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.