type: none"> <li>• <i>Private communication</i> means any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it.</li> </ul>	<p><b>Surveillance Device Warrant</b> <i>Search and Surveillance Act 2012 – s3</i></p> <ul style="list-style-type: none"> <li>• Private communication – means a communication (whether in oral or written form, or in the form of a telecommunication, or otherwise) made under circumstances that may reasonably be taken to indicate that any party to the communication desires it to be confined to the parties to the communication, but – does not include a communication of that kind occurring in circumstances in which any party to the communication ought reasonably to expect that the communication may be intercepted by some other person without having the express or implied consent of any party to do so.</li> </ul>	<p><b>Interception and Examination Warrant</b> <i>Investigatory Powers Act 2016 – s 261</i></p> <ul style="list-style-type: none"> <li>• <i>Communication</i> includes anything comprising speech, music, sounds, visual images or data of any description and signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus.</li> <li>• <i>Content of a communication</i> means any element of the communication or any data attached to or logically associated with the communication, which reveals anything of what might reasonably be considered to be the meaning of the communication.</li> </ul>	<p><i>Wiretap Act – s2510</i></p> <ul style="list-style-type: none"> <li>• <i>Electronic Communication</i> means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system that affects interstate or foreign commerce, but does not include: – any wire or oral communication, – any communication made through a tone-only paging device, – any communication from a tracking device (as defined in section 3117 of this title), or – electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.</li> </ul>



Australia	Canada	New Zealand	United Kingdom	United States
		<p><b>Type 1 Intelligence Warrants</b> <i>Intelligence and Security Act 2017</i> – s47</p> <ul style="list-style-type: none"> <li>• Communication includes signs, signals, impulses, writing, images, sounds, information, or data that a person or machine produces, sends, receives, processes, or holds in any medium.</li> <li>• <i>Private communication</i> means a communication (whether in oral or written form, or in the form of a telecommunication, or otherwise) made in circumstances that may reasonably be taken to indicate that any party to the communication desires it to be confined to the parties to the communication, but does not include a communication of that kind occurring in circumstances in which any party to the communication ought reasonably to expect that the communication may be intercepted by some other person without having the express or implied consent of any party to do so.</li> </ul>		<ul style="list-style-type: none"> <li>• <i>Wire communication</i> means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.</li> <li>• <i>Oral communication</i> means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication.</li> </ul>

	Australia	Canada	New Zealand	United Kingdom	United States
Definition of interception	<p><b>Interception Warrants</b> TIA Act – s6</p> <ul style="list-style-type: none"> <li>Interception of a communication passing over a telecommunications system consists of listening to or recording, by any means, such a communication in its passage over telecommunications system without the knowledge of the person making the communication.</li> </ul>	<p><b>Interception Authorisation</b> <i>Criminal Code Act – s183</i></p> <ul style="list-style-type: none"> <li>Intercept includes listen to, record or acquire a communication or acquire the substance, meaning or purport thereof.</li> <li>Electro-magnetic, acoustic, mechanical or other device means any device or apparatus that is used or is capable of being used to intercept a private communication, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing.</li> </ul> <p><b>Interception Warrant and measures to reduce threats to security of Canada</b> <i>Canadian Security Intelligence Service Act – s2</i></p> <ul style="list-style-type: none"> <li>Intercept has the same meaning as in section 183 of the Criminal Code.</li> </ul>	<p><b>Surveillance Device Warrant</b> <i>Search and Surveillance Act 2012 – s3</i></p> <ul style="list-style-type: none"> <li>Intercept, in relation to a private communication, includes hear, listen to, record, monitor, acquire or receive the communication either while it is taking place or while it is in transit.</li> </ul> <p><b>Type 1 Intelligence Warrants</b> <i>Intelligence and Security Act 2017 – s47</i></p> <ul style="list-style-type: none"> <li>Intercept, in relation to a private communication, includes to hear, listen to, record, monitor, acquire, or receive the communication, or acquire its substance, meaning, or sense,— (a) while it is taking place; or (b) in the course of transmission</li> </ul>	<p><b>Interception and Examination Warrant</b> <i>Investigatory Powers Act 2016 – s4</i></p> <ul style="list-style-type: none"> <li>Intercept, in the course of transmission by means of a telecommunication system, means conducting any of the following: <ul style="list-style-type: none"> <li>modifying or interfering with the system or its operation, or</li> <li>monitoring transmissions</li> </ul> </li> <li>with the effect of making any content of the communication available at a relevant time, to a person who is not the send or intended recipient of the communication.</li> </ul>	<p><i>Wiretap Act – s2510</i></p> <ul style="list-style-type: none"> <li>Intercept means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.</li> </ul>
Issuing authority	<p><b>Interception Warrant (ASIO)</b> TIA Act– s9, s9A</p> <ul style="list-style-type: none"> <li>The Attorney-General.</li> </ul> <p><b>Interception Warrant</b> TIA Act– s46, s46A</p> <ul style="list-style-type: none"> <li>An eligible Judge or nominated AAT member.</li> </ul> <p><b>Stored Communications Warrant</b> TIA Act– s116</p> <ul style="list-style-type: none"> <li>An eligible Judge or nominated AAT member.</li> </ul>	<p><b>Interception Authorisation</b> <i>Criminal Code Act – s186</i></p> <ul style="list-style-type: none"> <li>Judge/superior court of criminal jurisdiction judge and signed by the Attorney General of the province or the Minister of Public Safety and Emergency Preparedness or a designated minister.</li> </ul> <p><b>Interception Warrant</b> <i>Canadian Security Intelligence Service Act – s21</i></p> <ul style="list-style-type: none"> <li>Application to a Judge with approval of the Minister.</li> </ul>	<p><b>Surveillance Device Warrant</b> <i>Search and Surveillance Act 2012 – s49</i></p> <ul style="list-style-type: none"> <li>Judge.</li> </ul> <p><b>Type 1 Intelligence Warrants</b> <i>Intelligence and Security Act 2017 – ss58-59</i></p> <ul style="list-style-type: none"> <li>Issued jointly be the authorising Minister and a Commissioner of Intelligence Warrants.</li> </ul>	<p><b>Interception and Examination Warrant</b> <i>Investigatory Powers Act 2016 – ss19 and 23</i></p> <ul style="list-style-type: none"> <li>Secretary of State and Judicial Commissioner.</li> </ul> <p><b>General Warrant</b> <i>Intelligence Services Act 1994 – s5</i></p> <ul style="list-style-type: none"> <li>Secretary of State.</li> </ul>	<p><b>Order for interception of wire, oral, or electronic communication</b> <i>Wiretap Act – s2516</i></p> <ul style="list-style-type: none"> <li>Application to federal court judges of district courts, or authorised judges of State courts with general criminal jurisdiction with approval of a relevant Attorney.</li> </ul> <p><b>Required disclosure of wire or electronic communications</b> <i>Stored Communications Act – s2711</i></p> <ul style="list-style-type: none"> <li>Authorised by a court of competent jurisdiction, including any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals, or a court of general criminal jurisdiction of a State authorised by the law of that State to issue search warrants.</li> </ul>

Applicant	<p><b>Australia</b></p> <p><b>Interception Warrant (ASIO)</b> TIA Act- s9, s9A</p> <ul style="list-style-type: none"> <li>• The Director-General of Security.</li> </ul> <p><b>Interception Warrant</b> TIA Act- s39</p> <ul style="list-style-type: none"> <li>• Authorised officers of interception agencies.</li> </ul> <p><b>Stored Communications Warrant</b> TIA Act- s110</p> <ul style="list-style-type: none"> <li>• Authorised officers of criminal law enforcement agencies.</li> </ul>	<p><b>Canada</b></p> <p><b>Interception Authorisation</b> <i>Criminal Code Act – s186</i></p> <ul style="list-style-type: none"> <li>• A peace officer or a public officer who has been appointed or designated to administer or enforce any federal or provincial law.</li> </ul> <p><b>Interception Warrant and Measures to reduce threats to security of Canada</b> <i>Canadian Security Intelligence Service Act – s21</i></p> <ul style="list-style-type: none"> <li>• Director or any employee designated by the Minister.</li> </ul>	<p><b>New Zealand</b></p> <p><b>Surveillance Device Warrant</b> <i>Search and Surveillance Act 2012 – s49</i></p> <ul style="list-style-type: none"> <li>• Law enforcement officers.</li> </ul> <p><b>Type 1 Intelligence Warrants</b> <i>Intelligence and Security Act 2017 – ss58-59</i></p> <ul style="list-style-type: none"> <li>• Intelligence and Security Agencies.</li> </ul>	<p><b>United Kingdom</b></p> <p><b>Interception and Examination Warrant</b> <i>Investigatory Powers Act 2016 – s18</i></p> <ul style="list-style-type: none"> <li>• Heads of the intelligence agencies, the National Crime Agency, police services, Revenue and Customs, and the Chief of Defence Intelligence.</li> </ul> <p><b>General Warrant</b> <i>Intelligence Services Act 1994 – s5</i></p> <ul style="list-style-type: none"> <li>• Security Service, Intelligence Service or GCHQ.</li> </ul>	<p><b>United States</b></p> <p><b>Order for interception of wire, oral, or electronic communication</b> <i>Wiretap Act – ss2516 and 2518</i></p> <ul style="list-style-type: none"> <li>• An investigative or law enforcement officer (authorised by Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division or National Security Division, or the principal prosecuting attorney of any State, or any attorney for the Government).</li> </ul> <p><b>Required disclosure of wire or electronic communications</b> <i>Stored Communications Act – s2703</i></p> <ul style="list-style-type: none"> <li>• A 'government entity' being a department or agency of the US or any State or political subdivision thereof.</li> </ul>
-----------	--	---	--	---	--

Threshold	Australia	Canada	New Zealand	United Kingdom	United States
	<p><b>Interception Warrant (ASIO)</b> TIA Act- s9</p> <ul style="list-style-type: none"> <li>The telecommunications service is being used or is likely to be used by a person engaged in, reasonable suspected of being engaged in, or reasonably suspected of being likely to be engaged in activities prejudicial to security.</li> <li>Interception will or is likely to assist ASIO in carrying out its function of obtaining intelligence relating to security.</li> </ul> <p><b>Interception Warrant law enforcement</b> TIA Act- s46</p> <ul style="list-style-type: none"> <li>An officer must suspect on reasonable grounds that a person is using, or is likely to use, a telecommunications service.</li> <li>Intercepting communications would be likely to assist in an investigation of a 7 year offence.</li> </ul> <p><b>Stored Communications Warrant</b> TIA Act- s116</p> <ul style="list-style-type: none"> <li>Reasonable grounds to suspect that a carrier holds stored communications that the person has made, or that another person has made and for which the first person is the intended recipient.</li> <li>Information obtained by accessing stored communications would be likely to assist in an investigation by the agency of a 3 year offence.</li> </ul>	<p><b>Interception Authorisation</b> <i>Criminal Code Act – s186</i></p> <ul style="list-style-type: none"> <li>In the best interests of the administration of justice.</li> <li>Other investigative procedures have been tried/failed, or are unlikely to succeed, or the urgency would be impractical to investigate using other methods.</li> <li>These additional requirements are exempted for criminal organisations and terrorism offences.</li> </ul> <p><b>Interception Warrant and measures to reduce threats to security of Canada</b> <i>Canadian Security Intelligence Service Act – s21</i></p> <ul style="list-style-type: none"> <li>Required to enable the Service to investigate, within or outside Canada, a threat to the security of Canada or to conduct its functions in respect of collection of information concerning foreign states and persons.</li> </ul>	<p><b>Surveillance Device Warrant</b> <i>Search and Surveillance Act 2012 – s49</i></p> <ul style="list-style-type: none"> <li>Reasonable grounds: <ul style="list-style-type: none"> <li>to suspect that an offence, punishable by a term of imprisonment of 7 years or more, has been committed, or is being committed, or will be committed, and</li> <li>to believe that the proposed use of the surveillance device will obtain information that is evidential material in respect of the offence.</li> </ul> </li> </ul> <p><b>Type 1 Intelligence Warrants</b> <i>Intelligence and Security Act 2017 – ss58-59</i></p> <ul style="list-style-type: none"> <li>Necessary to contribute to the protection of national security and identifies, enables the assessment of, or protects against particular harms.</li> <li>Will contribute to the international relations and economic well-being of New Zealand and there are reasonable grounds to suspect activity relates to foreign persons, organisations, government or terrorist entities.</li> </ul>	<p><b>Interception and Examination Warrant</b> <i>Investigatory Powers Act 2016 – s19-20</i></p> <ul style="list-style-type: none"> <li>Necessary in the interests of national security, for the purpose of preventing or detecting serious crime, or the economic well-being of the UK so far as those interests are also relevant to the interests of national security.</li> <li>Conduct authorised is proportionate to what is sought to be achieved by that conduct.</li> </ul> <p>Where <i>serious crime</i> means:</p> <ul style="list-style-type: none"> <li>Reasonably expected to be sentenced to imprisonment for a term of 3 years or more.</li> <li>The conduct involves the use of violence, results in substantial financial gain or is conducted by a large number of persons in pursuit of a common purpose.</li> </ul> <p><b>General Warrant</b> <i>Intelligence Services Act 1994 – s5</i></p> <ul style="list-style-type: none"> <li>Necessary for the action to be taken for the purpose of assisting the agency in carrying out any of its legislated functions.</li> <li>The taking of the action is proportionate to what the action seeks to achieve.</li> <li>Satisfactory arrangements are in force with respect to the disclosure of information obtained under the warrant.</li> </ul>	<p><b>Order for interception of wire, oral, or electronic communication</b> <i>Wiretap Act – s2518</i></p> <ul style="list-style-type: none"> <li>Probable cause for believing an individual is committing, has committed or is about to commit certain offences, including an offence punishable by death or imprisonment for more than 12 months for various offences including espionage, kidnapping, treason, or any offence which involves murder, robbery or extortion.</li> <li>Probable cause for believing particular communications concerning that offence will be obtained through interception.</li> <li>Normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be dangerous.</li> </ul> <p><b>Required disclosure of wire or electronic communications</b> <i>Stored Communications Act – s2703</i></p> <ul style="list-style-type: none"> <li>Reasonable grounds to believe information likely to be obtained is relevant and material to any ongoing criminal investigation.</li> </ul>

# Computer access

	Australia	Canada	New Zealand	United Kingdom	United States
Prohibition	<p><i>Criminal Code Act 1995</i> – Part 10.7</p> <ul style="list-style-type: none"> <li>• Range of criminal offences for unlawfully accessing or interfering with a computer.</li> </ul>	<p><i>Criminal Code Act</i> – ss 342.1 and 430</p> <ul style="list-style-type: none"> <li>• Offence to obtain, directly or indirectly, any computer service.</li> <li>• Offence to, by means of an electromagnetic, acoustic, mechanical or other device, intercept or cause to be intercepted, directly or indirectly, any function of a computer system.</li> <li>• Offence to destroy, alter or render meaningless, useless or ineffective, computer data.</li> <li>• Offence to obstruct, interrupt or interfere with the lawful use of computer data.</li> </ul>	<p><i>Crimes Act 1961</i> – s250</p> <ul style="list-style-type: none"> <li>• Offence to intentionally or recklessly, and without authorisation, damage, delete, modify, or otherwise interfere with or impair any data or software in any computer system.</li> <li>• Offence to intentionally or recklessly, and without authorisation, cause any data or software in any computer system to be damaged, deleted, modified or otherwise interfered with or impaired.</li> </ul>	<p><i>Computer Misuse Act 1990</i> – s1</p> <ul style="list-style-type: none"> <li>• Offence to cause a computer to perform a function with intent to secure access to any program or data held in any computer or to enable any such access to be secured.</li> </ul>	<p><i>United States Constitution</i> Fourth Amendment</p> <ul style="list-style-type: none"> <li>• Provides protection against unreasonable searches or seizures.</li> </ul>
Warrant(s)	<p><b>Computer Access Warrant</b> <i>Australian Security Intelligence Organisation Act 1979</i> (ASIO Act) – s25A</p> <ul style="list-style-type: none"> <li>• Entering premises for the purpose of doing the things mentioned in the warrant.</li> <li>• Remotely and covertly accessing data held on a computer to gather data that is relevant to the security matter.</li> <li>• Adding, copying, deleting or altering data in the computer, if necessary to achieve the purpose.</li> </ul> <p><b>Computer Access Warrant</b> <i>Surveillance Devices Act 2004</i> (SD Act) – s27E</p> <ul style="list-style-type: none"> <li>• Entering premises for the purpose of doing the things mentioned in the warrant.</li> <li>• Remotely and covertly accessing data held on a computer to gather evidence in criminal investigations.</li> <li>• Adding, copying, deleting or altering data in the computer if necessary to achieve the purpose.</li> </ul>	<p><b>Interception Warrant</b> As detailed above. Search Warrant <i>Criminal Code Act</i> – s487</p> <ul style="list-style-type: none"> <li>• Search of the building, receptacle or place and seizure of the item.</li> <li>• Operation of computer system and copying equipment to search for data contained in or available to the computer system.</li> <li>• Reproduction and seizure of information for examination.</li> </ul>	<p><b>Search Warrant</b> <i>Search and Surveillance Act 2012</i> – ss98 and 111</p> <ul style="list-style-type: none"> <li>• To enter and search the place, vehicle, or other thing that the person is authorised to enter and search, and any item or items found in that place or vehicle or thing, at any time that is reasonable.</li> <li>• To use any reasonable measures to access a computer system or other data storage device located (in whole or in part) at the place, vehicle, or other thing if any intangible that is the subject of the search may be in that computer system or other device.</li> <li>• If remote access is warranted – use reasonable measures to gain access to a thing and copy intangible material.</li> </ul>	<p><b>General Warrant</b> As detailed above. <b>Targeted Equipment Interference Warrant</b> <i>Investigatory Powers Act 2016</i> – s99</p> <ul style="list-style-type: none"> <li>• Authorises or requires the person to secure interference with any equipment for the purpose of obtaining: <ul style="list-style-type: none"> <li>– communications (s135),</li> <li>– equipment data (s100), or</li> <li>– any other information.</li> </ul> </li> </ul>	<p><b>Search Warrant for Electronic Data</b> Federal Rules of Criminal Procedure, Rule 41 Search and Seizure</p> <ul style="list-style-type: none"> <li>• Persons or property subject to search or seizure. A warrant may be issued for any of the following: <ul style="list-style-type: none"> <li>– evidence of a crime,</li> <li>– contraband, fruits of crime or other items illegally possessed,</li> <li>– property designed for use, intended for use, or use in committing a crime, or</li> <li>– a person to be arrested or a person who is unlawfully restrained.</li> </ul> </li> <li>• A warrant may authorise remote access to search electronic storage media and to seize or copy electronically stored information.</li> </ul>

	Australia	Canada	New Zealand	United Kingdom	United States
Definition of computer / equipment	<p><b>Computer Access Warrant</b> ASIO Act SD Act – s4 – s6</p> <ul style="list-style-type: none"> <li>• Computer means all or part of: <ul style="list-style-type: none"> <li>– one or more computers,</li> <li>– one or more computer systems,</li> <li>– one or more computer networks, or</li> <li>– any combination of the above.</li> </ul> </li> </ul>	<p><b>Interception Warrant</b> As detailed above.</p> <p><b>Search Warrant</b> <i>Criminal Code Act – s342.1</i></p> <ul style="list-style-type: none"> <li>• Computer system means a device that, or a group of interconnected or related devices one of more of which, contain computer programs or other computer data and which, by means of computer programs, performs logic and control and any other function.</li> <li>• Computer data means representations, including signs, symbols or signals, which are in a form suitable for processing in a computer system.</li> </ul>	<p><b>Search Warrant</b> <i>Search and Surveillance Act 2012 – s3</i></p> <ul style="list-style-type: none"> <li>• Computer system means a computer, 2 or more interconnected computers, any communication links between computers, or 2 or more interconnected computers combined with any communication links between computers.</li> </ul>	<p><b>Targeted Equipment Interference Warrant</b> <i>Investigatory Powers Act 2016 – s101</i></p> <p>Targeted equipment interference may relate to:</p> <ul style="list-style-type: none"> <li>• equipment belonging to or used in the possession of: <ul style="list-style-type: none"> <li>– a particular person or organisation,</li> <li>– a group of persons who share a common purpose or who (may) carry on a particular activity, or</li> <li>– more than one person or organisation, where interference is for the purpose of a single investigation/operation,</li> <li>– equipment in a particular location or more than one location, where interference is for the purpose of a single investigation/operation,</li> <li>– equipment which is being, or may be, used for the purposes of a particular activity/activities, or</li> <li>– equipment which is being, or may be, used to train personnel, test, maintain or develop capabilities relating to interference with equipment.</li> </ul> </li> </ul>	<p>Nil</p>
Issuing authority	<p><b>Computer Access Warrant</b> ASIO Act – s25A</p> <ul style="list-style-type: none"> <li>• The Attorney-General.</li> </ul> <p><b>Computer Access Warrant</b> SD Act – s27A</p> <ul style="list-style-type: none"> <li>• Eligible Judges and nominated AAT members.</li> </ul>	<p><b>Interception Warrant</b> As detailed above.</p> <p><b>Search Warrant</b> <i>Criminal Code Act – s487</i></p> <ul style="list-style-type: none"> <li>• Provincial court judge, a judge of a superior court of criminal jurisdiction or a judge as defined in section 552.</li> </ul>	<p><b>Search Warrant</b> <i>Search and Surveillance Act 2012 – s108</i></p> <ul style="list-style-type: none"> <li>• Justice of the Peace, Community Magistrate, Registrar, Deputy Registrar or other person authorised by the Attorney-General to act as an issuing officer.</li> </ul>	<p><b>Targeted Equipment Interference Warrant</b> <i>Investigatory Powers Act 2016 – ss 102 and 108</i></p> <ul style="list-style-type: none"> <li>• Secretary of State and Judicial Commissioner.</li> </ul>	<p><b>Search Warrant for Electronic Data</b> <i>Federal Rules of Criminal Procedure, Rule 41 Search and Seizure</i></p> <ul style="list-style-type: none"> <li>• A magistrate judge.</li> </ul>

	Australia	Canada	New Zealand	United Kingdom	United States
Applicant	<p><b>Computer Access Warrant</b> ASIO Act – s25A</p> <ul style="list-style-type: none"> <li>• The Director-General of Security.</li> </ul> <p><b>Computer Access Warrant</b> SD Act – 27A</p> <ul style="list-style-type: none"> <li>• Law enforcement officer.</li> </ul>	<p><b>Interception Warrant</b> As detailed above.</p> <p><b>Search Warrant</b> <i>Criminal Code Act – s487</i></p> <ul style="list-style-type: none"> <li>• A peace officer or a public officer who has been appointed or designated to administer or enforce any federal or provincial law.</li> </ul>	<p><b>Search Warrant</b> <i>Search and Surveillance Act 2012 – s97</i></p> <ul style="list-style-type: none"> <li>• Constable.</li> <li>• Any other person authorised by the Act or Schedule 2.</li> </ul>	<p><b>Targeted Equipment Interference Warrant</b> <i>Investigatory Powers Act 2016 – s 102</i></p> <ul style="list-style-type: none"> <li>• On behalf of the head of an intelligence service by a person holding office under the Crown.</li> </ul>	<p><b>Search Warrant for Electronic Data</b> <i>Federal Rules of Criminal Procedure, Rule 41 Search and Seizure</i></p> <ul style="list-style-type: none"> <li>• A federal law enforcement officer or an attorney.</li> </ul>
Threshold	<p><b>Computer Access Warrant</b> ASIO Act – s25A</p> <ul style="list-style-type: none"> <li>• Reasonable grounds for believing that access to data held in a computer will substantially assist the collection of intelligence in respect of a matter that is important in relation to security.</li> </ul> <p><b>Computer Access Warrant</b> SD Act – s27A</p> <ul style="list-style-type: none"> <li>• Reasonable grounds to suspect that a 3 year offence is being committed and investigated.</li> <li>• Accessing data held in a computer is necessary for the purpose of enabling evidence to be obtained about the offence, or the offenders.</li> </ul>	<p><b>Interception Warrant</b> As detailed above.</p> <p><b>Search Warrant</b> <i>Criminal Code Act – s487</i></p> <ul style="list-style-type: none"> <li>• Reasonable grounds to believe: <ul style="list-style-type: none"> <li>– any offence against the Criminal Code or any other Act of Parliament has been committed, and</li> <li>– the actions will afford evidence with respect to investigation of the offence.</li> </ul> </li> </ul>	<p><b>Search Warrant</b> <i>Search and Surveillance Act 2012 – ss6 and 103</i></p> <ul style="list-style-type: none"> <li>• Reasonable grounds: <ul style="list-style-type: none"> <li>– to suspect that an offence specified in the application and punishable by imprisonment has been committed, or is being committed, or will be committed, and</li> <li>– to believe that the search will find evidential material in respect of the offence in or on the place, vehicle or other thing specified in the application.</li> </ul> </li> <li>• If the warrant authorises remote access search of a thing – the issuing officer must be satisfied that the thing is not located at a physical address that a person can enter and search.</li> </ul>	<p><b>Targeted Equipment Interference Warrant</b> <i>Investigatory Powers Act 2016 – s 102</i></p> <ul style="list-style-type: none"> <li>• Necessary on the interests of national security, preventing or detecting serious crime, or in the interests of economic well-being of the United Kingdom.</li> <li>• Proportionate to what is sought to be achieved by that conduct.</li> <li>• Satisfactory arrangements made for the purposes of sections 129 and 130 (safeguards relating to disclosure etc.) are in force in relation to the warrant.</li> </ul>	<p><b>Search Warrant for Electronic Data</b> <i>Federal Rules of Criminal Procedure, Rule 41 Search and Seizure</i></p> <ul style="list-style-type: none"> <li>• Must establish probable cause to issue the warrant, meaning: <ul style="list-style-type: none"> <li>– there is a fair probability that contraband or evidence of a crime will be found in the place to be searched<sup>106</sup>.</li> </ul> </li> <li>• May only authorise remote access when the district in which the media or information is located is not known because of the use of technology such as anonymizing software, or if the media to be searched are protected computers that have been damaged without authorisation, and they are located in many districts.</li> </ul>

106 Illinois v. Gates, 462 U.S. 213, 238 (1983).

# Surveillance devices

	Australia	Canada	New Zealand	United Kingdom	United States
Prohibition	The Commonwealth does not generally prohibit the use of surveillance devices. This is necessarily governed by state and territory legislation, which each have legislation that prohibits people from using certain surveillance devices in certain circumstances.	<i>Charter of Rights and Freedoms</i> – s8 <ul style="list-style-type: none"> <li>Everyone has the right to be secure against unreasonable search or seizure.</li> </ul>	<i>New Zealand Bill of Rights Act 1990</i> – s21 <p>Everyone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise.</p>	<i>Human Rights Act 1998</i> <p>Everyone has the right to respect for his private and family life, his home and his correspondence.</p>	<i>United States Constitution</i> Fourth Amendment <p>Provides protection against unreasonable searches or seizures.</p>
Warrant(s)	<p><b>Surveillance Device Warrant</b> ASIO Act – s26B</p> <ul style="list-style-type: none"> <li>Installation, use and maintenance of a surveillance device.</li> <li>Entry onto premises for the purpose of installing the device.</li> </ul> <p><b>Surveillance Device Warrant</b> SD Act – s18</p> <ul style="list-style-type: none"> <li>Installation, use and maintenance of a surveillance device.</li> <li>Entry onto premises for the purpose of installing the device.</li> </ul>	<p><b>Interception Warrant</b> As detailed above.</p> <p><b>General warrant</b> <i>Criminal Code Act</i> – s487.01</p> <ul style="list-style-type: none"> <li>Use any device or investigative technique or procedure that would, if not authorised, constitute an unreasonable search or seizure.</li> <li>Observe, by means of a television camera or other similar electronic device, any person who is engaged in activity in circumstances in which the person has a reasonable expectation of privacy.</li> </ul> <p><b>Tracking warrant</b> <i>Criminal Code Act</i> – s492.1</p> <ul style="list-style-type: none"> <li>Obtain tracking data about a transaction, thing, vehicle or individual by means of a tracking device.</li> <li>Install, activate, use, maintain, monitor and remove the tracking device, including covertly.</li> </ul>	<p><b>Surveillance Device Warrant and Type 1 Intelligence Warrant</b> As detailed above.</p>	<p><b>General Warrant</b> As detailed above.</p> <p><b>Directed surveillance</b> <i>Regulation of Investigatory Powers Act 2000</i> – s28</p> <ul style="list-style-type: none"> <li>Conducting covert but not intrusive surveillance to obtain private information about a person for the purposes of a specific investigation or operation.</li> <li>Surveillance is not intrusive if it is carried out: <ul style="list-style-type: none"> <li>by means only of a surveillance device designed for the purpose of providing information about the location of a vehicle, or</li> <li>by means of a surveillance device without that device being present on the premises or vehicle unless it provides the same quality and detail of information as a device present on the premises or vehicle.</li> </ul> </li> </ul>	<p><b>Order for interception of wire, oral, or electronic communication</b> As detailed above.</p>



	Australia	Canada	New Zealand	United Kingdom	United States
Issuing authority	<p><b>Surveillance Device Warrant</b> ASIO Act – s26</p> <ul style="list-style-type: none"> <li>• The Attorney-General</li> </ul> <p><b>Surveillance Device Warrant</b> SD Act – s14</p> <ul style="list-style-type: none"> <li>• Eligible Judges and nominated AAT members.</li> </ul>	<p><b>Interception Warrant</b> As detailed above.</p> <p><b>General warrant</b> <i>Criminal Code Act – s487.01</i></p> <ul style="list-style-type: none"> <li>• Provincial court judge, a judge of a superior court of criminal jurisdiction or a judge.</li> </ul> <p><b>Tracking warrant</b> <i>Criminal Code Act – s492.1</i></p> <ul style="list-style-type: none"> <li>• A Justice of the peace or a provincial court judge, or judge.</li> </ul>	Nil	<p><b>Intrusive surveillance</b> <i>Regulation of Investigatory Powers Act 2000 – s32</i></p> <ul style="list-style-type: none"> <li>• Obtaining private information about a person in relation to anything taking place on any residential premises or in any private vehicle through covert and intrusive use of a surveillance device.</li> </ul>	Nil
Applicant	<p><b>Surveillance Device Warrant</b> ASIO Act – s26</p> <ul style="list-style-type: none"> <li>• The Director-General of Security.</li> </ul> <p><b>Surveillance Device Warrant</b> SD Act – s14</p> <ul style="list-style-type: none"> <li>• A law enforcement officer.</li> </ul>	<p><b>Interception Warrant</b> As detailed above.</p> <p><b>General warrant</b> <i>Criminal Code Act – s487.01</i></p> <ul style="list-style-type: none"> <li>• Peace officer.</li> </ul> <p><b>Tracking warrant</b> <i>Criminal Code Act – s492.1</i></p> <ul style="list-style-type: none"> <li>• Peace officer, or public officer appointed or designated to administer or enforce a federal or provincial law and whose duties include the enforcement of the Criminal Code Act or any other Act.</li> </ul>	Nil	<p><b>Directed surveillance</b> <i>Regulation of Investigatory Powers Act 2000 – s30</i></p> <ul style="list-style-type: none"> <li>• Designated persons of particular offices, ranks or positions with relevant public authorities.</li> </ul> <p><b>Intrusive surveillance</b> <i>Regulation of Investigatory Powers Act 2000 – s32</i></p> <ul style="list-style-type: none"> <li>• Secretary of State and senior authorising officers.</li> </ul>	Nil

	Australia	Canada	New Zealand	United Kingdom	United States
Threshold	<p><b>Surveillance Device Warrant</b> ASIO Act – s26</p> <ul style="list-style-type: none"> <li>• The person is engaged in or is reasonably suspected of being engaged in, or of being likely to engage in activities prejudicial to security.</li> <li>• Use of a surveillance device by ASIO will assist in carrying out its function of obtaining intelligence relevant to security.</li> </ul> <p><b>Surveillance Device Warrant</b> SD Act – s14</p> <ul style="list-style-type: none"> <li>• Reasonable grounds for suspecting that a 3 year offence is being committed and investigated.</li> <li>• Use of a surveillance device is necessary for the purpose of enabling evidence to be obtained about the offence, or the offenders.</li> </ul>	<p><b>Interception Warrant</b> As detailed above. General warrant <i>Criminal Code Act – s487.01</i></p> <ul style="list-style-type: none"> <li>• It is in the best interests of the administration of justice to issue the warrant.</li> <li>• There is no other provision would provide for a warrant, authorisation or order permitting the activity.</li> <li>• Reasonable grounds: <ul style="list-style-type: none"> <li>– to believe any offence against the Criminal Code or any other Act of Parliament has been committed, and</li> <li>– to believe the actions will afford evidence with respect to investigation of the offence.</li> </ul> </li> </ul> <p><b>Tracking warrant</b> <i>Criminal Code Act – s492.1</i></p> <ul style="list-style-type: none"> <li>• Reasonable grounds to suspect that: <ul style="list-style-type: none"> <li>– an offence has been or will be committed against the Criminal Code or any other Act of Parliament, and</li> <li>– tracking the location of a transaction / the location or movement of a thing / an individual's movement by identifying the location of a thing will assist in the investigation of the offence.</li> </ul> </li> </ul>	Nil	<p><b>Directed surveillance</b> <i>Regulation of Investigatory Powers Act 2000 – s30</i></p> <ul style="list-style-type: none"> <li>• Necessary: <ul style="list-style-type: none"> <li>– in the interests of national security,</li> <li>– for the purposes of preventing or detecting crime or of preventing disorder,</li> <li>– in the interests of the economic well-being of the UK,</li> <li>– in the interests of public safety,</li> <li>– for the purpose of protecting public health,</li> <li>– for the purpose of assessing or collecting any tax, duty, levy, contribution or charge, or</li> <li>– for a purpose specified by an order made by the Secretary of State.</li> </ul> </li> </ul> <p><b>Intrusive surveillance</b> <i>Regulation of Investigatory Powers Act 2000 – s32</i></p> <ul style="list-style-type: none"> <li>• Necessary: <ul style="list-style-type: none"> <li>– in the interests of national security,</li> <li>– for the purposes of preventing or detecting crime or of preventing disorder, or</li> <li>– in the interests of the economic well-being of the UK.</li> </ul> </li> </ul>	Nil

# Telecommunications data

	Australia	Canada	New Zealand	United Kingdom	United States
Prohibition	<p><i>Telecommunications Act 1997</i> – s276-278</p> <ul style="list-style-type: none"> <li>It is an offence for certain participants in the telecommunications industry to use or disclose the contents of a person's communications, carriage services supplied by carriers and carriage service providers and the affairs or personal particulars of persons.</li> </ul>	<p><i>Charter of Rights and Freedoms</i> – s8</p> <ul style="list-style-type: none"> <li>Everyone has the right to be secure against unreasonable search or seizure.</li> </ul>	Nil	<p><i>Investigatory Powers Act 2016</i> – s11</p> <ul style="list-style-type: none"> <li>Knowingly or recklessly obtaining communications data from a telecommunications operator or a postal operator is an offence.</li> </ul>	<p><i>United States Code, Title 18: Crimes and Criminal Procedure</i>, Chapter 206, Pen Registers and Trap/Trace Devices (USC Chapter 206) – s3121</p> <ul style="list-style-type: none"> <li>Use and installation of pen registers and trap/trace devices is an offence.</li> </ul>
Warrants / Authorisations	<p><b>Telecommunications data authorisation (ASIO)</b></p> <p>TIA Act– ss175 and 176</p> <ul style="list-style-type: none"> <li>Authorises a carrier to disclose prospective or historical telecommunications data.</li> </ul> <p><b>Telecommunication law enforcement</b></p> <p>TIA Act– ss178, 178A, 179 and 180</p> <ul style="list-style-type: none"> <li>Allows agencies to authorise carriers to disclose prospective or historical telecommunications data.</li> </ul>	<p><b>Interception Warrant</b></p> <p>As detailed above.</p> <p><b>Production order – transmission data or tracking data</b></p> <p><i>Criminal Code Act</i> – ss487.016 and 487.017</p> <ul style="list-style-type: none"> <li>Order a person to prepare and produce a document containing transmission data or tracking data that is in their possession or control when they receive the order.</li> </ul> <p><b>Warrant for transmission data recorder</b></p> <p><i>Criminal Code Act</i> – s492.2</p> <ul style="list-style-type: none"> <li>Obtain transmission data by means of a transmission data recorder.</li> <li>Install, activate, use, maintain, monitor and remove the transmission data recorder, including covertly.</li> </ul>	Nil	<p><b>General Warrant</b></p> <p>As detailed above.</p> <p><b>Authorisations for obtaining communications data</b></p> <p><i>Investigatory Powers Act 2016</i> – s61</p> <ul style="list-style-type: none"> <li>Obtaining communications data from any person that relates to: <ul style="list-style-type: none"> <li>a telecommunication system, or</li> <li>data derived from a telecommunication system.</li> </ul> </li> <li>Does not authorise conduct consisting in the interception of communications in the course of their transmission by means of a telecommunication system.</li> </ul> <p><b>Bulk acquisition warrant</b></p> <p><i>Investigatory Powers Act 2016</i> – s158</p> <ul style="list-style-type: none"> <li>Requiring a telecommunications operator to disclose any communications data in their possession or obtain any data not in their possession.</li> </ul>	<p><b>Order for use of a Pen Registers or Trap/Trace Device</b></p> <p><i>USC Chapter 206</i> – ss3122-3123</p> <ul style="list-style-type: none"> <li>Installation and use of a pen register or a trap and trace device.</li> <li>Used to compel the disclosure of metadata – dialling, routing, addressing, and signalling data – regarding an electronic communication.</li> </ul>

Definition(s)	Australia	Canada	New Zealand	United Kingdom	United States
	<p>Nil</p>	<p><b>Interception Warrant</b> As detailed above.</p> <p><b>Production order – transmission data or tracking data</b> <i>Criminal Code Act – ss487.01</i></p> <ul style="list-style-type: none"> <li>• <i>Transmission data</i> means data that: <ul style="list-style-type: none"> <li>– relates to the telecommunication functions of dialling, routing, addressing or signalling,</li> <li>– is transmitted to identify, activate or configure a device in order to establish or maintain access to a telecommunication service for the purpose of enabling a communication, or is generated during the creation, transmission or reception of a communication, and</li> <li>– does not reveal the substance, meaning or purpose of the communication.</li> </ul> </li> <li>• <i>tracking data</i> means data that relates to the location of a transaction, individual or thing</li> </ul> <p><b>Warrant for transmission data recorder</b> <i>Criminal Code Act – s487.01</i></p> <ul style="list-style-type: none"> <li>• <i>Transmission data</i> means data that: <ul style="list-style-type: none"> <li>– relates to the telecommunication functions of dialling, routing, addressing or signalling,</li> <li>– is transmitted to identify, activate or configure a device in order to establish or maintain access to a telecommunication service for the purpose of enabling a communication, or is generated during the creation, transmission or reception of a communication, and</li> <li>– does not reveal the substance, meaning or purpose of the communication.</li> </ul> </li> </ul>	<p>Nil</p>	<p><b>Authorisations for obtaining communications data and bulk acquisition warrant</b> <i>Investigatory Powers Act 2016 – s261</i></p> <ul style="list-style-type: none"> <li>• <i>Communications data</i> in relation to a telecommunications operator, service or system means data: <ul style="list-style-type: none"> <li>– which is, or is capable of, being held or obtained by, or on behalf of, a telecommunications operator,</li> <li>– which is available directly from a telecommunication system and is comprised in, included as part of, or logically associated with a communication for the purposes of a telecommunication system, or</li> <li>– is about the architecture of a telecommunication system and not about a specific person.</li> </ul> </li> </ul>	<p><b>Order for use of a Pen Registers or Trap/Trace Device</b> USC Chapter 206 – s3127</p> <ul style="list-style-type: none"> <li>• <i>Pen register</i> means a device or process which records or decodes dialling, routing, addressing or signalling information transmitted by wire or electronic communication, provided that such information shall not include the contents of any communication.</li> <li>• <i>Trap and trace device</i> means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialling, routing, addressing, and signalling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.</li> </ul>

	Australia	Canada	New Zealand	United Kingdom	United States
Issuing authority	<p><b>Telecommunications data authorisation (ASIO)</b> TIA Act— ss175 and 176</p> <ul style="list-style-type: none"> <li>• Director-General of Security, Deputy Director-General or Security or ASIO employee or affiliate in a position of SES Band 2 or above.</li> </ul> <p><b>Telecommunications data authorisation</b> TIA Act— ss178, 178A, 179 and 180</p> <ul style="list-style-type: none"> <li>• Authorised officer of an enforcement agency.</li> </ul>	<p><b>Interception Warrant</b> As detailed above.</p> <p><b>Production order – transmission data or tracking data</b> <i>Criminal Code Act – ss487.016 and 487.017</i></p> <ul style="list-style-type: none"> <li>• Provincial court judge, a judge of a superior court of criminal jurisdiction or a judge.</li> </ul> <p><b>Warrant for transmission data recorder</b> <i>Criminal Code Act – s492.2</i></p> <ul style="list-style-type: none"> <li>• Provincial court judge, a judge of a superior court of criminal jurisdiction or a judge.</li> </ul>	Nil	<p><b>Authorisations for obtaining communications data</b> <i>Investigatory Powers Act 2016 – s61</i> Investigatory Powers Commissioner. Designated Senior Officer.</p> <p><b>Bulk acquisition warrant</b> <i>Investigatory Powers Act 2016 – s158</i></p> <ul style="list-style-type: none"> <li>• Secretary of State.</li> </ul>	<p><b>Order for use of a Pen Registers or Trap/Trace Device</b> USC Chapter 206 – ss3122-3123</p> <ul style="list-style-type: none"> <li>• Any court of competent jurisdiction.</li> </ul>
Applicant	<p><b>Telecommunications data authorisation (ASIO)</b> TIA Act— s175 and 176 ASIO officer.</p> <p><b>Telecommunications data authorisation</b> TIA Act— s178, 178A, 179 and 180</p> <ul style="list-style-type: none"> <li>• Officer of an enforcement agency.</li> </ul>	<p><b>Interception Warrant</b> As detailed above.</p> <p><b>Production order – transmission data or tracking data</b> <i>Criminal Code Act – ss487.016 and 487.017</i></p> <ul style="list-style-type: none"> <li>• Peace officer or public officer.</li> </ul> <p><b>Warrant for transmission data recorder</b> <i>Criminal Code Act – s492.2</i></p> <ul style="list-style-type: none"> <li>• Peace officer or public officer.</li> </ul>	Nil	<p><b>Authorisations for obtaining communications data</b> <i>Investigatory Powers Act 2016 – s61</i></p> <ul style="list-style-type: none"> <li>• Designated senior officer of a relevant public authority.</li> </ul> <p><b>Bulk acquisition warrant</b> <i>Investigatory Powers Act 2016 – s158</i></p> <ul style="list-style-type: none"> <li>• Head of an intelligence service.</li> </ul>	<p><b>Order for use of a Pen Registers or Trap/Trace Device</b> USC Chapter 206 – s3122</p> <ul style="list-style-type: none"> <li>• Federal attorneys (i.e. prosecutors) and state investigative or law enforcement officers (unless prohibited by state law).</li> </ul>

	Australia	Canada	New Zealand	United Kingdom	United States
Threshold	<p><b>Telecommunications data authorisation (ASIO)</b> TIA Act – s175 and 176</p> <ul style="list-style-type: none"> <li>Where satisfied that the disclosure would be in connection with the performance by ASIO of its functions.</li> </ul> <p><b>Telecommunications data authorisation</b> TIA Act – s178, 178A, 179 and 180</p> <ul style="list-style-type: none"> <li>Historical data – where reasonably necessary for the enforcement of the criminal law, enforcement of a law imposing a pecuniary penalty, protection of public revenue, or the location of a missing person.</li> <li>Prospective data – where reasonably necessary for the investigation of a 3 year offence.</li> </ul>	<p><b>Interception Warrant</b> As detailed above.</p> <p><b>Production order – transmission data or tracking data</b> <i>Criminal Code Act – ss487.016 and 487.017</i></p> <ul style="list-style-type: none"> <li>Reasonable grounds to suspect: <ul style="list-style-type: none"> <li>an offence against the Criminal Code or any other Act of Parliament has been or will be committed, and</li> <li>the transmission data or tracking data is in the person's possession or control and will assist in the investigation of the offence.</li> </ul> </li> </ul> <p><b>Warrant for transmission data recorder</b> <i>Criminal Code Act – s492.2</i></p> <ul style="list-style-type: none"> <li>Reasonable grounds to suspect: <ul style="list-style-type: none"> <li>an offence against the Criminal Code or any other Act of Parliament has been or will be committed, and</li> <li>the transmission data will assist in the investigation of the offence.</li> </ul> </li> </ul>	Nil	<p><b>Authorisations for obtaining communications data</b> <i>Investigatory Powers Act 2016 – s61</i></p> <ul style="list-style-type: none"> <li>Necessary to obtain communications data for a range of circumstances, including national security, preventing serious crime and protecting public safety.</li> <li>Necessary to obtain the data: <ul style="list-style-type: none"> <li>for the purposes of a specific investigation or a specific operation, or</li> <li>for testing, maintaining or developing equipment, systems or other capabilities.</li> </ul> </li> <li>That the conduct authorised by the authorisation is proportionate to what is sought to be achieved. Where serious crime means: <ul style="list-style-type: none"> <li>An offence capable of being sentenced to imprisonment for a term of 12 months or more, or</li> <li>An offence: <ul style="list-style-type: none"> <li>by a person who is not an individual, or</li> <li>involves, as an integral part of it, the sending of a communication or a breach of a person's privacy.</li> </ul> </li> </ul> </li> </ul> <p><b>Bulk acquisition warrant</b> <i>Investigatory Powers Act 2016 – s158</i></p> <ul style="list-style-type: none"> <li>Necessary in the interests of national security, for the purpose of preventing or detecting serious crime, or in the interests of the economic well-being of the UK.</li> <li>Conduct to be authorised is proportionate to what is sought to be achieved.</li> </ul>	<p><b>Order for use of a Pen Registers or Trap/Trace Device</b> USC Chapter 206 – s3123</p> <ul style="list-style-type: none"> <li>If the court finds the applicant has certified that information likely to be obtained is relevant to an ongoing criminal investigation.</li> </ul>

# Foreign Intelligence Collection

	Australia	Canada	New Zealand	United Kingdom	United States
Prohibition	Nil	Nil	Nil	Nil	<i>Foreign Intelligence Surveillance Act of 1978</i> 50 U.S.C. ss1801-1871 <ul style="list-style-type: none"> <li>Electronic surveillance of foreign powers and agents of foreign powers is an offence.</li> </ul>
Warrant(s)	<p><b>Telecommunications service or named person warrants for collection of foreign intelligence</b></p> <p>TIA Act- ss11A and 11B</p> <ul style="list-style-type: none"> <li>Interception of communications made to or from a service, including accessing stored communications.</li> <li>Interception of communications that are being made to or from any telecommunications service that a specified person is using including stored communications.</li> <li>For the purpose of obtaining foreign intelligence relating to a matter specified</li> <li>Foreign communications warrant for collection of foreign intelligence</li> </ul> <p>TIA Act- s11C</p> <ul style="list-style-type: none"> <li>Intercept foreign communications for the purpose of obtaining foreign intelligence relating to a matter specified.</li> </ul>	<p><b>Interception Warrant</b></p> <p>As detailed above.</p> <p><b>Foreign Intelligence Authorisations</b></p> <p><i>Communications Security Establishment Act</i> – s26</p> <ul style="list-style-type: none"> <li>Gain access to a portion of the global information infrastructure.</li> <li>Acquire information on or through the global information infrastructure.</li> <li>Install, maintain, copy, distribute, search, modify, disrupt, delete or intercept anything on or through the global information infrastructure.</li> <li>Do anything reasonably necessary to maintain the covert nature of the activity.</li> </ul>	<p><b>Type 2 Intelligence Warrants</b></p> <p><i>Intelligence and Security Act 2017</i> – s60</p> <ul style="list-style-type: none"> <li>Carry out otherwise unlawful activities for the purpose of collecting information, or to do any other thing in circumstances where a Type 1 warrant is not required.</li> </ul>	<p><b>Bulk Interception Warrants</b></p> <p><i>Investigatory Powers Act 2016</i> – s136</p> <ul style="list-style-type: none"> <li>Interception of overseas-related communications, being those sent/received by individuals outside the British Islands.</li> <li>Obtaining of secondary data from such overseas-related communications.</li> <li>Selection for examination any such collected content or secondary data.</li> </ul> <p><b>Authorisation of acts outside the British Islands</b></p> <p><i>Intelligence Services Act 1994</i> – s7</p> <ul style="list-style-type: none"> <li>Doing of an act outside the British Islands which would otherwise cause the person to be liable for doing the act.</li> </ul>	<p><b>Electronic Surveillance Authorisation</b></p> <p><i>Foreign Intelligence Surveillance Act</i> – ss1801-1813</p> <ul style="list-style-type: none"> <li>Conduct electronic surveillance, being the acquisition by an electronic, mechanical or other surveillance device of the contents of any wire or radio communication.</li> <li>Communications transmitted by means of communications used exclusively between or among foreign powers.</li> <li>The acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power.</li> </ul> <p><b>Pen Registers or Trap/Trace Device for Foreign Intelligence Purposes</b></p> <p><i>Foreign Intelligence Surveillance Act</i> – ss1841-1846</p> <ul style="list-style-type: none"> <li>Use of Pen Registers or Trap/Trace Device (as above) for foreign intelligence information.</li> </ul>

	Australia	Canada	New Zealand	United Kingdom	United States
Definition(s)	<p><b>TIA Act</b> s5 Interpretation</p> <ul style="list-style-type: none"> <li>Foreign communication means a communication sent or received outside Australia.</li> <li>Foreign intelligence means intelligence about the capabilities, intentions or activities of people or organisations outside Australia.</li> </ul>	<p><b>Interception Warrant</b> As detailed above.</p> <p><b>Foreign Intelligence Authorisations</b> <i>Communications Security Establishment Act – s2</i></p> <ul style="list-style-type: none"> <li>Global information infrastructure includes electromagnetic emissions, any equipment producing such emissions, communications systems, information technology systems and networks, and any data or technical information carried on, contained in or relating to those emissions, that equipment, those systems or those networks.</li> </ul>	Nil	<p><b>Bulk interception warrants</b> <i>Investigatory Powers Act 2016 – s136 (3)</i></p> <p>"overseas-related communications" means—</p> <ol style="list-style-type: none"> <li>communications sent by individuals who are outside the British Islands, or</li> <li>communications received by individuals who are outside the British Islands.</li> </ol>	<p><b>702/703/704 Orders</b> <i>Foreign Intelligence Surveillance Act – ss1881-1881g</i></p> <ul style="list-style-type: none"> <li>702 orders: Conduct collection of foreign intelligence from non-US persons, groups or entities located outside the US.</li> <li>703 orders: Conduct electronic surveillance or acquire stored electronic communications or data within the US, of a US person outside the US.</li> <li>704 orders: Conduct collection outside the US of a US person outside the US.</li> </ul> <p><b>Electronic Surveillance Definitions</b> <i>Foreign Intelligence Surveillance Act – s 1801 –</i></p> <p>"Foreign intelligence information" means—</p> <ol style="list-style-type: none"> <li>information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against— <ol style="list-style-type: none"> <li>actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;</li> <li>sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or</li> <li>clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or</li> </ol> </li> <li>information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to— <ol style="list-style-type: none"> <li>the national defense or the security of the United States; or</li> <li>the conduct of the foreign affairs of the United States.</li> </ol> </li> </ol>



	Australia	Canada	New Zealand	United Kingdom	United States
Issuing authority	<p><b>Telecommunications service or named person warrants for collection of foreign intelligence</b></p> <p>TIA Act– ss11A and 11B</p> <ul style="list-style-type: none"> <li>The Attorney-General, on the basis of advice received from the Minister for Defence or the Minister for Foreign Affairs.</li> </ul> <p><b>Foreign communications warrant for collection of foreign intelligence</b></p> <p>TIA Act– s11C</p> <ul style="list-style-type: none"> <li>The Attorney-General, on the basis of advice received from the Minister for Defence or the Minister for Foreign Affairs.</li> </ul>	<p><b>Interception Warrant</b></p> <p>As detailed above</p> <p><b>Foreign Intelligence Authorisations</b></p> <p><i>Communications Security Establishment Act</i> – s26</p> <ul style="list-style-type: none"> <li>Application to the Minister of National Defence with approval of the Intelligence Commissioner.</li> </ul>	<p><b>Type 2 Intelligence Warrants</b></p> <p><i>Intelligence and Security Act 2017</i> – s60</p> <ul style="list-style-type: none"> <li>The authorising Minister.</li> </ul>	<p><b>Bulk Interception Warrants</b></p> <p><i>Investigatory Powers Act 2016</i> – s138</p> <ul style="list-style-type: none"> <li>Secretary of State.</li> </ul> <p><b>Authorisation of acts outside the British Islands</b></p> <p><i>Intelligence Services Act 1994</i> – s7</p> <ul style="list-style-type: none"> <li>Secretary of State.</li> </ul>	<p><b>Electronic Surveillance Authorisation</b></p> <p><i>Foreign Intelligence Surveillance Act</i></p> <ul style="list-style-type: none"> <li>ss1801-1813</li> <li>President, through the Attorney-General may authorise without a court order.</li> <li>District Court Judges, publicly designated by the Chief Justice.</li> </ul> <p><b>Pen Registers or Trap/Trace Device for Foreign Intelligence Purposes</b></p> <p><i>Foreign Intelligence Surveillance Act</i></p> <ul style="list-style-type: none"> <li>ss1841-1846</li> <li>Jointly by Foreign Intelligence Surveillance Court (FISO), or US Magistrate Judge publicly designated by the Chief Justice.</li> </ul> <p><b>702/703/704 Orders</b></p> <p><i>Foreign Intelligence Surveillance Act</i></p> <ul style="list-style-type: none"> <li>ss1881-1881g</li> <li>Jointly by Attorney General and Director of National Intelligence.</li> </ul>
Applicant	<p><b>Telecommunications service or named person warrants for collection of foreign intelligence</b></p> <p>TIA Act– ss11A and 11B</p> <ul style="list-style-type: none"> <li>The Director-General of Security.</li> </ul> <p><b>Foreign communications warrant for collection of foreign intelligence</b></p> <p>TIA Act– s11C</p> <ul style="list-style-type: none"> <li>The Director-General of Security.</li> </ul>	<p><b>Interception Warrant</b></p> <p>As detailed above.</p> <p><b>Foreign Intelligence Authorisations</b></p> <p><i>Communications Security Establishment Act</i> – s33</p> <ul style="list-style-type: none"> <li>The Chief of the Communications Security Establishment.</li> </ul>	<p><b>Type 2 Intelligence Warrants</b></p> <p><i>Intelligence and Security Act 2017</i> – s60</p> <ul style="list-style-type: none"> <li>Intelligence and Security Agencies.</li> </ul>	<p><b>Bulk Interception Warrants</b></p> <p><i>Investigatory Powers Act 2016</i> – s138</p> <ul style="list-style-type: none"> <li>Heads of an intelligence service.</li> </ul> <p><b>Authorisation of acts outside the British Islands</b></p> <p><i>Intelligence Services Act 1994</i> – s7</p> <ul style="list-style-type: none"> <li>Intelligence Service and GCHQ.</li> </ul>	<p><b>Electronic Surveillance Authorisation</b></p> <p><i>Foreign Intelligence Surveillance Act</i></p> <ul style="list-style-type: none"> <li>ss1801-1813</li> <li>A federal officer with prior approval of the Attorney General.</li> </ul> <p><b>Pen Registers or Trap/Trace Device for Foreign Intelligence Purposes</b></p> <p><i>Foreign Intelligence Surveillance Act</i></p> <ul style="list-style-type: none"> <li>ss1841-1846</li> <li>The Attorney General, Deputy, Acting or Assistant Attorney-General or a designated Attorney.</li> </ul> <p><b>702/703/704 Orders</b></p> <p><i>Foreign Intelligence Surveillance Act</i></p> <ul style="list-style-type: none"> <li>ss1881-1881g</li> <li>A federal officer with prior approval of the Attorney General.</li> </ul>

Threshold	Australia	Canada	New Zealand	United Kingdom	United States
	<p><b>Interception warrant for collection of foreign intelligence</b> TIA Act – s11A</p> <ul style="list-style-type: none"> <li>Collection of foreign intelligence relating to that matter is in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well being.</li> </ul> <p><b>Named person warrant for collection of foreign intelligence</b> TIA Act – s11B</p> <ul style="list-style-type: none"> <li>Collection of foreign intelligence relating to that matter is in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well being.</li> <li>It is necessary to intercept the communications of the person or foreign organisation in order to obtain the intelligence.</li> <li>Relying on a telecommunications service warrant or named person warrant would be ineffective.</li> </ul> <p><b>Foreign communications warrant for collection of foreign intelligence</b> TIA Act – s11C</p> <ul style="list-style-type: none"> <li>Collection of foreign intelligence relating to that matter is in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well being.</li> <li>It is necessary to intercept foreign communications in order to collect the intelligence.</li> <li>Relying on a telecommunications service warrant or named person warrant would be ineffective.</li> </ul>	<p><b>Interception Warrant</b> As detailed above.</p> <p><b>Foreign Intelligence Authorisations</b> <i>Communications Security Establishment Act – s34</i></p> <ul style="list-style-type: none"> <li>Reasonable grounds to believe that: <ul style="list-style-type: none"> <li>any activity that would be authorised are reasonable and proportionate, having regard to the nature of the objective to be achieved and the nature of the activities,</li> <li>any information acquired could not reasonably be acquired by other means and will be retained for no longer than is reasonably necessary, and</li> <li>information acquired that is identified as relating to a Canadian or a person in Canada will be used, analysed or retained only if the information is essential to international affairs, defence or security.</li> </ul> </li> </ul>	<p><b>Type 2 Intelligence Warrants</b> <i>Intelligence and Security Act 2017 – ss60 and 61</i></p> <ul style="list-style-type: none"> <li>The Minister is satisfied that: <ul style="list-style-type: none"> <li>the warrant will enable the agency to carry out an activity that is necessary to contribute to the protection of national security, or that will contribute to the international relations and well-being, or economic well-being, of New Zealand,</li> <li>the activity is not in respect of a person, or class of persons, for which a Type 1 warrant is required,</li> <li>the carrying out of otherwise unlawful activity is necessary to enable the agency to perform its legislated functions, and proportionate to the purpose for which it is to be carried out,</li> <li>the purpose of the warrant cannot reasonably be achieved by less intrusive means, and</li> <li>there are satisfactory arrangements in place to ensure nothing is done beyond what is reasonably necessary, all reasonably practicable steps will be taken to minimise the impact of the activity on members of the public, and all information will be retained, used and disclosed in accordance with the Act.</li> </ul> </li> </ul>	<p><b>Bulk Interception Warrants</b> <i>Investigatory Powers Act 2016 – s138</i></p> <ul style="list-style-type: none"> <li>Necessary in the interests of national security, for the purpose of preventing or detecting serious crime, or in the interests of the economic well-being of the UK.</li> <li>Conduct to be authorised is proportionate to what is sought to be achieved.</li> </ul> <p><b>Authorisation of acts outside the British Islands</b> <i>Intelligence Services Act 1994 – s7</i></p> <ul style="list-style-type: none"> <li>Necessary for the proper discharge of a function of the Intelligence Service or GCHQ.</li> <li>The nature and likely consequences of the acts will be reasonable, having regard to the purposes for which they are carried out.</li> <li>Satisfactory arrangements are in force with respect to the disclosure of information obtained under the warrant.</li> </ul>	<p><b>Electronic Surveillance Authorisation</b> <i>Foreign Intelligence Surveillance Act – ss1801-1813</i></p> <ul style="list-style-type: none"> <li>Probable cause to believe the target is a foreign power/agent of a foreign power and that the facilities is being used/about to be used, by a foreign power or an agent of a foreign power.</li> </ul> <p><b>Pen Registers or Trap/Trace Device for Foreign Intelligence Purposes</b> <i>Foreign Intelligence Surveillance Act – ss1841-1846</i></p> <ul style="list-style-type: none"> <li>Information likely to be obtained is foreign intelligence information not concerning a US person.</li> <li>Relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities.</li> </ul> <p><b>702 Orders</b> <i>Foreign Intelligence Surveillance Act – s1881a</i></p> <ul style="list-style-type: none"> <li>Written certification must attest that a significant purpose of the acquisition is to obtain foreign intelligence information.</li> </ul> <p><b>703/704 orders</b> <i>Foreign Intelligence Surveillance Act – ss1881b-1881c</i></p> <ul style="list-style-type: none"> <li>Probable cause to believe the target is a foreign power, agent of a foreign power or an officer or employee of a foreign power.</li> </ul>

# Attachment C: List of questions

## Part 1: Who can access information under the new framework?

1. Do the existing prohibitions and offences against unlawful access to information and data adequately protect privacy in the modern day?
  - a) If so, which aspects are working well?
  - b) If not, which aspects are not working well and how could the new prohibition and/or offences be crafted to ensure that information and data is adequately protected?
2. Do the existing prohibitions and offences against unlawful access to information and data adequately allow the pursuit of other objectives of societal benefit, e.g. cyber security of networks, online safety, scam protection/reduction?
3. Are there any additional agencies you consider should have powers to access particular information and data to perform their functions? If so, which agencies, and why?
4. Do you agree with the proposed considerations for determining whether additional agencies should be permitted to access peoples' information and data? Are there any additional considerations that have not been outlined above?

## Part 2: What information can be accessed?

5. Are there other kinds of information that should be captured by the new definition of 'communication'? If so, what are they?
6. Are there other key concepts in the existing framework that require updating to improve clarity? If so, what are they?
7. How could the framework best account for emerging technologies, such as artificial intelligence and information derived from quantum computing?
8. What kinds of information should be defined as 'content' information? What kinds of information should be defined as 'non-content' information? Is there a quantity at which non-content information becomes content information and what kinds of information would this apply to?
9. Would adopting a definition of 'content' similar to the UK be appropriate, or have any other countries adopted definitions which achieve the desired outcome?
10. Are there benefits to distinguishing between different kinds of non-content information? Are there particular kinds of non-content information that are more or less sensitive than others?
11. Should the distinction between 'live' and 'stored' communications be maintained in the new framework?

12. Do each of these kinds of information involve the same intrusion into privacy?  
Or should the impact of each be considered differently?
13. What type of Australian communications providers should have obligations to protect and retain information, and comply with warrants, authorisations and assistance orders under the new framework?
14. What are your thoughts on the above proposed approach? In particular, how do you think the information captured by surveillance and tracking devices could be explained or defined?

### **Part 3: How can information be accessed?**

15. How could the current warrant framework be simplified to reflect the functional equivalency of many of the existing warrants while ensuring appropriate privacy protections are maintained?
16. What other options could be pursued to simplify the warrant framework for agencies and oversight bodies, while also enabling the framework to withstand rapid technological change?

### **Part 4: When will information be accessed?**

17. Is it appropriate to harmonise legislative thresholds (as outlined above) for covert access to private communications, content data and surveillance information where existing warrants are functionally equivalent?
18. Are there any other changes that should be made to the framework for accessing this type of data?
19. What are your views on the proposed thresholds in relation to access to information about a person's location or movements?
20. What are your views on the proposed framework requiring warrants and authorisations to be targeted at a person in the first instance (with exceptions for objects and premises where required)?
21. Is the proposed additional warrant threshold for third parties appropriate?
22. Is the proposed additional threshold for group warrants appropriate?
23. What are your views on the above proposed approach? And are there any other matters that should be considered by an issuing authority when considering necessity and proportionality?
24. Should magistrates, judges and/or AAT members continue to issue warrants for law enforcement agencies seeking access to this information?
25. What are your thoughts on the proposed principles-based, tiered approach to use and disclosure?

26. When should agencies be required to destroy information obtained under a warrant?
27. What are your thoughts on the proposed approach to emergency authorisations?

## **Part 5: Safeguards and oversight**

28. Are there any additional safeguards that should be considered in the new framework?
29. Is there a need for statutory protections for legally privileged information (and possibly other sensitive information, such as health information)?
30. What are the expectations of the public and industry in relation to oversight of these powers, and how can a new oversight framework be designed to meet those expectations?
31. What, if any, changes are required to the scope, role and powers of the Commonwealth Ombudsman to ensure effective oversight of law enforcement agencies' use of powers in the new framework?
32. How could the new framework streamline the existing record-keeping and reporting obligations to ensure effective and meaningful oversight?
33. Are there any additional reporting or record-keeping requirements should agencies have to improve transparency, accountability and oversight?

## **Part 6: Working together: Industry and Government**

34. How workable is the current framework for providers, including the ability to comply with Government requests?
35. How could the new framework reduce the burden on industry while also ensuring agencies are able to effectively execute warrants to obtain electronic surveillance information?
36. How could the new framework be designed to ensure that agencies and industry are able to work together in a more streamlined way?

## Part 7: Interaction with existing and recent legislation and reviews

37. Do you have views on how the framework could best implement the recommendations of these reviews? In particular:
- a) What data generated by 'Internet of Things' and other devices should or should not be retained by providers?
  - b) Are there additional records that agencies should be required to keep or matters that agencies should be required to report on in relation to data retention and to warrants obtained in relation to journalists or media organisations? How can any new reporting requirements be balanced against the need to ensure sensitive law enforcement or security investigations and capabilities are not compromised or revealed?
  - c) Is it appropriate that the Public Interest Advocate framework is expanded only in relation to journalists and media organisations?
  - d) What would be the impact on reducing the number of officers who may be designated as 'authorised officers' for the purposes of authorising the disclosure of telecommunications data?

# Attachment D: Agency powers under the current electronic surveillance framework

Agency powers under the current framework of the TIA Act.

Agency	Surveillance Device Warrants	Computer Access Warrants	Data Disruption Warrants	Network Activity Warrants	Tracking Device Authorisations
ASIO	✓	✓	✓	✓	✓
ACCC	x	✓	✓	✓	x
ASIC	x	✓	✓	✓	x
HA	x	✓	✓	✓	x
ACLEI	✓	✓	✓	✓	x
ACIC	✓	✓	✓	✓	x
AFP	✓	✓	✓	✓	x
CCC WA	✓	✓	✓	✓	x
QLD CCC	✓	✓	✓	✓	x
IBAC	✓	✓	✓	✓	x
NSW ICAC	✓	✓	✓	✓	x
NSW CC	✓	✓	✓	✓	x
NSW POL	✓	✓	✓	✓	x
NT POL	✓	✓	✓	✓	x
LECC	✓	✓	✓	✓	x
QLD POL	✓	✓	✓	✓	x
ICAC SA	✓	✓	✓	✓	x
SA POL	✓	✓	✓	✓	x
TAS POL	✓	✓	✓	✓	x
VIC POL	✓	✓	✓	✓	x
WA POL	✓	✓	✓	✓	x

Agency powers under the current framework of the *Surveillance Devices Act 2004*<sup>107</sup>

Agency	Surveillance Device Warrants	Computer Access Warrants	Data Disruption Warrants	Network Activity Warrants	Tracking Device Authorisations
ASIO	X	X	X	X	X
ACCC	X	X	X	X	X
ASIC	X	X	X	X	X
HA	X	✓	X	X	✓
ACLEI	✓	✓	X	✓	✓
ACIC	✓	✓	✓	✓	✓
AFP	✓	✓	✓	✓	✓
CCC WA	✓	✓	X	X	✓
QLD CCC	✓	✓	X	X	✓
IBAC	✓	✓	X	X	✓
NSW ICAC	✓	✓	X	X	✓
NSW CC	✓	✓	X	X	✓
NSW POL	✓	✓	X	X	✓
NT POL	✓	✓	X	X	✓
LECC	✓	✓	X	X	✓
QLD POL	✓	✓	X	X	✓
ICAC SA	✓	✓	X	X	✓
SA POL	✓	✓	X	X	✓
TAS POL	✓	✓	X	X	✓
VIC POL	✓	✓	X	X	✓
WA POL	✓	✓	X	X	✓

A retrieval warrant can also be issued for agencies that have installed a surveillance device under a surveillance device warrant or tracking device authorisation.

ASIO powers under the *Australian Security Intelligence Organisation Act 1979*

Agency	Surveillance Device Warrants	Computer Access Warrants	Data Disruption Warrants	Network Activity Warrants	Tracking Device Authorisations
ASIO	✓	✓	✓	✓	✓

<sup>107</sup> For states and territories the *Surveillance Devices Act 2004* may apply for federal offences or state offences with a federal aspect.



