# Regulation Impact Statement for the Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime

Nearly every crime and threat to national security has an online element and requires the collection of electronic data. Often this electronic data is held by communications service providers with global operations and which may have customers all over the world. Accessing this data is of increasingly high value to Australian law enforcement and national security agencies. However, it is not an easy task.

According to the Australian Institute of Criminology, the estimated cost of serious and organised crime in Australia in 2016-2017 was up to $47.4 billion,[1] with up to 70 per cent of Australia's serious and organised crime threats originating offshore or having strong offshore links. Furthermore, the Australian Criminal Intelligence Commission has identified the use of technology and digital infrastructure by serious and organised crime as a 'key determinant of significant changes in the criminal landscape into the future'. However, due to difficulties associated with accessing data stored offshore by communications service providers, it is often very difficult to effectively investigate and prosecute these crimes and bring criminals to justice.

## 1. WHAT IS THE PROBLEM?

Communications service provider business models often involve offices and data storage facilities located in many different jurisdictions. They may even offer services in one country and have no physical or legal presence in that country. The nature of modern data storage systems and 'cloud computing' means that data is transient. Data stored by a company automatically moves between physical international servers making it often challenging for law enforcement and national security agencies to identify where and by whom it is held. Further, this data is often deleted before law enforcement or national security agencies can obtain it.

Circumstances where foreign communications service providers hold electronic data relevant to Australian criminal investigations and prosecutions often involve a complex web of legal compliance and regulation. What would traditionally have been an entirely domestic communication—between two people in Australia using a communications service offered to the Australian public—may now move through many different countries and may be subject to the laws of multiple countries restricting the disclosure of electronic data.

For example, foreign jurisdictions may heavily restrict the disclosure of the content of communications, or prevent the disclosure of that information in its entirety without a mutual legal assistance request. Where foreign communications service providers store data in third party foreign jurisdictions, they may be subject to laws of the country in which they operate, the laws of the country where the data is stored, and the laws of the country with jurisdiction over the criminal matter. Accessing electronic data in these circumstances significantly frustrates the ability for Australian agencies to combat crime, putting the Australian community at risk.

---

[1] Australian Institute of Criminology, *Statistical Report 09: Estimating the cost of serious and organised crime in Australia 2016-17* (10 October 2018), 1 <https://www.aic.gov.au/sites/default/files/2020-05/sr09.pdf>.

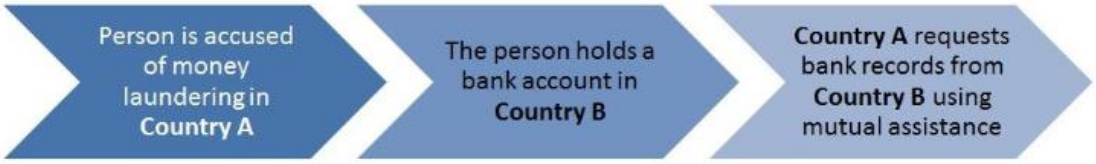
The need to act fast has never been more critical. However, often this data can only be obtained through international cooperation via the cumbersome mutual legal assistance process. Such a process can take anywhere between 6 – 12 months for an Australian authority to receive data in response to a mutual legal assistance request. This delay often comes not from the Australian authorities involved, but the time it takes for a foreign government to review, process, and use legal process on Australia's behalf to obtain the electronic data.

## International crime cooperation

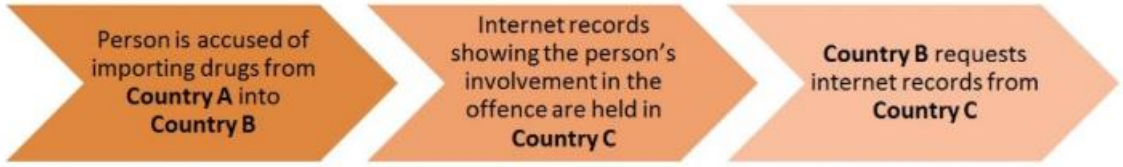
International crime cooperation mechanisms are critical to obtain evidence, including electronic data, from foreign jurisdictions for use in criminal investigations and prosecutions. Australia's law enforcement and national security agencies currently rely heavily on international crime cooperation mechanisms, such as mutual legal assistance, to access critical electronic data needed to combat serious crime.

Mutual legal assistance is the process countries use to obtain government-to-government assistance in criminal investigations and prosecutions. Mutual legal assistance can also be used to identify and recover the proceeds of crime. Australia's mutual legal assistance system is governed by the *Mutual Assistance in Criminal Matters Act 1987*.

The below diagrams demonstrate the need for mutual legal assistance:




Mutual legal assistance is a reciprocal process. Australia can make requests to any foreign country and can receive requests from any foreign country. Countries assist on the understanding that they will receive assistance in return when the need arises. This is shown in the following diagram:




These existing cooperation mechanisms were designed before the internet and without considering the nature of modern telecommunications networks. Under the mutual legal assistance process, requests for communications data from foreign jurisdictions can take a significant amount of time.

This is not an issue unique to Australia; the challenges of government-to-government international crime cooperation continue to be acknowledged internationally. As an example, the Cybercrime Convention Committee for the Council of Europe Budapest Convention on Cybercrime reported in 2014 that inefficiencies in these processes regularly lead to abandoned requests and investigations.[2] A working group of the Committee also reported in 2016 that while these processes are inefficient in general, with respect to electronic data, the use of mutual legal assistance is not always a realistic solution to access evidence in the context of remotely stored data.[3]

[2] Cybercrime Convention Committee, *T-CY assessment report: The mutual legal assistance provisions if the Budapest Convention on Cybercrime* (3 December 2014), 123 [5.1.1] <https://rm.coe.int/16802e726c>.
[3] Cybercrime Convention Committee Cloud Evidence Group, *Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY* (16 September 2016), 9 [2.4] <https://rm.coe.int>.

Alternatives to the mutual legal assistance process are also utilised to obtain electronic data from foreign jurisdictions, such as police to police and agency to agency assistance. However, these approaches can also be lengthy, and in some cases can result in information being provided that is not admissible in court due to the requirements of the *Foreign Evidence Act 1994*. Communications service providers also provide electronic data on a voluntary basis to law enforcement agencies, although this is not done by all providers in all circumstances and can therefore be an unreliable source of obtaining critical information for an investigation or prosecution.

### Access to electronic data from the United States

Between 2007 and 2020, Australia made approximately 4000 mutual assistance requests in total. These requests were for a variety of purposes, including requesting the execution of search warrants, the production of documents, the taking of evidence, and the registering or otherwise enforcing proceeds of crime orders. Approximately one quarter of all the requests made by Australia between 2007 and 2020 were directed to the United States seeking records from communications service providers. This demonstrates both the importance of communications records to Australian law enforcement investigations and prosecutions, and that the United States houses a vast amount of data on Australian communications activity by virtue of the large numbers of technology and communications service providers based there.

Historically, requests for electronic data to United States-based communications service providers (e.g. Google and Facebook) can take 12 months or longer, to receive data back for Australian law enforcement agencies to utilise as part of an investigation or prosecution. Criminal activity can continue in this time, and there is also a risk that prosecutions may not proceed due to lack of sufficient evidence. Some agencies may even choose to not pursue requesting this evidence in the first place due to the known delays and administrative burdens of the mutual legal assistance process. This means that the demand for this data may even be higher than what is ultimately requested. As a result, Australian agencies continue to risk the loss of valuable evidence and continue to face unacceptable delays to criminal justice outcomes.

## 2. WHY IS GOVERNMENT ACTION NEEDED?

The Government's first priority is to ensure the safety and security of all Australians. The ever-changing dynamics of serious transnational criminal activity, including child sexual abuse and terrorism, presents new challenges to law enforcement and national security agencies. Evidence critical to these investigations and prosecutions are stored across a myriad of devices and networks operated by private companies internationally. It is critical to equip Australian law enforcement and national security agencies with the tools they need to gather information and evidence to combat serious crimes.

Under Australian law, Australian agencies can quickly access information from Australian telecommunications service providers. However, as more people use non-Australian based services for all of their communications, agencies are increasingly required to use international legal frameworks to gain access to information which would previously have been held by Australian-based providers.

Many of the global providers are located in the United States. This means Australian law enforcement agencies are heavily reliant on electronic data held by communications service providers located in the United States for investigations and prosecutions of serious criminal activity.

United States-based communications service providers have, to date, been cooperative and understand the requirement of Government to fulfil its duties to protect the Australian community. However, some providers cannot legally or, where they can legally, do not voluntarily, disclose certain electronic data directly to foreign governments conducting criminal investigations.[4] This is due to their concerns that they would be acting against foreign laws.

[4] US Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law around the World: The Purpose and Impact of the CLOUD Act* (April 2019) 2.

Where communications service providers do choose to provide voluntary assistance it is often inconsistent and dependent on whether their internal disclosure policies adopt a conservative or broad interpretation as to what can and cannot be disclosed under their domestic law (such policies may also change at any time). This ultimately reduces the ability to rely on voluntary assistance without any clear structured framework, especially where electronic data is required in an emergency or urgent circumstance.

The inherent voluntary nature of these disclosure policies leaves international crime cooperation in the hands of companies, such as social media providers, rather than a clear pathway provided by consenting governments (such as the United States CLOUD Act and Australia's international production order framework).

Government action is required to provide more certainty to both United States and domestic communications service providers, and the Australian community, as to when, how, and why data can be accessed for the purposes of combating serious crime (especially where that involves efforts for cross-border access to data).

Reliance on United States communications service providers for assistance is not unique to Australian law enforcement and national security agencies. Formal international crime cooperation mechanisms are used by many countries to obtain electronic data they hold, leading to many thousands of requests being made to the United States government through government-to-government mechanisms. Formal international crime cooperation mechanisms must be used to receive electronic data in a form admissible in court as evidence, or to obtain the content of communications. This drives demand for the use of these formal mechanisms, as opposed to less formal mechanisms such as police to police assistance or voluntary assistance from communications service providers.

The United States government must prioritise and review the many thousands of requests it receives from all over the world, and then follow the necessary domestic legal processes to obtain that information on behalf of the requesting country. This can result in significant delays, often months or even years, in obtaining information.

As an example, if Australia makes a mutual legal assistance request for Facebook communications data – in accepting and processing the request, the United States authorities would need to review it alongside the other many other similarly urgent requests received from other countries around the world. Once it has been reviewed and approved, those authorities would ordinarily seek a domestic warrant or order from an issuing authority (such as a court) to serve on Facebook and obtain that data. This must then be reviewed by the central authority before being provided to Australia, again alongside the many other thousands of requests considered by the United States central authority.

This inherently involves lengthy timeframes and hinders the ability of law enforcement and national security agencies to effectively investigate and prosecute crime. Delays in obtaining critical data can mean that investigations cannot be progressed, criminals can continue offending against the Australian community, and evidence can be lost due to the passage of time.

The international community faces a critical question of how to provide governments efficient and effective access to information (often critical evidence) needed to protect public safety. Without Government action, the increasing demands for electronic information held offshore and ongoing delays will negatively affect Australia's overall security. As such, Government action is needed to support Australian agencies with their investigations and prosecutions of serious crime.

# 3. WHAT POLICY OPTIONS ARE YOU CONSIDERING?

### Option 1: Maintain the status quo

Maintaining the status quo would mean Australian requests for electronic data will continue to be made through the mutual legal assistance regime. There are a range of complex challenges associated with the international crime cooperation such as mutual legal assistance, including significant delays and inefficiencies resulting from cumbersome government-to-government processes. While this will remain a viable pathway for other forms of mutual legal assistance, existing processes pose great risks with respect to electronic data, which is often only retained for short periods of time and, if not obtained quickly, can be lost forever. With the increasing transnational nature of serious crime and the use of global communications technologies and services as part

of that criminality, the status quo is likely to involve an increased reliance on mutual legal assistance to obtain electronic data, exacerbating the current challenges.

There would be limited modernisation of international crime cooperation as communications technology continues to evolve and the adopting of these techniques by organised criminal syndicates continues to occur. This will continue to be detrimental to investigations and prosecutions of criminal and terrorist activity in Australia as delays would increase, resulting in some investigations and prosecutions not being able to proceed.

### Option 2: Modernising the mutual legal assistance process and other international crime cooperation mechanisms

As the current process of obtaining electronic data from foreign communications service providers is to utilise mutual legal assistance and other international crime cooperation mechanisms, an option is to enhance mutual legal assistance through working closely with foreign governments to establish mechanisms to:

- monitor and streamline the efficiency of the mutual legal assistance process;
- develop more effective and efficient pathways for communicating with foreign governments, and for the provision/receipt of electronic data;
- amend current bilateral and multilateral treaties (including negotiation of future treaties) to include national security agencies, such as the Australian Security Intelligence Organisation.

Ongoing reviews of the mutual legal assistance and other international crime cooperation processes ensure law enforcement and national security objectives are supported as effectively as possible. The Government reviews Australia's model mutual legal assistance treaty on an ongoing basis to ensure it reflects best practice in international cooperation taking into account the evolving nature of crime types, such as transnational and cybercrime. The most recent review of the model mutual legal assistance treaty concluded in early 2020 with amendments approved by the former Attorney-General. These changes bring Australia's model treaty in line with the United Nations model treaty and mutual assistance practices of other countries. The changes also align Australia's model treaty with Australian domestic law, following amendments in 2018 to the *Mutual Assistance in Criminal Matters Act 1987* regarding the nature of interim proceeds of crime orders, improved casework practices and law enforcement imperatives.

To further refine mutual legal assistance processes, the Government participates in the e-mutual legal assistance working group, an Interpol initiative. This initiative examines the legal feasibility of a streamlined system to transmit mutual legal assistance requests and evidence obtained in response to those requests. Although beneficial, the development and implementation of such processes is anticipated to take time and as such, this option is not anticipated to significantly alter the status quo in the short term.

While all these efforts are being undertaken by the Government to improve Australian processes, it is difficult to be able to mandate these kinds of reforms by foreign countries and industry. For example, a significant amount of delay may be caused by the foreign countries' law enforcement authorities' ability to use its domestic legal processes effectively and efficiently. It would be open for the Australian Government to request a foreign country to consider how its processes could be improved to better support Australian law enforcement and national security purposes, although whether the foreign country does so is outside Australia's control.

Further, while some efficiencies can be obtained, the involvement of two separate governments in each request for mutual legal assistance limits the benefits that can be obtained from process improvements.

### Option 3: A cross-border access to data agreement with the United States

A cross-border access to data agreement with the United States (commonly referred to as the 'AUS-US CLOUD Act Agreement') will facilitate the timely lawful exchange of electronic data between Australia and the United States by enabling certain Australian agencies to give orders for interception, stored communications and telecommunications data directly to communications service providers in the United States, and vice versa.

An AUS-US CLOUD Act Agreement (supported by the international production order framework set out in Schedule 1 to the *Telecommunications (Interception and Access) Act 1979*) enables communications service providers in Australia and the United States to respond to lawful orders from the other country by removing legal restrictions on disclosure. The removal of these restrictions will facilitate timely and effective direct engagement between foreign law enforcement agencies and communications service providers holding electronic data that is crucial to modern investigations and prosecutions. The projected large number of Australian orders to the United States will be supported through a purpose built technical solution. Conversely, the United States will primarily serve Australian communications service providers through their existing technical methods, as they do not expect to serve many orders to Australia.

While the type of electronic data that will be able to be obtained under the AUS-US CLOUD Act Agreement can currently be sought through the mutual legal assistance process, this Agreement is a significant step in increasing the effectiveness of investigations and prosecutions of serious crimes without the significant delay that can often accompany mutual legal assistance. The AUS-US CLOUD Act Agreement will complement, not replace, the mutual legal assistance process.

Orders can be made for interception, stored communications, telecommunications data, and subscriber information when sought alongside another type of data. Subscriber information may also be obtained independent of orders for other types of data where it relates to the prevention, detection, investigation or prosecution of crime.

*Australian Designated Authority*

As part of entering into the AUS-US CLOUD Act Agreement, Australia is required to create an Australian Designated Authority to give outgoing orders to communications service providers in the relevant foreign country. It is contemplated the Australian Designated Authority will have the capacity to also service possible future bilateral or multilateral agreements other than the AUS-US CLOUD Act Agreement. The creation of the Australian Designated Authority will oversee the process by providing a central coordinating entity for international production orders. This will benefit the new framework by providing a central point of contact for both Australian and United States communications service providers, Australian law enforcement and national security agencies, and the United States Designated Authority. The Australian Designated Authority will have a strong understanding of United States law relevant to the framework under the AUS-US CLOUD Act Agreement and of requirements in regards to international crime cooperation.

The Australian Designated Authority will operate from within the Attorney-General's Department. The Australian Designated Authority will be responsible for a range of agreement functions, including providing guidance upon request to ensure Australian communications service providers comply with a lawful request for data under the underlying bilateral agreement, including assisting with disputes, and providing general support to queries from Australian industry in regards to the operation of the framework.

*Regulatory Changes*

The AUS-US CLOUD Act Agreement will result in some change to the legal frameworks associated with Australian communications service providers' disclosure of electronic data (such as intercepted communications, stored communications and telecommunications data). The Agreement will operate under the international production order framework set out in Schedule 1 to the *Telecommunications (Interception and Access) Act 1979* as a 'designated international agreement'. The AUS-US CLOUD Act Agreement and the international production order framework will work together to allow Australian communications service providers to disclose electronic data to authorities in the United States for the purposes of detecting, preventing, investigating and prosecuting serious crime, where the agreement is invoked.

Australian communications service providers will still be subject to the prohibitions and regulation of the disclosure of certain types of data, such as those under the *Telecommunications (Interception and Access) Act 1979*, the *Telecommunications Act 1997*, and the *Privacy Act 1988*. However, the international production order framework and the designation of an agreement as a '*designated international agreement'* will serve as lawful authority to disclose electronic data in line with the framework. This maintains protections for communications as expected by the Australian community, while also providing a clear legal pathway for Australian communications service providers to disclose electronic data to foreign authorities of countries with which Australia has an agreement. This will significantly reduce the risk of conflict of laws issues.

# 4. THE LIKELY NET BENEFIT OF EACH OPTION

## Option 1: Maintain the status quo

This option would have no immediate increased regulatory or compliance costs for Australian communications service providers, with the existing international crime cooperation process continuing unchanged. Foreign authorities will continue to seek the disclosure of electronic data from the Australian Government.

The impact to Australia of maintaining the status quo will also be a weakening of Australia's ability to keep up with the evolving trend of criminals using communications technology to conduct their activities. This could diminish our national security and criminal justice efforts, potentially putting Australia at risk of increased levels of crime, lengthy prosecutions and investigations, and the potential loss of crucial evidence. The mutual legal assistance process would continue to be relied upon. Similarly, voluntary provision of electronic data by communications service providers would continue to be relied upon, noting the ongoing risk of changes to their policies in providing this information.

There are no benefits or change in cost to industry associated with this option and the net benefit of maintaining the status quo is nil.

## Option 2: Modernising the mutual legal assistance process and other international crime cooperation mechanisms

Foreign authorities will continue to seek the disclosure of electronic data from the Australian government. Accordingly, there will be no increased regulatory impact with respect to industry's role in facilitating the access and disclosure of electronic data through mutual legal assistance mechanisms.

While mutual legal assistance could be recalibrated and better resourced, due to the framework being designed before the modern communications environment existed, ad-hoc fixes to the current mutual legal assistance process will not solve the problem. As outlined in section 1 of this paper, the accelerating flow of requests will eventually outpace the ability of any government to staff and resource its mutual legal assistance infrastructure.

Attempts to upgrade or modify mutual legal assistance have been ongoing for nearly two decades. Although concerted effort has been undertaken during this time, it is still not considered to be an efficient and effective process. Efforts to modernise the international crime cooperation mechanism are highly dependent on foreign governments to also update their own processes, which is outside of Australia's control. Further, while international crime cooperation mechanisms remain government-to-government based, it will inevitably remain a slower process than dealing directly with foreign service providers.

Option 2 would likely realise minimal benefits, although the cost to industry compared to current arrangements would be nil.

## Option 3: A cross-border access to data agreement with the United States

The purpose of an AUS-US CLOUD Act Agreement would be to advance public safety and security, and to ensure the ongoing protection of privacy rights, civil liberties, and an open Internet, by resolving potential conflict of law issues between the United States and Australia (e.g. blocking statutes). This includes when communications service providers are served with orders or requests from either country for the production of electronic data, where those communications service providers may also be subject to the laws of the other country, among others. To that end, an Agreement provides an efficient, effective, and privacy-protective means for Australia and the United States to obtain, subject to appropriate targeting restrictions, electronic data in a manner consistent with international law obligations and the domestic laws of both countries.

As outlined above, approximately one quarter of all mutual legal assistance requests made by Australia are to the United States, and a significant proportion of those are for electronic data. Increasing delays may mean that investigations relying on electronic data from foreign jurisdictions (such as the United States) are abandoned due to anticipated delays and inefficiencies in obtaining such data. This is not a unique issue to

Australian law enforcement agencies and prosecutorial bodies, as identified in the Council of Europe reports outlined above which have for many years identified this as an ongoing experience across the globe.[5]

An AUS-US CLOUD Act Agreement will significantly reduce the delays associated with obtaining such information. Although difficult to quantify due to the varying nature of each request for electronic data, for routine requests it is expected that this waiting period will be reduced to a matter of weeks or days. This is anticipated to have long term benefits for the effectiveness of Australian national security operations and criminal investigations and prosecutions.

The mechanism established by the AUS-US CLOUD Act Agreement will also alleviate pressure on the need for resources to be allocated to responding to mutual legal assistance requests. In this way, the AUS-US CLOUD Act Agreement will benefit other countries as well by reducing the overall workload for the United States in responding to mutual legal assistance requests. It is in Australia's best interests that the mutual legal assistance process is under less strain so as to support both Australia's and the United States' overall international crime cooperation efforts.

Given the majority of electronic communications data is held in the United States, the AUS-US CLOUD Act Agreement is the first agreement between Australia and another country to streamline the sharing of electronic communications data. It is anticipated that similar agreements with other countries could follow. Further, Schedule 1 to the *Telecommunications (Interception and Access) Act 1979*, the domestic framework which would facilitate the AUS-US CLOUD Act Agreement, provides for the designation of any international agreement that meets the requirements of the legislation, paving the way for any future agreements to be readily implemented.

*Potential Costs to Australian Communications Service Providers*

There are costs to industry associated with fulfilling orders for relevant data. Between 2007 and 2020 Australia received less than 30 requests for the types of data that would be available for request under the AUS-US CLOUD Act Agreement. Of these 30 requests, not all would be permitted to be served under the new Agreement due to the additional safeguards imposed by the targeting restrictions.

In the event the number of requests from the US increase, resulting in a significant cost impact on Australian communications service providers, it is open to Australian providers to seek cost reimbursement from the United States in accordance with its domestic law.

*Compliance by Communications Service Providers*

The AUS-US CLOUD Act Agreement will not compel communications service providers in either country to comply with an order. However, the United States or Australia may decide to enforce orders under their own domestic law, including whether a provider would be compelled to comply with an order.

For Australia, the framework for enforcing orders is located in Schedule 1 to the *Telecommunications (Interception and Access) Act 1979*, which imposes civil penalties for non-compliance with Australian orders. It is likely United States communications service providers will comply with Australian orders issued under the AUS-US CLOUD Act Agreement, noting broad support in the United States telecommunications industry for a framework that clarifies their rights and obligations with respect to cross-border data transfers.

On 6 February 2018, five of the largest United States communications service providers, Apple, Facebook, Google, Microsoft, and Oath (formerly known as Verizon), published a joint letter in support of the CLOUD Act. The letter notes that

> [i]ntroduction of the [CLOUD Act] is an important step toward enhancing and protecting individual privacy rights, reducing international conflicts of law and keeping us all safer…The [CLOUD Act] would further allow law enforcement to investigate cross-border crime and terrorism in a way that avoids international legal conflicts.[6]

---

[5] Cybercrime Convention Committee, above n 2, 123 [5.1.1]; Cybercrime Convention Committee Cloud Evidence Group, above n 3, 9 [2.4].

[6] Apple et al, *Tech Companies Letter of Support for House CLOUD Act* (6 February 2018) Microsoft <https://blogs.microsoft.com/wp-content/uploads/sites/149/2018/02/Tech-Companies-Letter-of-Support-for-House-CLOUD-Act-020618.pdf>.

The United States does not have a specific international production order regime like Australia. The United States will utilise their existing relevant disclosure frameworks (such as the Stored Communications Act[7]). Some of these frameworks involve mandatory orders, including enforceability mechanisms with penalties for non-compliance. However, the Government expects the instances of the United States applying penalties on Australian communications service providers for non-compliance with an order will be extremely rare. In such a circumstance, the AUS-US CLOUD Act Agreement allows for the Australian Designated Authority to mediate disputes between the United States Designated Authority and Australian communications service providers. Accordingly, while unlikely, there may be a cost impact on Australian communications service providers should they challenge an order made under the domestic legal framework of the United States.

A cross-border access to data agreement with the United States would have significant benefits to the Australian community, through more timely access to vital information for Australian national security and law enforcement agencies to aid their role in keeping the community safe. There is expected to be a negligible regulatory cost for Australian communications service providers. Option 3 has a high net benefit.

# 5. CONSULTATION

*Commonwealth, State and Territory government agencies*

On 7 October 2019, the Minister for Home Affairs and the United States Attorney General jointly announced the commencement of formal negotiations towards a bilateral AUS-US CLOUD Act Agreement. Following that announcement, consultation with key Commonwealth stakeholders focused on developing a variety of policy proposals to inform the negotiation of the AUS-US CLOUD Act Agreement and development of associated legislation. Consultation with Commonwealth stakeholders occurred through a senior executive-level interdepartmental steering committee as well as with other Commonwealth agencies not members of this committee. Commonwealth agencies, including oversight bodies such as the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security, were key stakeholders in the development of the Agreement and the *Telecommunications Legislation Amendment (International Production Orders) Act 2021*, as well as planning for implementation of these frameworks.

State and Territory policy departments and law enforcement agencies were also consulted on the development of the legislation and throughout the negotiation of the AUS-US CLOUD Act Agreement, engaging in regular teleconferences and meetings commencing in late 2019. State and Territory agencies were given the opportunity on several occasions to review and provide their comments on draft versions of the legislation. These comments proved to be valuable contributions in shaping the legislative framework that underpins the AUS-US CLOUD Act Agreement. From mid-2020 onwards, extensive consultation with State and Territory agencies occurred in to inform negotiation of the Agreement and build understanding of the proposed framework and plan for its implementation.

*Communications Service Providers*

In addition to the extensive consultation with key Commonwealth, State and Territory government agencies, major communications service providers in Australia and the United States were also consulted during the development of the *Telecommunications Legislation Amendment (International Production Orders) Act 2021*. The Communications Alliance, the Law Council of Australia, and major United States communications service providers (including Apple, Microsoft, Google and Facebook) were also briefed on the operation of the legislation and the impact of a CLOUD Act Agreement (where appropriate given the confidential nature of international negotiations). This consultation process was productive and assisted in the development of the Act and the AUS-US CLOUD Act Agreement.

Feedback from these discussions consistently indicated industry support of the intent of the AUS-US CLOUD Act Agreement. Both Australian and United States industry have noted the importance of working closely with law enforcement and national security agencies to keep our communities safe, including through the AUS-US CLOUD Act Agreement and international production order framework. This is further displayed in the open letter jointly authored by five of the largest United States communications service providers referred to above.

[7] Codified at 18 U.S.C. Chapter 121.

Engagement with Australian industry commenced at a special industry-government day meeting of the Interception Consultative Committee in late 2019. The Interception Consultative Committee is an established government forum that includes representatives of Commonwealth and State and Territory government agencies that are able to obtain interception information. During the meeting industry participants were largely supportive of the proposed AUS-US CLOUD Act Agreement with the United States, and raised questions in regards to the practical impacts of implementation. These discussions included how Australian communications service providers would respond to an order under the Agreement and how dispute resolution would operate.

To ensure involvement of Australian communications service providers, an industry working group was created to foster engagement and consultation. The industry working group comprises of Telstra, Vodafone, Optus, TPG, NBN Co, and Vocus. The industry working group meetings were held in late 2019 and early 2020. Consultation was also undertaken with Fastmail, an Australian email service provider that has previously received some mutual legal assistance requests from foreign countries.

These meetings involved detailed discussions on how the international production order framework in the *Telecommunications Legislation Amendment (International Production Orders) Act 2021* would operate in conjunction with a possible AUS-US CLOUD Act Agreement. During these sessions, discussions surrounded a range of issues related to the CLOUD Act Agreement and supporting legislation, including:

- compliance with the framework;
- estimated incoming volume of requests from the United States;
- types of data likely to be requested;
- the ability to challenge orders; and
- the status of mutual legal assistance under this new Agreement.

Some of the key issues identified by stakeholders during this consultation include ways to make the legislation more easily readable and understandable. As a result of this feedback, various changes were made to the draft legislation. For example, in response to a request by industry to clearly distinguish the parts of the international production order framework that related to incoming orders compared to outgoing orders, the part of the legislation titled 'Incoming orders and requests' was restructured. Another issue raised by industry stakeholders during this consultation period related to the definition of certain key requirements. This feedback was instrumental in ensuring that the Explanatory Memorandum to the legislation contained detailed explanation of the definitions.

As well as these changes, Australian communications service providers provided details of their position on the role of the United States Designated Authority, processes to seek reimbursement from complying with orders from the United States, and dispute resolution mechanisms. Generally, Australian communications service providers expressed no significant issues with these aspects, and were primarily focused as to how these aspects would operate in practical terms. These discussions assisted in ensuring that negotiations would consider and support the issues of most concern to Australian communications service providers.

The Government will continue to work closely with industry to ensure the AUS-US CLOUD Act Agreement and respective legislative frameworks are clearly understood by Australian communications service providers. Consultation will be critical over the life (including implementation and successful operation) of the AUS-US CLOUD Act Agreement (initial period of 5 years).

# 6. THE CHOSEN OPTION – Cross-border access to data agreement with the United States

Entering into an AUS-US CLOUD Act Agreement (Option 3) is the best option as it will have the highest overall net benefit. It is strongly in Australia's interests to enter into a cross-border access to data agreement with the United States given that such an agreement is expected to:

- support Australia's interests to ensure that Australian law enforcement agencies and the Australian Security Intelligence Organisation can effectively and efficiently obtain electronic data;

- reduce the current burdens on international crime cooperation mechanisms. This will reduce the workload at the United States end in responding to mutual legal assistance requests;
- enhance the already strong relationships between the governments of Australia and the United States, as well as between Australia and United States communications service providers; and
- contain a set of safeguards and limitations that require both countries to ensure that data obtained under the Agreement are to be afforded reasonable, necessary and proportionate privacy protections.

The AUS-US CLOUD Act Agreement will significantly enhance Australian law enforcement and national security agencies ability to prevent, detect, investigate and prosecute all manners of serious crime. The Agreement will expedite the process of receiving electronic data from United States communications service providers and will mean the delay ordinarily associated with obtaining data across borders will no longer impede or halt investigations. The timely receipt of electronic data will also enable prosecutors to meet court timeframes and avoid situations where charges are withdrawn, or less serious charges are laid due to critical evidence being delayed in the mutual legal assistance process.

A draft RIS was developed shortly after the introduction of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 and has been utilised and updated during the development of the international production order framework, including the development of the AUS-US CLOUD Act Agreement.

# 7. IMPLEMENTATION

Implementation of the Agreement will not require further domestic legislative reform as the framework allowing for international agreements of this kind was addressed as part of the *Telecommunications Legislation Amendment (International Production Orders) Act 2021.* Once domestic processes are complete (including parliamentary consideration of the text of the agreement), Australia and the United States will exchange diplomatic notes advising that the ratification process has been completed by both Parties. The Government anticipates entry into force in mid-2022.

The provisions of the AUS-US CLOUD Act Agreement set out a range of review clauses and processes. Firstly, the ability for periodic reviews in terms of each Parties' compliance with the agreement. Secondly, agreements are only for a term of 5 years with the possibility of extension. The AUS-US CLOUD Act Agreement provides for mechanisms for unilateral termination by either Party.

Additional funding from the Federal Budget 2021-2022 provided additional resources to various Commonwealth agencies to effectively implement the AUS-US CLOUD Act Agreement. This includes additional resources being provided to the Administrative Appeals Tribunal to support the expected increase in orders being sought. Similarly, as the AUS-US CLOUD Act Agreement will likely result in an increase in the number of criminal matters being prosecuted, additional resourcing will be provided to the Commonwealth Director of Public Prosecutions commencing in the 2021-22 financial year. To oversee the operation of agencies using the regime, the Office of the Commonwealth Ombudsman and the Office of the Inspector-General of Intelligence and Security will also receive additional resourcing.

A technical solution has been designed to effectively manage the forecasted large volume of outgoing orders to the United States. Incoming orders to Australian communications service providers would not utilise this technical solution. This technical solution has been designed through consultation with Commonwealth agencies with consideration to the needs and capabilities of State and Territory agencies. As the technical solution is designed for the sole purpose of serving orders to the United States (and future countries that Australia has a designated international agreement with), Australian communications service providers were not consulted on the solution as it would have no impact on incoming orders from the United States. There will not be any regulatory costs to Australian industry or individuals as a result of this technical solution.