CS1800 Situation Analysis

Attached is the **Exceptional Access** Situation Analysis for CS1800. The date you are making the recommendation is **December 1, 2018**. Please do not consider any information released after that date. In this situation analysis, you will be advising an Australian Senator on whether to support the Assistance and Access Bill.

Some things to remember:

- **Think multidimensionally**: Cyber policy impacts many different issues, and it is important to identify potential risks and opportunities in your analysis. Consider the strengths and weaknesses of several possible responses and select the optimal response.
- **Engage the scenario**: Assume that the situation which we have provided you is plausible. At the same time, think critically about the information that you have been provided and its origins.
- **Consider interests:** Organizations have a broad and diverse set of interests. How might your decision impact other interests which your organization would like to secure? If you choose one course of action, would a different office at your organization reject your approach? Be sure to be able to justify your response as strongly as possible.
- **Think holistically:** It is important to also consider not just your interests, but *all* parties' interests, including states and non-state actors.
- **Take a clear stance:** These situations are intentionally divisive, even amongst cybersecurity and policy experts. Your task is to recommend a decision, not describe the situation, so taking a strong stance and defending it is encouraged.

What you are responsible for:

1. A brief, informal oral presentation by your group in section. There are no requirements for using visual materials, nor are there requirements for how many members of your group must speak. Expect to outline your course of action for roughly five, but no more than ten, minutes.

2. Engaging in a brief Q&A from your classmates and your TAs afterwards. We will be assessing the degree to which you have prepared justifications for your course of action.

3. A brief, informal one-page summary of your proposed plan of action to be emailed to your TAs before your presentation. Formatting is not especially important – we just want a record of your approach for evaluation purposes. Bullet points are acceptable in this assignment. No bibliography is required.

4. Filling out a peer evaluation after your presentation, during which you will have the opportunity to inform the HTAs about whether all members of your group contributed fairly to your group assignment.

Included in this brief:

1. A letter from the office of the Australian Senator you are advising.
2. A summarized version of the Assistance and Access Bill.
3. A graphic explaining the structure and accountability mechanisms of the agencies granted powers by the bill.
4. Home Affairs Minister Peter Dutton's speech in the House arguing in favor of the bill.
5. Apple Inc.'s submission arguing against the bill.

You are advisors to an independent Senator for New South Wales in the Australian Senate, asked to consider the Assistance and Access Bill 2018. The Senator's policy staff have compiled a summarized version of the bill, as well as a summary of the structure of the Australian intelligence, law enforcement and national security communities. Australia features a bicameral legislature similar to the United States, with legislation first needing to pass the House of Representatives, in which the Government by definition has a plurality, before being considered by the Senate.

The Assistance and Access Bill gives new powers to Australia's national security agencies and police departments, forcing technology companies to assist in national security and law enforcement investigations. The bill is targeted at encryption technologies which limit Australia's ability to obtain intelligence and evidence from intercepted communications, and has been described as the strongest attempt a liberal democracy has made at obtaining "exceptional access" to encrypted communications. While a bill of this nature would normally involve a period of extended consultation, the Government has decided to shrink the timeline in an attempt to pass the bill before Christmas, a period which intelligence agencies claim carries an increased risk of terrorism. As such, we urgently seek your advice on whether to support the bill.

There is strong evidence that encryption does make some government operations less effective. Peter Dutton, the Minister for Home Affairs, has claimed that 90% of intelligence and national security operations are negatively impacted by encryption. Particularly difficult is the warning from the Australian Security Intelligence Organisation (ASIO) that Sydney, located in the Senator's state, is a likely target of potential Christmas-period terrorist activity, and that their ability to disrupt these threats is being limited by the increased use of end-to-end encryption. However, a coalition of technology companies, cybersecurity experts and civil liberties groups has been formed, launching a series of allegations against the bill. Their principal complaints are that the bill weakens cybersecurity, the Australian technology industry, and the protection of civil liberties. The concern regarding civil liberties is not that the bill will circumvent warrants – warrants must still be issued for the Government to access information, regardless of the means of access – but rather that the bill lowers the level of effort required to access information, the overall level of surveillance.

While the bill is expected to pass the House of Representatives by virtue of the Government's one-seat majority, its passage through the Senate is far less certain. The balance of power is held by crossbenchers such as the Senator, who are not part of the Government or the Opposition. Thus, the Senator's vote may be deciding, and so we ask for your careful consideration of the bill. To aid your decision-making, we have attached two submissions to the bill's consideration. The first, by Peter Dutton, is strongly in favour of the bill, while the second,

by Apple Inc., is strongly against. Please note that Apple's 6th complaint, extraterritoriality, has been addressed since their submission. Furthermore, we have attached a document describing the structure and accountability of the Australian law enforcement community. If you desire additional background, we suggest consulting the bill's senate hearing or additional submissions.

Summary of Assistance and Access Bill 2018

Definitions

Interception agency: the Australian Security Intelligence Organisation (ASIO), the Australian Federal Police (AFP), the Australian Criminal Intelligence Commission (ACIC), or a state police force.

Agency director: Director-General of Security (ASIO), Commissioner of the AFP, CEO of ACIC, or chief officer of a state police force

Relevant objective: enforcing the law for serious criminal offenses in Australia, assisting the enforcement of the law in a foreign country, and safeguarding national security.

Service provider: any person or corporation who creates, supplies or supports software, computer hardware or telecommunications technologies.

Target technology: any software, carriage service, electronic service, or computer hardware used or likely to be used by the person(s) of interest.

Systemic vulnerability or weakness: a vulnerability or weakness that affects a whole class of technology, but does not include a vulnerability or weakness that is selectively introduced to one or more target technologies that are connected with a particular person.

Relevant clauses:

This bill creates three ways through which agencies may enlist external assistance:

1. Technical Assistance Request (TAR): A request, served by an agency director, that asks a service provider to voluntarily assist an interception agency in achieving a relevant objective using existing capabilities.
2. Technical Assistance Notice (TAN): A notice, served by an agency director, that compels a service provider to assist an interception agency in achieving a relevant objective using existing capabilities.
3. Technical Capability Notice (TCN): A notice, served by the Attorney-General, that compels a service provider to create a new technical capability to assist an interception agency in achieving a relevant objective.

Persons and organizations do not bear civil liability for any actions taken in accordance with a TAR, TAN or TCN, but do bear criminal liability.

The service provider must not be issued a TAR, TAN or TCN that requires them to build a systemic vulnerability or weakness, as determined by the issuer of the notice.

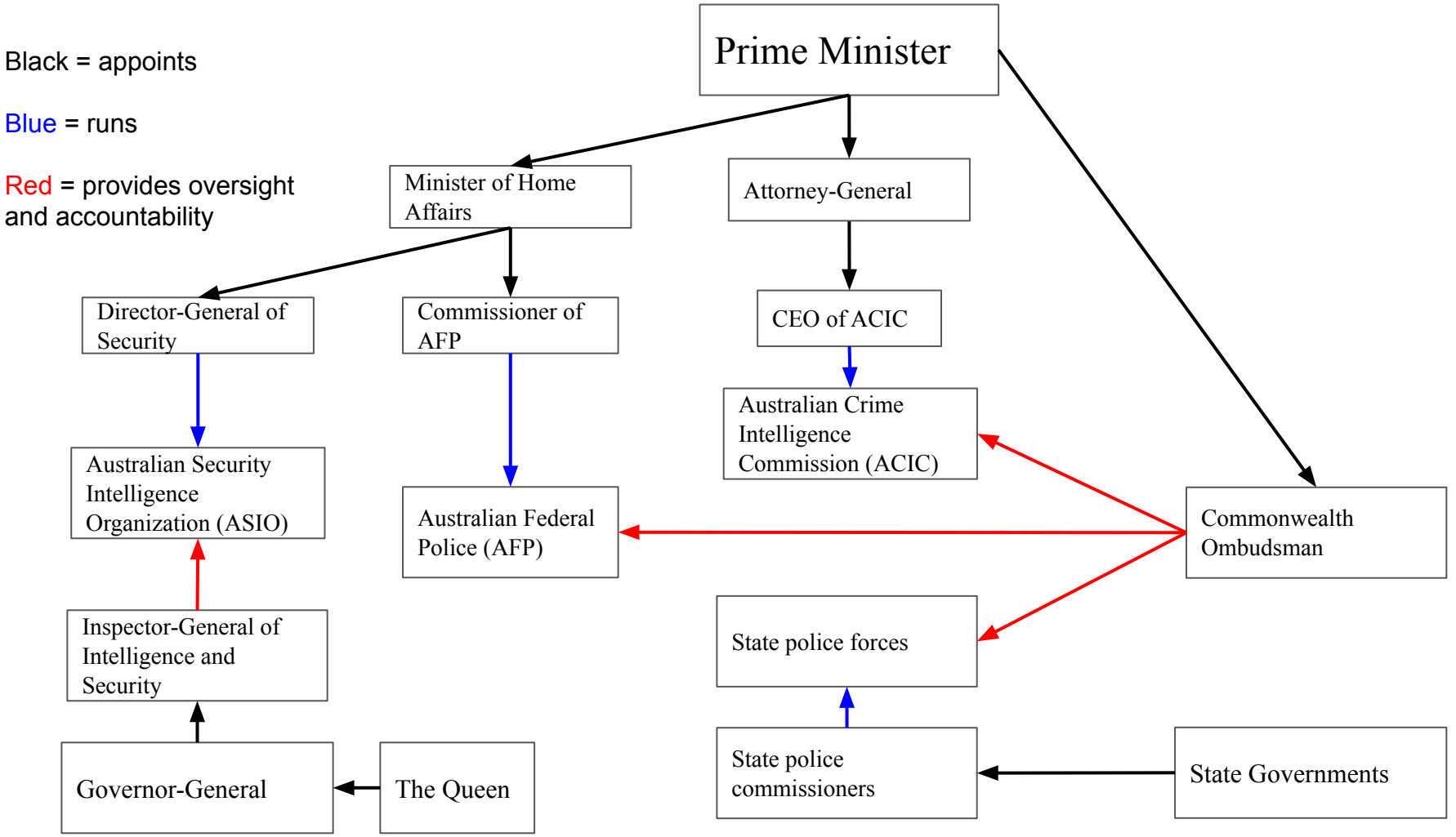
No TAR, TAN, or TCN can be issued unless the issuer is satisfied that it is reasonable, proportionate, and technically feasible. They may also not be issued if compliance necessitates breaking the laws of foreign countries.

The unauthorized disclosure of a TAR, TAN or TCN results in 5 years' imprisonment.

Failure to comply with a TAN or TCN results in a fine of AU$10,000,000 for a provider that is a body corporate and AU$50,000 for a provider that is not a body corporate

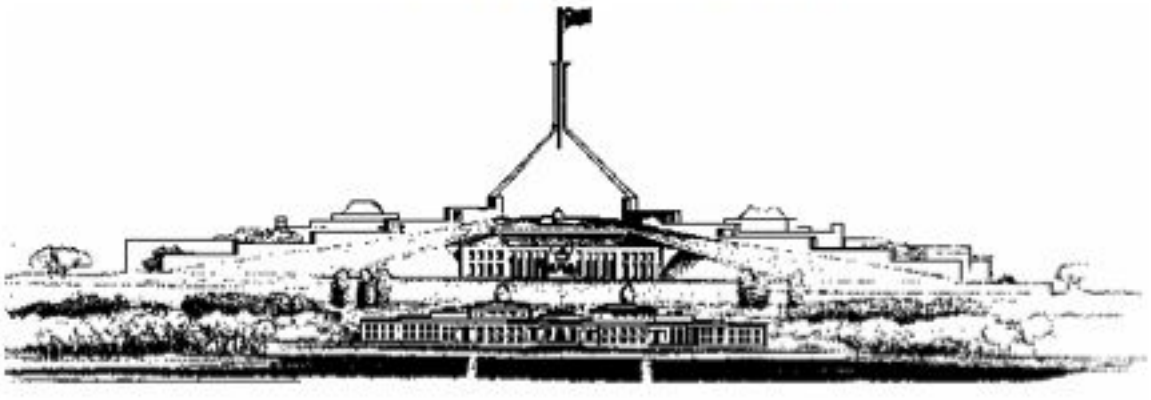
If a service provider disagrees with a TAN or TCN issued and wishes to appeal, the following process is followed:

1. The Attorney-General appoints three assessors to evaluate the notice.
2. The assessors submit a report to the Attorney-General, the service provider, and the Inspector-General of Intelligence and Security (if ASIO) or the Commonwealth Ombudsman (if AFP, ACIC, or a state police force).
3. The Attorney-General decides whether to revoke or vary the notice, or to dismiss the complaint and enforce compliance.


Black = appoints
Blue = runs
Red = provides oversight and accountability
Prime Minister
Minister of Home Affairs
Attorney-General
Director-General of Security
Commissioner of AFP
CEO of ACIC
Australian Crime Intelligence Commission (ACIC)
Australian Security Intelligence Organization (ASIO)
Australian Federal Police (AFP)
Commonwealth Ombudsman
Inspector-General of Intelligence and Security
State police forces
Governor-General
The Queen
State police commissioners
State Governments

COMMONWEALTH OF AUSTRALIA

PARLIAMENTARY DEBATES



HOUSE OF REPRESENTATIVES

BILLS

Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

Second Reading

SPEECH

Thursday, 20 September 2018

BY AUTHORITY OF THE HOUSE OF REPRESENTATIVES

SPEECH

Date	Thursday, 20 September 2018	**Source**	House
Page	9671	**Proof**	No
Questioner		**Responder**	
Speaker	Dutton, Peter, MP	**Question No.**	

Mr DUTTON (Dickson—Minister for Home Affairs) (11:34): I move:

That this bill be read a second time.

New communications technology, including encryption, is eroding the capacity of Australia's law enforcement and security agencies to investigate serious criminal conduct and protect Australians.

The Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 contains amendments to various legislation to create a package of reforms that strengthens the ability of Australia's law enforcement and national security agencies to deal with the challenges of encryption.

Encryption underpins modern information and communication technology. It is a tool that protects personal, commercial and government information and supports confidence in a secure cyberspace. These technologies allow us to confidently transact online and to use the internet for services such as banking and shopping.

However, criminal syndicates and terrorists are increasingly misusing and, indeed, exploiting these technologies.

Terrorist organisations in Australia and overseas are using secure messaging services to obscure their identities and plans from the authorities. For example, ISIL-inspired terrorists used secure messaging services to plan the November 2015 Paris attacks.

The lack of access to encrypted communications presents an increasingly significant barrier for national security and law enforcement agencies in investigating serious crimes and national security threats.

According to ASIO, encryption has impacted intelligence operations in at least nine out of every 10 of its priority cases.

The AFP advise that encrypted communications have directly impacted around 200 operations conducted by the AFP in the last 12 months, all of which related to the investigation of serious criminal offences carrying a penalty of seven years imprisonment or more.

The uptake of encrypted communications platforms by criminal and terrorist groups has been sudden. It represents a seismic shift in the operational environment for our law enforcement and security agencies.

In June 2013, only three per cent of internet communications intercepted by ASIO, under warrant, were encrypted. By 1 July 2017, that figure had increased to more than 55 per cent. Most of the material of intelligence value is in the encrypted proportion.

Similarly, more than 90 per cent of data lawfully intercepted by the AFP is now encrypted in some form.

No responsible government can sit by while those who protect our community lose access to the tools they need to do their job. In the current threat environment, we cannot let this problem get worse.

The bill represents a package of reasonable and proportionate measures which will enhance our approach. The government has undertaken extensive industry and public consultation on the bill and has made amendments to account for the constructive feedback received.

Outline of Measures in the Bill

Industry assistance, including technical assistance and technical capability warrants

The supply of communications is a global industry. With major technology providers headquartered overseas, we must work with international partners to adapt to a world characterised by ubiquitous encryption.

The communications industry is in a unique position to assist in tackling the challenges we face.

Encrypted products are developed and operated by a range of private providers—both inside and outside of Australia—and in a range of forms across the communications supply chain.

National security and law enforcement agencies already work cooperatively with industry partners on these issues, to protect Australians.

The bill seeks to enhance those existing relationships to achieve lawful and non-arbitrary access to available information in the context of serious criminal and national security threats.

It complements the existing obligations of domestic service carriers to provide reasonable assistance to law enforcement under the Telecommunications Act 1997.

The bill facilitates a multilevel approach to industry assistance, creating a framework to support the wide range of providers that assist law enforcement and intelligence agencies voluntarily, including foreign providers.

This is reinforced and clarified by the creation of two new powers: the technical assistance notice and the technical capability notice.

Technical assistance notices will be issued by an agency head or their delegate to compel assistance that a provider is capable of giving.

Technical capability notices will be issued by the Attorney-General and require a company to take reasonable steps to develop and maintain a capability to respond to agency requests.

The legislation will not weaken encryption or mandate backdoors into encryption. The bill specifically provides that companies cannot be required to create systemic weaknesses in their encrypted products, or be required to build a decryption capability.

This is also not a new vehicle to collect personal information. Surveillance and interception must be authorised by existing warrants and authorisations, which are subject to their own safeguards, including judicial oversight.

The bill requires that any obligations within a technical assistance notice and technical capability notice are reasonable, proportionate, practicable and technically feasible. We are not in the business of asking industry to do the impossible.

The legislation provides for cost recovery by providers for complying with new requirements and also provides immunity from civil liability.

Alternative capabilities for law enforcement

Modern information and communications technology has provided more ways to stay connected and to store information. These capabilities include a wide variety of electronic protection. Agencies need expanded capabilities to adapt and to meet the needs of the evolving digital environment.

To this end, the bill provides law enforcement agencies with additional powers for overt and covert computer access. Computer access involves the use of software to collect information directly from devices. Commonwealth, state and territory law enforcement agencies would be able to use this power to investigate offences with a federal aspect.

The Surveillance Devices Act will include a new covert computer access power for law enforcement, like those powers currently available to ASIO. This will enable law enforcement agencies to apply for computer access warrants when investigating serious federal crimes with a maximum penalty of three years imprisonment or more, including terrorism and child exploitation.

The cross-border storage of information and overseas location of service providers makes Australia's mutual assistance framework critical in enabling Australian and foreign authorities to gain access to information to inform investigations and to obtain evidence. Under that framework, foreign authorities will be able to make a request to the Attorney-General to authorise an eligible law enforcement officer to apply for, and execute, a computer access warrant to assist in a foreign investigation or investigative proceeding.

Amendments will be made to the Crimes Act search warrant framework to ensure law enforcement officers do not have to physically be on premises in order to access a computer under a search warrant.

Amendments to the Customs Act will enable a judicial officer to issue a search warrant authorising the ABF to search a device (such as a smartphone) held on a person. Currently, devices can only be searched when found on a premise or premises.

The Crimes Act and the Customs Act will be amended to increase the maximum penalty for a person who fails to provide assistance to law enforcement in accessing a device which is the subject of a search warrant. These assistance orders must be issued by a judicial officer. The maximum penalty will be increased to five years. An aggravated offence will be created for serious offences like espionage, terrorism, child exploitation and pornography, with a maximum penalty of 10 years imprisonment.

The increased penalties for noncompliance with orders for access to a device reflect the value of evidentiary material on devices and the fact that persons who have undertaken criminal activity would rather accept the current low penalties than provide data that could be evidence in a more serious prosecution.

Given the increased complexity of devices and higher volumes of data stored, law enforcement agencies will now have 30 days to conduct forensic examinations of seized computers and data storage devices. This is an increase on the currently inadequate 14-day time frame for police forces and 72-hour period for the Australian Border Force.

ASIO p owers

ASIO is responsible for investigating some of the gravest threats to Australia's national security, including espionage, terrorism and attacks on Australia's defence systems.

ASIO's ability to collect intelligence using traditional means, such as telecommunications interception, is declining due to encryption.

To mitigate this decline, the bill will introduce a new framework to ensure that persons and bodies who voluntarily assist ASIO are given appropriate legal protections for this assistance. The purpose of this new framework is to give members of the public the highest degree of confidence that they may lawfully help ASIO to protect Australia's national security.

Conclusion

The bill demonstrates the government's commitment to ensuring that law enforcement and national security agencies have the tools they need to keep Australians safe. The government has consulted extensively with industry and the public on these measures and has made amendments to reflect the feedback in the legislation now before the parliament. The government is committed to ensuring that our legislative response to the challenges of an evolving technological landscape is reasonable, is proportionate and meets national security and law enforcement needs. I commend this bill to the House.

Debate adjourned.

Apple, Inc.

**SUBMISSION TO THE
PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY (PJCIS)
ON THE
TELECOMMUNICATIONS AND OTHER LEGISLATION AMENDMENT (ASSISTANCE AND ACCESS) BILL 2018**

Apple shares this Committee's commitment to security. We have a long history of cooperating with the Australian government on critical issues and we thank the Parliament for allowing us this opportunity to share our perspectives on this topic.

We take technology's role generally —and Apple's role specifically — in protecting national security and citizens' lives extremely seriously. Even as we strive to deliver delightful experiences to users of iPhones, iPads, and Macs, our team works tirelessly to stay one step ahead of criminal attackers who seek to pry into personal information and even co-opt devices for broader assaults that endanger us all. These threats only grow more serious and sophisticated over time.

It is precisely because of these threats that we support strong encryption. Every day, over a trillion transactions occur safely over the internet as a result of encrypted communications. These range from online banking to credit card transactions to the exchange of healthcare records, from photos of a new grandchild to messages exchanged between loved ones. The threats to those communications and data are very real and increasingly sophisticated.

According to the Australian government's Notifiable Data Breaches database, there were 2.5 or more data breaches per day over the last reporting quarter — and that's just breaches that were identified and reported. These attacks have not only exploited users' personal information, they have also targeted critical infrastructure. Last year, for example, the infamous NotPetya rendered useless tens of thousands of computers at multinational corporations and hospitals. It hit Australia hard — effectively shutting down Cadbury's manufacturing operation and impacting other firms.

The devices you carry not only contain personal emails, health information and photos but are also conduits to corporations, infrastructure and other critical services. Vital infrastructure — like power grids and transportation hubs — become more vulnerable when individual devices get hacked. Criminals and terrorists who want to infiltrate systems and disrupt sensitive networks may start their attacks by accessing just one person's smartphone.

In the face of these threats, this is no time to weaken encryption. There is profound risk of making criminals' jobs easier, not harder. Increasingly stronger — not weaker — encryption is the best way to protect against these threats.

The encryption technology built into today's iPhone represents the best data security available to consumers. And cryptographic protections on the device don't just help prevent unauthorized access to your personal data — they're a critical line of defense against a criminal who seeks to implant malware or spyware, and use the device of an unsuspecting person to gain access to a business, public utility or government agency.

We also challenge the idea that weakening encryption is necessary to aid law enforcement. We continue to work with the Australian government and other law enforcement agencies around the world in the shared interest of public safety. In just the past five years alone, we have processed over 26,000 requests from Australian law enforcement agencies for information to help investigate, prevent and solve crimes. We recently announced efforts to expand our law enforcement training efforts so that we can help law enforcement officers understand how they can obtain information from Apple consistent with our legal guidelines. In fact, we conducted extensive law enforcement training in Australia last month. Like we have always done, we will continue to work with Australian authorities in connection with lawful investigations.

We appreciate the government's outreach to Apple and other companies during the drafting of this bill. While we are pleased that some of the suggestions incorporated improve the legislation, the unfortunate fact is that the draft legislation remains dangerously ambiguous with respect to encryption and security.

We encourage the government to stand by their stated intention not to weaken encryption or compel providers to build systemic weaknesses into their products. Due to the breadth and vagueness of the bill's authorities, coupled with ill-defined restrictions, that commitment is not currently being met. For instance, the bill could allow the government to order the makers of smart home speakers to install persistent eavesdropping capabilities into a person's home, require a provider to monitor the health data of its customers for indications of drug use, or require the development of a tool that can unlock a particular user's device regardless of whether such tool could be used to unlock every other user's device as well. All of these capabilities should be as alarming to every Australian as they are to us. While we share the goal of protecting the public and communities, we believe more work needs to be done on the bill to iron out the ambiguities on encryption and security to ensure that all Australians are protected to the greatest extent possible in the digital world.

To be effective, laws need to be clear and unambiguous. It is imperative that this law include a firm mandate that prohibits the weakening of encryption or security protections. Encryption is the single best tool we have to protect data and ultimately lives. Software innovations of the future will depend on the foundation of strong device security. To allow for those protections to be weakened in any way slows our pace of progress and puts everyone at risk.

Some suggest that exceptions can be made, and access to encrypted data could be created just for only those sworn to uphold the public good. That is a false premise. Encryption is simply math. Any process that weakens the mathematical models that

protect user data for anyone will by extension weaken the protections for everyone. It would be wrong to weaken security for millions of law-abiding customers in order to investigate the very few who pose a threat.

We urge the government to seriously consider the comments submitted by industry and civil society and consider changes that would protect the security and privacy of Apple's users and all Australians.

Specific Concerns

While the bill presents many questions and opportunities for clarification, we focus our comments on several overarching themes: (1) overly broad powers that could weaken cybersecurity and encryption; (2) a lack of appropriate independent judicial oversight, (3) technical requirements based only on the government's subjective view of reasonableness and practicability, (4) unprecedented interception requirements, (5) unnecessarily stifling secrecy mandates, and (6) extraterritoriality and global impact.

(1) Overly Broad Authorities Could Weaken Cybersecurity and Encryption

Though the government has provided some assurance that they will interpret the bill's provisions to preserve strong encryption, future governments could interpret the bill's broad and vague terms quite differently, wielding its provisions to weaken encryption. This is not to say that the government's efforts have been for naught; Apple is appreciative of the government's inclusion of language that prohibits requiring a provider "to implement or build a systemic weakness or systemic vulnerability," or prevent remediation of "a systemic weakness, or a systemic vulnerability." Similarly, we appreciate the bill's clarification that a provider cannot be compelled to make changes that would render systemic methods of encryption or authentication "less effective."

Despite this encouraging language, the bill grants extraordinarily broad and vague powers that, the government may argue, allow them to force companies to build tools that ultimately weaken the security of their products or create significant cybersecurity risks more broadly.

For instance, the government may seek to compel a provider to develop custom software to bypass a particular device's encryption. The government's view is that if it only seeks such tool for a particular user's device, it will create no systemic risk. As we have firmly stated, however, the development of such a tool, even if deployed only to one phone, would render everyone's encryption and security less effective.

Additionally, the government may seek to compel providers to install or test software or equipment, facilitate access to customer equipment, turn over source code, remove forms of electronic protection, modify characteristics of a service, or substitute a service, among other things. The potential of each and every one of these actions undermines

consumer trust in the security of commercial products and the privacy of the data they place on them.

Moreover, key terms in the bill are undefined, leaving the government ample room to interpret them in myriad ways, further undercutting the bill's limitations. Most notably, perhaps, are the absence of definitions for "systemic weakness" and "systemic vulnerability." Without clearly defined parameters, we see no reason why the government could not seek to prevent particular users from receiving general security updates or prohibit providers from fixing mere security flaws that impact large numbers of customers but that may not qualify as "systemic" in the government's eyes.

What is clear, is that without well-defined terms and narrowly tailored parameters, the government could compel providers to weaken critical protections that safeguard their customers' most sensitive personal data.

(2) Insufficient Judicial Review Reduces Customer Trust and Security

Independent judicial review is a necessary component of any surveillance statute and has been included regularly in similar legislation around the word. See Investigatory Powers Act 2016, Section 23 (United Kingdom); Foreign Intelligence Surveillance Act, 50 U.SC. §1861 (United States). At best, the proposed bill is unclear with respect to the scope and breadth of the available judicial review. At worst, it fails to provide for vital oversight and redress procedures.

As a threshold matter, we are concerned that independent judicial review is not required before the government may issue a technical assistance notice (TAN) or technical capability notice (TCN). We urge the government to consider a provision similar to one in the United Kingdom's Investigatory Powers Act that requires judicial review of a proposed technical capability notice before such notice can be served on a provider. We believe that any bill permitting the government to mandate sweeping technical changes that could jeopardize the security and privacy of countless users should require approval by an independent judicial body *prior* to issuance of such a directive.

The bill's lack of pre-issuance judicial review notwithstanding, the scope of post-issuance judicial review is unclear. Though the Explanatory Document accompanying the bill states that Australian courts "retain their inherent powers of judicial review of a decision of an agency head or the Attorney-General to issue a notice," it appears that review is limited to whether a decision to issue a directive was made *lawfully*, not that the "proper" decision was reached. (Explanatory Document, p. 11).

Separately, the bill and Explanatory Document reference the possibility of the appointment of an arbitrator in "exceptional cases where providers and government disagree on the terms and conditions for compliance with a notice." (Section 317ZK; Explanatory Document, pp. 48-49). The legislation itself does not describe the circumstances or criteria that would qualify as an "exceptional case," nor the nature of

disagreement over "terms and conditions" that would allow for the appointment of an arbitrator, but the Explanatory Document makes clear that the appointment of an arbitrator only applies to disagreement over cost-sharing arrangements borne by the provider and the government associated with compliance.

Australian law already contemplates a substantive merits review that allows an independent arbiter to assess the facts, law, and policy dimensions of the government's actions. We believe that the bill should be amended to ensure adequate judicial oversight prior to and after issuance of a TAN or TCN.

(3) Determinations Based Only on Government's Subjective View Gives Short Shrift to the Realities of Modern Consumer Technologies

We are concerned that key factual determinations depend only on the government's assessment of the circumstances and technical complexities. Whether a TAN or TCN is "reasonable" and "proportionate" or whether compliance with a notice is "practicable" and "technically feasible" should not rest only on the government's view, but should take into account the views of security experts, academics, and privacy considerations. Reliance on the government's subjective view invites uncertainty, confusion, and potential abuse.

We applaud the government's recent addition to the bill that requires the government to issue a "consultation notice" prior to issuance of a TAN or TCN. In particular, we are pleased to see that the government and a provider may jointly appoint an expert to assess whether a proposed TCN complies with the law's limitations. We believe this new provision could be strengthened, at a minimum, to require the government to seek judicial approval if it intends to issue a TCN despite significant reservations identified in the assessment.

Though this new provision is welcome, the bill still gives undue weight to the government's interpretation of the law's terms and the technical facts. For instance, if the government believes that a particular measure is reasonable and proportionate, it would matter little that a wide swath of security experts and technology companies believe it to be dangerous and irresponsible.

To ensure that the government's orders do not weaken vital security protections, the appropriate standard of review should be objective, balancing the government's prerogatives with technical realities.

(4) The Bill Creates Broad New Intercept Authorities for Domestic Intelligence

Among the bill's provisions is new authority that could permit the Australian Security Intelligence Organization (ASIO) to require that providers build intercept capabilities that, until now, Australian law has prohibited. We are deeply concerned that the government may seek to force providers to provide real-time interception of messages or internet-based audio or video calls should the law pass in its current form. The bill

must be clarified to ensure that no new intercept capabilities can be ordered for encrypted systems.

On its face, the bill seems to forbid the government from requiring a provider to maintain an interception capability. Yet, like the bill's other purported limitations, the exceptions swallow the rule. Here, the limitation does not apply to ASIO computer access warrants, which can authorise access to a targeted computer to gather intelligence. This bill would allow ASIO to issue an order to a provider to build a capability to intercept encrypted communications to and from a particular device.

If the government's intent is to so expand the authority of ASIO, it would be an unprecedented step for Australia. Ordering providers to develop capabilities that would allow the government to eavesdrop on their customers would undermine security and shake confidence in the very technology that users rely on to process financial transactions, communicate sensitive information to their family members, or send intimate health data to healthcare providers.

In meetings, the government assured us that the bill does not expand intercept authority beyond what is authorised in the Telecommunications (Intercept and Access) Act of 1979 (TIA Act). The government must explicitly clarify that the bill does not expand such powers beyond the TIA Act.

(5) The Bill Contains Unnecessarily Stifling Secrecy Requirements

Transparency is a necessary and important piece of any lawful access authority. We are pleased that the bill allows disclosure of the number of TANs and TCNs a provider receives for aggregate statistical purposes.

The bill's stiff penalties for unauthorised disclosure, however, are too broad and could stifle innocent disclosures or disclosures for the purpose of reporting abuse. For instance, if an engineer working for a provider tasked with complying with a TCN had a legitimate legal or ethical concern, they could be imprisoned for five years for merely disclosing the fact of a TCN to his or her employer's human resources office. Similarly, an employee of a provider who legitimately believed a TAN or TCN violated the law, could not disclose that concern for fear of punishment.

We understand that the Government has an important interest in maintaining secrecy in appropriate circumstances. Yet we believe that there is a balance between such secrecy and giving providers, their customers, and their employees confidence that the laws are being executed properly and lawfully.

(6) Extraterritoriality and Global Impact

We are pleased that the latest draft of the bill makes clear that in civil proceedings against a provider for noncompliance with a TAN or TCN, the provider may claim as a

defense, that compliance would contravene a foreign jurisdiction's law. This is a welcome step, but does not fully address the bill's extraterritorial application.

Like Australia, many foreign countries have laws that prevent (in some cases in the form of criminal penalties) a party from accessing, altering, or providing access to a communications system or data storage device. Accordingly, a TAN or TCN may require an act or omission which, if carried out, would breach the law of a foreign country. In addition to suffering potential criminal liability for complying with a TAN or TCN in a foreign country, a provider may also suffer severe civil liability.

Even though this bill grants immunity for compliance with a TAN or TCN, it does not and cannot extend that immunity to cover liability in foreign jurisdictions. For instance, most user content is stored in the United States and U.S. law controls access to that data by law enforcement. Failure on the part of any U.S. entity to follow those requirements gives rise to criminal and civil liability. Most relevant, Title III of the U.S. Omnibus Crime Control and Safe Streets Act would subject Apple to criminal sanctions for any unauthorised interception of content in transit, which this bill could permit. If Australian authorities were to issue a TAN or TCN that required access to data of European Union citizens, Apple could face stiff penalties of up to 4% of its annual turnover under the General Data Protection Regulation, were it to comply.

Forcing business with operations outside Australia to comply with TANs or TCNs that violate the laws of other countries in which they operate, will just incentivize criminals to use service providers that never assist Australian authorities or ones that operate underground in jurisdictions unfriendly to Australian interests. Rather than serving the interests of Australian law enforcement, it will just weaken the security and privacy of regular customers while pushing criminals further off the grid.

Though we are encouraged by the bill's new language, we believe that the law should draw clear lines that do not put providers in criminal and civil jeopardy for violations of foreign law.