



Where the Record Stops

REFERENCE	AOS-AWS-2026-001
VERSION	1.1
DATE	9 September 2026
CLASSIFICATION	Released
DIRECTOR	Brunei Al-Bijwaie

Where the Record Stops

Version 1.1, 9 September 2026. This revision adds the two Australian Acts v1.o named as unread, the *Crimes Act 1914* Part IAA and the *Australian Security Intelligence Organisation Act 1979* Part III, in a new Section 5 and five new elements of the finding, Ten to Fourteen, v1.o's tenth element becoming Fifteen; rewords one Scope sentence and one heading sentence that were true of the two Acts v1.o read and are not true of four; replaces the Limitations sentence that named the two Acts as unread; and adds two refusals. No element of v1.o's finding is withdrawn or narrowed. The v1.o note below is carried verbatim, and its sentence naming "the two Australian Acts that decide whom a domestic warrant or authorisation reaches" describes what v1.o read; this revision reads four. This practice's corrections register records that sentence and one Scope sentence as overtaken at v1.o and not a correction; they are reworded here because the document now reads four Acts, not because v1.o was wrong.

Version 1.o note, carried verbatim. Version 1.o, 7 September 2026. This assessment asks who can lawfully compel Amazon Web Services Australia Pty Ltd to produce or give access to data it holds for an Australian government customer, and reports what the published record establishes about that and where it stops. It reads the provider's own customer agreement and service terms, the register of the company and of its holding company, the United States statute the corpus has already read, and the two Australian Acts that decide whom a domestic warrant or authorisation reaches, each at its current compilation and pinned by hash. It adjudicates nothing: it does not say whether the provider is inside any definition the Acts use, and it names the one question the record cannot answer. Every claim rests on an artefact pinned in this case's register or already pinned in this corpus, and every quotation was tested against the pinned bytes at the passage where it sits.

Scope

What is assessed. One provider, Amazon Web Services Australia Pty Ltd, as the contracting party for an Australian account; what its published terms say it sells; the United States instrument that reaches a provider subject to that jurisdiction; the Australian instruments of interception, stored communications and telecommunications data, and the definitions they turn on; the international production order regime that sits between the two; and, from this revision, the two Australian Acts that reach a person by relation to a computer, the *Crimes Act 1914* Part IAA and the *Australian Security Intelligence Organisation Act 1979* Part III.

What is not assessed. Whether the provider is a carrier or a carriage service provider, which is the reading on which every instrument of the carrier route turns and which the record does not carry; whether the provider, or any computer on which its services run, is within any of the six classes of person or any definition the two

Acts of Section 5 use, which no document the practice holds speaks to; whether any data in an Australian region is within any United States entity's possession, custody or control; whether any instrument has ever been used; and anything in a contract that is not published. Each is refused in the section where it would otherwise be made, and again at the end.

The method. Each artefact was retrieved with a logged request and, for every page, fetched a second time within the minute so its stability is recorded (convention 50 of this practice). Six pages read here hash differently on every fetch: the AWS Customer Agreement and contracting party table [T-AWS-1, T-AWS-2], the AWS Service Terms at both its addresses [A-AWS-ST-1, A-AWS-ST-2], the AWS Australia FAQs [S3] and the AWS security blog page [S4]. For those six, the hash printed on the verification record is of the copy this practice read at the logged time and cannot be confirmed by fetching the address; every other artefact returned the same bytes twice. Every count below names the test that produced it. Every statement that something is absent names the population it was searched in and the control that shows the search reads what it searches. Quotations from the Acts are taken from the authorised compilation PDFs by text extraction; the Acts' italic defined terms and paragraph indents are not reproduced, and that is the only departure from the source's typography. Where a quotation stops before the end of its passage, the sentence says so.

1 Who contracts

The contracting party for an Australian account is Amazon Web Services Australia Pty Ltd, ABN 63 605 345 891. The AWS Customer Agreement, as served 6 September 2026 [T-AWS-1, sha256 8eb9c9fb4f6caf06..., unstable], defines the "AWS Contracting Party" as "the party identified in the table below, based on your Account Country". That table, served the same day [T-AWS-2, sha256 d625c8815d8e9321..., unstable], carries the row, cell by cell, "Australia", "Amazon Web Services Australia Pty Ltd (ABN: 63 605 345 891)", "N/A", "Level 37, 2-26 Park Street, Sydney, NSW, 2000, Australia". The Service Terms, as served 7 September 2026 [A-AWS-ST-1, sha256 8e1f479fa3db80cd..., unstable], carry the same entity and number in a table whose Australia row reads "w.e.f. 1 October 2022". AWS's own Australia FAQs, as served 5 September 2026 [S3, sha256 e7fb9e591b73e01b..., unstable], record that use of AWS Cloud services for eligible Australian accounts is "automatically transferred from Amazon Web Services, Inc. to Amazon Web Services Australia Pty Ltd, as your AWS Contracting Party". The Australian Business Register's record for ABN 63 605 345 891, as served 5 September 2026 [S5, sha256 c5dccb7f06dcd596..., unstable], carries that number; the served page has changed since its pin and the claim rests on the pinned copy.

Its declared ultimate holding company is Amazon.com, Inc., a United States company. ASIC's current company extract for AMAZON WEB SERVICES AUSTRALIA PTY LTD, ACN 605 345 891, dated 18 July 2026 [H-AWS-1, sha256 69eda18e3696b335..., held under cba-compellability-2026-07 and inherited here], records registration on 29/03/2016 and the declared ultimate holding company AMAZON.COM, INC. The corpus's entity resolution for the Hosting Certification Framework's Strategic tier stops there under its third stopping condition, a declared foreign ultimate holding company [hcf-strategic-2026-07/source/ENTITIES.md]. Amazon.com, Inc.'s Exhibit 21.1 to its Form 10-K for the year ended 31 December 2021, as served by the SEC on 5 September 2026 [S2, sha256

725a6e73e7d75f66...], lists, in the exhibit's own layout, "Amazon Web Services, Inc. Delaware 100 %".

2 What is sold

On its own terms, the provider sells the processing, storage and hosting of a customer's Content. The Customer Agreement [T-AWS-1] defines "Service" as "each of the services made available by us or our affiliates, including those web services described in the Service Terms"; "Your Content" as "Content that you or any End User transfers to us for processing, storage or hosting by the Services in connection with your AWS account"; and "Content" as "software (including machine images), data, text, audio, video, or images". The customer may "specify the AWS regions in which Your Content will be stored". The Hosting Certification Framework's certified service providers page, as served 5 September 2026 [S10, sha256 0036bc5d6b8d18ad...], lists at Strategic "Amazon Web Services - Cloud Service offering (Australian Regions)", and AWS's security blog, as served the same day [S4, sha256 7405e346a41464f4..., unstable], states that "our new AWS Melbourne Region has achieved Strategic Certification".

The Service Terms describe services, and they describe no carriage. The document the agreement incorporates by address, "Last Updated: September 1, 2026" [A-AWS-ST-1], carries 74 numbered service sections, counted as headings followed by a ".1" subsection in the text stripped of markup. In that text the word "storage" occurs 19 times, each of a thing done to Content, and the word "carriage" occurs 0 times, both by whole-word, case-insensitive search; the same search finds "storage" 19 times, which is the control that the search reads the text. The body carries no section for Amazon S3; "Amazon S3" and "Simple Storage" occur 0 times below the document's heading, and "S3" occurs twice on the page, both in the site's navigation. **The nearest sentences on the record to carriage are the provider's own, and they are scoped.** In the Amazon Chime section and the Amazon Connect section, each on a PSTN calling feature, the terms say, twice and identically: "AWS is not a telecommunications provider and does not provide any telecommunications-related services". That sentence sits inside those two sections and speaks of those calling features; it is not a statement about the services as a whole, and this assessment does not read it as one. A second sentence of the same kind sits in the section on "Amazon Pinpoint and AWS End User Messaging", formerly the SMS, MMS, voice message and push notification features of Amazon Pinpoint, at section 29.6: "From time to time, telecommunication providers may change or modify their rules, requirements, and policies (collectively "Carrier Policies")", and "AWS may pass through fees imposed by carriers for violations of Carrier Policies". Both are the provider's characterisation of a named service, the calling features of two products and the messaging features of a third; each speaks of that service and of no other; and neither settles whether any service is a carriage service or over what it is supplied. This assessment reads them as what they are and no further.

3 The foreign instrument

The CLOUD Act obliges a provider subject to United States jurisdiction to disclose data in its possession, custody or control wherever it is located. 18 U.S.C. § 2713, in the United States Code 2024 edition as served by govinfo.gov on 5 September 2026 [S7, sha256 3a242ef2c1ee7a06...], provides in full: "A

provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."

Two predicates stand between that section and any provider, and this assessment resolves neither.

This practice's instrument map, the data file its verification engine reads, names them: that the entity is a provider of "electronic communication service" or "remote computing service", "no adjudication assumed"; and that the data is "within the reachable entity's possession, custody, or control — fact-dependent, unassumed" [lib/instrument_map.yaml, version 1.1.0]. Whether data held by an Australian subsidiary in an Australian region is within a United States parent's possession, custody or control is the second predicate. No pinned artefact answers it for this provider, and the assessment restates it as open.

4 The domestic instruments, and what they turn on

Under the Telecommunications (Interception and Access) Act 1979, an interception warrant, a stored communications warrant and an authorisation to disclose telecommunications data each reach a person only as a carrier. Compilation No. 134 of that Act, compilation date 27 August 2026, registered 3 September 2026, in its two authorised volumes [L-TIA-1, sha256 02f345d733bb1e59...; L-TIA-2, sha256 5946ec06eaae59d1...], defines the word at section 5: "carrier means: (a) except in Parts 5-4 and 5-4A: (i) a carrier (within the meaning of the Telecommunications Act 1997); or (ii) a carriage service provider", and "carriage service provider has the meaning given by the Telecommunications Act 1997". A stored communication is one that "is held on equipment that is operated by, and is in the possession of, a carrier" (section 5); a stored communications warrant issues where there are reasonable grounds for suspecting "that a particular carrier holds stored communications" (section 116(1)(c)) and authorises access to a communication held by "the carrier that holds the communication" (section 117). Chapter 4 sets out when "sections 276, 277 and 278 of the Telecommunications Act 1997 do not prohibit a disclosure of information or a document" (section 171(1)), and never "the contents or substance of a communication" (section 172). The persons those three sections bind are, at section 271 of the Telecommunications Act, "(a) a carrier; or (b) a carriage service provider; or (c) an employee of a carrier; or (d) an employee of a carriage service provider; or (e) a telecommunications contractor; or (f) an employee of a telecommunications contractor" [L-TA-1]; that passage crosses a page in the authorised PDF and is quoted across the break. **Every domestic instrument read here reaches the provider, if it reaches it, through those two words.**

A carrier is the holder of a licence, and this provider does not hold one on the register as captured. The Telecommunications Act 1997, Compilation No. 117, compilation date 4 June 2026, registered 12 June 2026, in its first two volumes [L-TA-1, sha256 7fd3fc9570cfc621...; L-TA-2, sha256 2416755cf9a0473c...], provides at section 7 that "carrier means the holder of a carrier licence" and that a carrier licence is one "granted under section 56". The Australian Communications and Media Authority's register of licensed carriers, captured as rendered on 4 August 2026 [SC-ACMA-4, sha256 761389675694d6d0...], carries 651

licence rows, counted by status token in the stripped capture (337 Current, 276 Surrendered, 38 Cancelled, one status to a row). In that capture “Amazon Web Services” occurs 0 times and “605 345 891” occurs 0 times, by substring search; the control on the same capture and the same search is row 617, which reads, cell by cell, “Amazon Kuiper Australia Pty Ltd”, “652 115 421”, “Current”, “24-Apr-24”, so the search finds an Amazon company where one is present. The Federal Register of Legislation’s API, searched by instrument title for “Amazon” on 7 September 2026, returns two notices for that company, a carrier licence (C2024600253) and Nominated Carrier Declaration 197 (C2024600543), both in force; neither is pinned, and the search reads titles only. **Nothing on the record connects that company’s licence or declaration to any service of Amazon Web Services Australia Pty Ltd, and this assessment does not.**

A carriage service provider is defined by what is supplied, over what, and to whom. Section 87(1) of the Telecommunications Act: “if a person supplies, or proposes to supply, a listed carriage service to the public using: (a) a network unit owned by one or more carriers; or (b) a network unit in relation to which a nominated carrier declaration is in force; the person is a carriage service provider” [L-TA-1]. Three terms carry it. A listed carriage service is, at section 16(1)(a), “a carriage service between a point in Australia and one or more other points in Australia”, and a carriage service is, at section 7, “a service for carrying communications by means of guided and/or unguided electromagnetic energy”. A network unit is, at section 26(1), a line link connecting distinct places in Australia “at least the statutory distance apart”, the distance being “500 metres”, or under sections 27 to 29 multiple line links, a designated radiocommunications facility, or a facility the Minister determines. Supply to the public is, at section 88(2), where “each end-user is outside the immediate circle of the supplier”. The words hosting, cloud, storage and data centre occur 0 times, and content 10 times, across every section read of that Act, sections 7, 15, 16, 23, 26 to 30, 42, 56, 87, 88, 271, 276 to 278 and 313, by whole-word search over the text of those sections; every occurrence of content is in or about section 15’s “content service”, which section 87 does not use.

The duty to help is in the Telecommunications Act, and it runs to the same two words. Section 313(3): “A carrier or carriage service provider must, in connection with: (a) the operation by the carrier or provider of telecommunications networks or facilities; or (b) the supply by the carrier or provider of carriage services; give officers and authorities of the Commonwealth and of the States and Territories such help as is reasonably necessary for the following purposes: (c) enforcing the criminal law and laws imposing pecuniary penalties”; the list runs to “(e) safeguarding national security”, and purposes (ca), (cb) and (d) between them are not quoted here. Section 313(7): giving help “includes a reference to giving help by way of: (a) the provision of interception services, including services in executing an interception warrant under the Telecommunications (Interception and Access) Act 1979; or (b) giving effect to a stored communications warrant under that Act” [L-TA-2]; that passage too crosses a page and is quoted across the break, and its later paragraphs on preservation notices and authorisations are not quoted. The TIA Act’s own Chapter 2 imposes no such duty in its text: every line of its warrant provisions mentioning a carrier was read against the words execute, assist, comply, reasonable steps, must and shall, and none imposes one (OPEN-ITEMS 139 of this practice).

5 The two Acts that reach a person by relation to a computer

Under the Crimes Act 1914, a search warrant reaches data by relation to a computer found, wherever the data is held. Compilation No. 167 of that Act, compilation date 27 August 2026, registered 2 September 2026, in the first of its three authorised volumes [L-CA-7, sha256 3f405cc09c4c5a21...], provides at section 3E(1): “An issuing officer may issue a warrant to search premises if the officer is satisfied, by information on oath or affirmation, that there are reasonable grounds for suspecting that there is, or there will be within the next 72 hours, any evidential material at the premises.” An issuing officer is “(a) a magistrate; or (b) a justice of the peace or other person employed in a court of a State or Territory who is authorised to issue search warrants or warrants for arrest, as the case may be.” (section 3C), and a constable is “a member or special member of the Australian Federal Police or a member of the police force or police service of a State or Territory.” (section 3). Section 3F(2A) authorises the use of a computer found in the search, “a telecommunications facility operated or provided by the Commonwealth or a carrier” or any other equipment “for the purpose of obtaining access to data (the relevant data) that is held in the computer or device”, and, where reasonable, “to use any other computer or a communication in transit to access the relevant data”; section 3F(2D): “it is immaterial whether a thing mentioned in subsection (2A) or (2B) is done: (a) at the premises; or (b) at any other place.” Section 3L(1) authorises operating equipment at the premises “to access data (including data not held at the premises)”. Section 3C: “data held in a computer includes: (a) data held in any removable data storage device for the time being held in a computer; or (b) data held in a data storage device on a computer network of which the computer forms a part.” The word *computer* is not defined for Part IAA in section 3 or section 3C, tested by searching both for a definition line; Part IAAC defines it for its own purposes in the words the ASIO Act uses below.

Section 3LA orders a person to assist access by relation to the computer and by knowledge, in six classes. “A constable may apply to a magistrate for an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow a constable to do one or more of the following” [L-CA-7], the things being access to, copying of, or conversion of “data held in, or accessible from, a computer or data storage device that” is on warrant premises, found on a searched person, moved for examination, or seized. The magistrate may grant the order if satisfied that “(a) there are reasonable grounds for suspecting that evidential material is held in, or is accessible from, the computer or data storage device; and (b) the specified person is: (i) reasonably suspected of having committed the offence stated in the relevant warrant; or (ii) the owner or lessee of the computer or device; or (iii) an employee of the owner or lessee of the computer or device; or (iv) a person engaged under a contract for services by the owner or lessee of the computer or device; or (v) a person who uses or has used the computer or device; or” and “(vi) a person who is or was a system administrator for the system including the computer or device; and (c) the specified person has relevant knowledge of: (i) the computer or device or a computer network of which the computer or device forms or formed a part; or (ii) measures applied to protect data held in, or accessible from, the computer or device.”; the passage crosses a page in the authorised PDF and is quoted across the break. Non-compliance is punishable by “Imprisonment for 5 years or 300 penalty units, or both.”

Under the Australian Security Intelligence Organisation Act 1979, a computer access warrant

reaches a computer by association with a person, and computer means any part of any combination of computers, systems and networks. Compilation No. 84 of that Act, compilation date 27 August 2026, registered 5 September 2026, in its one authorised volume [L-ASIO-4, sha256 93c590df0df5b9de...], provides at section 25A(1): “If the Director-General requests the Attorney-General to do so, and the Attorney-General is satisfied as mentioned in subsection (2), the Attorney-General may issue a warrant in accordance with this section.” The test is “reasonable grounds for believing that access by the Organisation to data held in a computer (the target computer) will substantially assist the collection of intelligence in accordance with this Act in respect of a matter (the security matter) that is important in relation to security.” The target may be “a computer associated with, used by or likely to be used by, a person (whose identity may or may not be known).” The warrant may authorise, where reasonable, “using any other computer or a communication in transit to access the relevant data”, and, to conceal access, entry to “any premises where the computer is reasonably believed to be”. Section 4: “computer means all or part of: (a) one or more computers; or (b) one or more computer systems; or (c) one or more computer networks; or (d) any combination of the above.”

Section 34AAD orders assistance in the same six classes. “The Director-General may request the Attorney-General to make an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the Organisation to do one or more of the following” [L-ASIO-4], and the Attorney-General may make the order satisfied “that the specified person is: (i) reasonably suspected of being involved in activities that are prejudicial to security; or (ii) the owner or lessee of the computer or device; or (iii) an employee of the owner or lessee of the computer or device; or (iv) a person engaged under a contract for services by the owner or lessee of the computer or device; or (v) a person who uses or has used the computer or device; or (vi) a person who is or was a system administrator for the system including the computer or device; and (d) the Attorney-General is satisfied, on reasonable grounds, that the specified person has relevant knowledge of: (i) the computer or device or a computer network of which the computer or device forms or formed a part; or (ii) measures applied to protect data held in, or accessible from, the computer or device.” Classes two to six, and the two heads of relevant knowledge, are word for word identical in the two Acts, tested by comparing the extracted texts. The differences are the first class, and the ASIO Act’s issuing words, “the Attorney-General is satisfied, on reasonable grounds, that”, which wrap both limbs and which the Crimes Act places once, at the head of section 3LA(2). Non-compliance: “Imprisonment for 5 years or 300 penalty units, or both.”

In neither Act, at the width read, does carrier or carriage service provider name a person the Act compels. In Part IAA of the Crimes Act [L-CA-7] the two words occur 10 times, counted by whole-word search over the Part’s extracted text from its body heading to Part IAAA’s: 3 inside the section 3C definition, “carrier means: (a) a carrier within the meaning of the Telecommunications Act 1997; or (b) a carriage service provider within the meaning of that Act.”, and 7 in the phrase “a telecommunications facility operated or provided by the Commonwealth or a carrier”, each naming a facility a constable may use. In the ASIO Act [L-ASIO-4] the two words occur 9 times over the whole extracted volume: the two section 4 definitions, each “has the same meaning as in the Telecommunications Act 1997.”; three in the section 22 definition for Division 2, in the Crimes Act’s words; the facility phrase in sections 25A(4) and 27E(2); and both words in section 33’s reference to interception of a communication “passing over a telecommunications system

operated by a carrier or a carriage service provider.” None names a person either Act orders or authorises against. The Crimes Act’s other Parts are not read.

The record stops in two places. For the carrier route it stops at the network unit, as Section 6 says. For the six-class route the questions the Acts pose are which computer a warrant would name and who owns, leases, uses or administers it and under what contract; no warrant is on the record, and the eight documents Section 6 names were searched on 9 September 2026, whole word, case-insensitive, for *lessee*, *contract for services* and *system administrator* (0 in every document), *owner* (10 in the Service Terms, every one a customer’s project, account, Space or face-vector ownership or a patent owner; 3 in the FAQs, a Payer account owner; 0 elsewhere), *administrator* (6 in the Service Terms, every one the customer’s own End Users with administrative privileges or its learning administrator; 0 elsewhere), *administer* and its forms (12 in the Customer Agreement, every one an arbitration’s administering authority; 0 elsewhere), *operated by* and *managed by* (2 and 3, all in the Service Terms), and *operate* and its forms (17 in the Service Terms, 1 in the Customer Agreement, 2 in the FAQs). The control is the word *Amazon*, found in every one of the eight; it shows the search reads each text and not that a synonym would be found. **In the Acts’ words, the documents say nothing about the systems the services run on.** Five sentences in the Service Terms [A-AWS-ST-1] say who operates or owns a named thing, and each is scoped to its section: 4.7, “Services running at AWS operated facilities”; 16.2, “AWS will permit data center operators or other service providers to connect your hardware to AWS’s hardware at the AWS Direct Connect location(s) that you select.”; 66.1, “These facilities, and the fiber between the AWS Data Transfer Terminal connection points and the AWS network router, may be owned and/or managed by our colocation providers.”; 79.1, Amazon Bracket Content “may be processed by the Hardware Provider outside of facilities operated by AWS”; and 95.2, “Access to AWS Nitro System EC2 instance APIs – which enable AWS personnel to operate the system without access to Your Content - is always logged, and always requires authentication and authorization.” Each speaks of the service it sits in and of no other, as Section 2 reads the two telecommunications sentences, and this assessment reads them as what they are and no further. **The buyer’s question gains a second half: whose computer, administered by whom, under what contract for services.**

6 The one question the record does not answer

Whether Amazon Web Services Australia Pty Ltd is a carriage service provider turns on whether its services are supplied over a network unit that a carrier owns or a nominated carrier declaration covers, and no published document this practice holds says over what network unit they are supplied.

The documents searched are the eight the provider publishes or is named in that this case pins or inherits: the Customer Agreement, the contracting party table, the Service Terms at both addresses, the Australia FAQs, the blog page, the ABN record and the ASIC extract. Each was searched for the terms network unit, line link, facility and carrier, whole word, case-insensitive. The Service Terms carry “carrier” 9 times: 5 as the carrier that “accepts the Outposts Equipment for delivery back” or to which an Appliance is provided “for redelivery to us” (sections 4.8, 9.2 and 9.5), and 4 in section 29.6 as “Carrier Policies”, the sentence Section 2 quotes. They carry “facility” 21 times: the customer’s “Designated Facility” for Outposts Equipment (sections 4.3 to 4.8), the “AWS Data Transfer Terminal facility” (sections 66.1 to 66.5), and the customer’s “Facility” for Amazon One Enterprise Devices (sections 101.2 and 101.3). None of the 30 occurrences is the term network unit or line link, and none says over what the services are supplied. The other seven documents carry none of the four terms. The control is that the same search finds “telecommunications” 5 times in the Service Terms. The Federal Register of Legislation’s API, searched by title for “Carriage Service Provider” on 7 September 2026, returns no declaration under section 87(4) naming the provider; the two instruments it returns are a repealed security-information determination and its amendment, and a title search is the width of that nil. The other readings section 87 needs are on the record: the end-users of the 134 contract notices AusTender reports under the provider’s ABN [DS-AWS-2, sha256 6a22d71e2cdb2823..., export retrieved 6 August 2026] are 28 distinct agencies, none of whose names contains “Amazon”, counted from the export’s Agency column; the ACMA lookup is in Section 4. **The record stops at the network unit for the carrier route, and at the computer for the six-class route of Section 5. This assessment does not fill the gap by inference from the words cloud, storage or hosting, and it names the question a buyer would put to the provider: over what network unit, owned by whom, are the services supplied; and whose computer, administered by whom, under what contract for services.**

7 Schedule 1, and who it is drawn for

Schedule 1 to the TIA Act reaches a storage provider by what it does rather than by the word carrier.

Its subject is the “prescribed communications provider”, defined at clause 1 as “(a) a network entity; or (b) a transmission service provider; or (c) a message/call application service provider; or (d) a storage/back-up service provider; or (e) a general electronic content service provider” [L-TIA-2]. Clause 7(1): “storage/back-up service means a service that enables end-users to store or back-up material, where the uploading of the material for storage or back-up is by means of a transmission service”. An order binds a provider that meets the enforcement threshold, which clause 125(1)(d) sets where “a prescribed communications provider provides a storage/back-up service to one or more Australians”. The term “designated communications provider” occurs 0 times in the Schedule, by search of the extracted volume.

The Australia–United States agreement is a designated international agreement, and its entry

into force rests on the department's statement. Clause 3(1) designates an agreement where “a copy of the English text of the agreement is set out in the regulations” and “the agreement has entered into force for Australia and the foreign country”. Regulation 26A of the Telecommunications (Interception and Access) Regulations 2017, Compilation No. 12, compilation date 13 December 2025 [L-TIA-7, sha256 2d4e40e4f9694530...], provides: “For the purposes of paragraph 3(1)(b) of Schedule 1 to the Act, a copy of the English text of the Agreement between the Government of Australia and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime is set out in Schedule 2 to this instrument.” The Attorney-General's Department's page on the international production order framework, as served 7 September 2026 to a browser agent after the practice's own agent received no response from that host [A-AGD-1, sha256 f92b9749509a5905...], states: “On 30 January 2024, Australia and the United States brought into force the Agreement” and that this was done “through a formal exchange of diplomatic notes”. The notes themselves, the Australian Treaty Series entry and the Attorneys-General joint statement of 31 January 2024 that the page links were not retrieved: twenty-nine addresses were tried in thirty-one logged requests, across the treaties database, AustLII, the department's live site, the National Library's web archive under four forms, the Department of Justice and the State Department, and none served the document; the control is that the same requests, under the same agents, served the department's page and the agreement's unofficial text at the Department of Justice. The date is therefore the department's statement of it, and this assessment carries it as that.

An international production order is drawn for a provider based in or operating in the foreign country, and on the record that is the parent, not the subsidiary. Clause 10A(2): a body corporate is based in a foreign country “if, and only if: (a) the provider is incorporated in the foreign country; or (b) the provider has its principal place of business in the foreign country”. The ASIC extract records Amazon Web Services Australia Pty Ltd as an Australian proprietary company registered 29/03/2016 [H-AWS-1]; Exhibit 21.1 records Amazon Web Services, Inc. as incorporated in Delaware [S2]. What follows from that for any order against any data is not adjudicated here. The orders are Australian-issued: an interception agency applies, “the eligible Judge or nominated ART member” issues (clause 30), and the order is given through “the Australian Designated Authority”, who is “the Secretary of the Attorney-General's Department”, to “the prescribed communications provider to whom the order is directed” (clauses I and III). **The domestic Act is therefore the vehicle by which an Australian agency reaches a provider in the United States under the agreement, and the two halves of the question are not separable.**

8 The finding

Each element below is stated with its own artefact and its own date. Each is what the artefact shows. No sentence here says what they compose into.

One. The contracting party for an Australian AWS account is Amazon Web Services Australia Pty Ltd, ABN 63 605 345 891. T-AWS-2, as served 6 September 2026, unstable; A-AWS-ST-1, as served 7 September 2026, unstable.

Two. That company's declared ultimate holding company is Amazon.com, Inc., and Amazon Web Services,

Inc. is a Delaware subsidiary of that company. H-AWS-1, extract dated 18 July 2026; S2, as served 5 September 2026.

Three. The provider's terms define what it sells as the processing, storage and hosting of Content, use the word "carriage" 0 times across the Service Terms' stripped body, carry no section for Amazon S3 in that body, and say of two calling features that AWS is not a telecommunications provider. T-AWS-1, as served 6 September 2026, unstable; A-AWS-ST-1, as served 7 September 2026, unstable.

Four. 18 U.S.C. § 2713 obliges a provider of electronic communication service or remote computing service to disclose data within its possession, custody or control regardless of where it is located. S7, United States Code 2024 edition, as served 5 September 2026.

Five. Under the TIA Act, Compilation No. 134, interception, stored communications and telecommunications data reach a person only as a carrier, which that Act defines by reference to the Telecommunications Act 1997. L-TIA-1, as served 7 September 2026.

Six. Under the Telecommunications Act 1997, Compilation No. 117, a carrier is the holder of a licence granted under section 56, and Amazon Web Services Australia Pty Ltd is not on the register of licensed carriers as captured 4 August 2026; Amazon Kuiper Australia Pty Ltd is. L-TA-1, as served 7 September 2026; SC-ACMA-4, captured 4 August 2026.

Seven. A carriage service provider is, at section 87(1), a person who supplies a listed carriage service to the public using a network unit owned by a carrier or covered by a nominated carrier declaration, and no document the practice holds that the provider publishes or is named in states over what network unit its services are supplied. L-TA-1, as served 7 September 2026; the eight documents named in Section 6, searched 7 September 2026.

Eight. The duty to give help in executing an interception warrant or a stored communications warrant is section 313 of the Telecommunications Act and runs to a carrier or carriage service provider. L-TA-2, as served 7 September 2026.

Nine. Schedule 1 to the TIA Act names a storage/back-up service provider among the persons an international production order may be directed to; the Australia–United States agreement is set out in the regulations; the Attorney-General's Department states it was brought into force on 30 January 2024 by exchange of notes; and a body corporate is based in a foreign country under clause 10A(2) if incorporated there or with its principal place of business there. L-TIA-2, L-TIA-7, as served 7 September 2026; A-AGD-1, as served 7 September 2026.

Ten. Under the Crimes Act 1914, Compilation No. 167, a search warrant issued by an issuing officer on information on oath or affirmation authorises access from a computer found on the premises to data not held at the premises and to data on a computer network of which the computer forms a part, by any other computer or a communication in transit, at any other place. L-CA-7, as served 9 September 2026.

Eleven. Under section 3LA of that Act, a magistrate may order a person to assist access to a computer or device on warrant premises, moved or seized, where the person is one of six classes, suspect, owner or lessee,

employee of the owner or lessee, a person engaged under a contract for services by the owner or lessee, user, or system administrator for the system including the computer or device, and has relevant knowledge of the computer, a network it forms part of, or the measures protecting its data. L-CA-7, as served 9 September 2026.

Twelve. Under the ASIO Act 1979, Compilation No. 84, the Attorney-General on the Director-General's request may issue a computer access warrant over a computer associated with, used by or likely to be used by a person, where computer means all or part of any combination of computers, computer systems and computer networks, authorising access by any other computer or a communication in transit and entry to any premises where the computer is reasonably believed to be. L-ASIO-4, as served 9 September 2026.

Thirteen. Under section 34AAD of that Act the Attorney-General may order a person to assist access in the same six classes and on the same knowledge condition as section 3LA, classes two to six and the two heads of knowledge word for word identical, the first class and the ASIO Act's satisfaction words alone differing. L-ASIO-4, L-CA-7, as served 9 September 2026.

Fourteen. In Part IAA of the Crimes Act and in the whole of the ASIO Act, the words carrier and carriage service provider name a facility that may be used, a definition, or a system another Act governs, 10 and 9 occurrences each enumerated, and never a person the Act compels; and no document the provider publishes or is named in states who owns, leases, administers or contracts for the systems its services run on, in those words, searched 9 September 2026. L-CA-7, L-ASIO-4; the eight documents named in Section 6.

Fifteen. Nothing in this assessment states whether Amazon Web Services Australia Pty Ltd, or any computer on which its services run, is inside or outside any definition or class quoted above, or whether any instrument reaches any data it holds.

Limitations

The register of licensed carriers is read at one capture, 4 August 2026. A licence granted since would not be in it. The register is a rendered capture: the table is client-rendered and absent from the raw response.

Six pages hash differently on every fetch, named in the method; their hashes on the verification record are of the copies read, not of anything a reader can fetch. The ABN record has changed since its pin.

The Service Terms describe services and not how communications reach them. Their absence of the word carriage is a fact about a document, not about a network.

The entry into force of the agreement is the department's statement. The notes and the treaty series entry were not retrieved at the width stated in Section 7.

Sections 314 and 81 of the Telecommunications Act are unread, as is any declaration under section 87(4) beyond a search of instrument titles.

The Crimes Act 1914, Compilation No. 167, and the Australian Security Intelligence Organisation Act 1979, Compilation No. 84, are read for Part IAA and Part III Division 2 respectively and no further. Sections 3QA and 3ZQU and Parts IAAA and IAAC of the first, and sections 26 to 34AAC and Division 3 of

the second, are unread. The *Online Safety Act 2021*, which supplies the terms *electronic service* and *account* to the Crimes Act's account-based data, is unread. Section 5's count for the Crimes Act is over Part IAA only, and its search of the provider's documents is over eight documents and the words named; a synonym, or a document the practice does not hold, is outside it.

The United States half is read at the statute and not at any case, and the instrument map's two predicates are stated, not resolved.

The practice's own retrieval agent is refused by several Commonwealth hosts; where a browser agent was used instead, the sentence says so, and a pin made with one agent cannot be checked with the other.

What this assessment is not

It is not a finding that Amazon Web Services Australia Pty Ltd is, or is not, a carriage service provider. The reading that decides it, the network unit over which its services are supplied, is on no document the practice holds.

It is not a finding that any data in an Australian region is within a United States entity's possession, custody or control. That is the second predicate of the instrument map, fact-dependent and unadjudicated.

It is not a claim that any instrument, foreign or domestic, has been used against the provider or any customer's data. No pinned artefact says so and the assessment does not look.

It is not a reading of the whole-of-government arrangement or of the Strategic tier Deed of Certification. Neither is published; the Deed's template is pinned in this corpus and the executed instrument is not.

It is not a reading of the words cloud, storage or hosting into any definition. The words are the provider's; the definitions are the Acts'; the reading between them is the adjudication this assessment does not make.

It is not a finding that a contractor for services or a system administrator under section 3LA or section 34AAD reaches a hosting or cloud provider, or this provider. Neither Act names one; whether "the system including the computer or device" or "a computer network of which the computer or device forms or formed a part" reaches a system operated by a person other than the owner or lessee is what each Act leaves unanswered.

It is not a finding that any computer on which the provider's services run is associated with, used by or likely to be used by any person, or is on any premises, for the purposes of any warrant. No warrant is on the record, and no document the practice holds says whose computer any service runs on.

It is not a connection between the Kuiper carrier licence and any AWS Australia service. Two facts on the register, and nothing between them.

Related published assessments

- **AOS-CMP-2026-001**, *The Compellability Gap in Commonwealth Cloud Assurance*, vi.4. The two Home Affairs instruments and whether either tests lawful foreign compulsion; the CLOUD Act at 18 U.S.C. § 2713 pinned there as S7, and the AWS artefacts S2 to S5 this assessment inherits.
- **AOS-CBA-2026-001**, *Jurisdictional Exposure of Commonwealth Bank Cloud and Model Dependencies*. The ASIC extract for Amazon Web Services Australia Pty Ltd is held under that case.
- **AOS-HCF-2026-001**, *Jurisdiction of Control in the Hosting Certification Framework, Strategic Tier*. The entity resolution that stops at Amazon.com, Inc.
- **AOS-CPI-2026-001**, *Who the Record Names*. The same question put to the Microsoft arrangement: which company a Commonwealth customer contracts with, and what the record does not connect.
- **AOS-TEL-2026-001**, *Telstra CLOUD Act Assessment*. The Australia–United States agreement’s entry into force is asserted there as 30 January 2024 without a pinned source; this assessment pins the department’s statement.

References

Every artefact is pinned by SHA-256 in this case’s register or in the register of the case or finding named beside it, and re-verified against its recorded hash at this case’s pin.

- T-AWS-1, T-AWS-2 — AWS Customer Agreement; AWS Contracting Party table. `general-findings/strategic-service-terms-2026-09`, 6 September 2026.
- A-AWS-ST-1, A-AWS-ST-2 — AWS Service Terms, “Last Updated: September 1, 2026”, at the canonical address and at the address the agreement names. This case, 7 September 2026.
- A-A6D-1 — Attorney-General’s Department, International production order framework. This case, 7 September 2026.
- S2, S3, S4, S5, S7, S10 — Amazon.com, Inc. FY2021 10-K Exhibit 21.1; AWS Australia FAQs; AWS Security Blog, Hosting Certification Framework tag; ABN Lookup, ABN 63 605 345 891; 18 U.S.C. § 2713, United States Code 2024 edition, govinfo.gov; Hosting Certification Framework, Certified Service Providers. `compellability-gap-2026-07`, 5 September 2026.
- H-AWS-1 — ASIC current company extract, Amazon Web Services Australia Pty Ltd, 18 July 2026. `hcf-strategic-2026-07`, inheriting `cba-compellability-2026-07`.
- SC-ACMA-4 — ACMA register of licensed carriers, rendered capture. `general-findings/submarine-cable-scoping-2026-08`, 4 August 2026.
- DS-AWS-2 — AusTender contract notice export, supplier ABN 63 605 345 891. `general-findings/demand-side-tractability-2026-08`, 6 August 2026.
- L-TIA-1, L-TIA-2, L-TIA-7 — Telecommunications (Interception and Access) Act 1979, Compilation No. 134, C2026C00372, volumes 1 and 2; Telecommunications (Interception and Access) Regulations 2017, Compilation No. 12, F2025C01245. `general-findings/tia-act-2026-09`, 7 September 2026.

- L-TA-1, L-TA-2 — Telecommunications Act 1997, Compilation No. 117, C2026Coo224, volumes 1 and 2. [general-findings/telecommunications-act-2026-09](#), 7 September 2026.
- L-CA-7 — Crimes Act 1914, Compilation No. 167, C2026Coo368, volume 1 of 3, Parts I to IA. [general-findings/crimes-act-2026-09](#), 9 September 2026.
- L-ASIO-4 — Australian Security Intelligence Organisation Act 1979, Compilation No. 84, C2026Coo387, one volume. [general-findings/asio-act-2026-09](#), 9 September 2026.

End of document.