THOUGHTWORKS AUSTRALIA SUBMISSION

Parliamentary Joint Committee on Intelligence and Security
Review of the
Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

22 February 2019

ThoughtWorks Australia is a custom software development firm employing over 300 people in Australia. We are part of a worldwide firm of some 5000 people across 40 offices in 14 countries. We build business software including websites, mobile applications, and complex solutions. We also provide IT consulting services for many leading organisations in Australia and the world.

ThoughtWorks welcomes the opportunity to make a submission on the Assistance and Access Act, despite it being among the worst examples of policy making we have witnessed. Shortcomings include: inadequate consultation with stakeholders; inordinate haste in passage through the parliament, with 67 pages of quickly-drafted amendments passed without debate on the very day they were tabled; and a review of their implication occurring after the fact of Royal Assent.

ThoughtWorks broadly associates itself with the submission of the Communications Alliance, of which we are a member, as well as many points made in the Australian Civil Society Coalition submission. We note an unprecedented unanimity among the business, academic, and civil society sectors on the damage wrought by the improper process to complex policy change as well as the intended and unintended consequences of the content of the legislation, which:

- **compromises the trust, standing and therefore economic viability of Australian tech firms,** particularly SMEs, on which there will be significant impact;
- **contains insufficient safeguarding of the data of Australians;**
- **contains unprecedented powers with an unreasonably broad remit;**
- **threatens to drive firms overseas due to the extraordinary secrecy provisions about capability notices,** reducing customers' confidence in products and services originating in Australia.

Breaking a secure system for one person necessarily makes it insecure for everyone who uses it. Because this legislation has the direct and inevitable consequence of compromising the integrity of cryptographic systems, ThoughtWorks rejects the assertion that the government is not interested in breaking encryption. Whilst the Assistance and Access Act may not explicitly mandate the breaking of cryptographic algorithms, it requires tech companies to compromise/break the security of their systems and their users' data. Regardless of how tech companies implement the surveillance mechanisms requested, the potential outcome in terms of digital security is devastating.

Once it is understood that code can be deployed secretly against users of a system, that system (and all systems that depend on it) cannot be viewed as reliably secure. If one device

is rendered insecure, for example, by a surveillance mechanism applied by a software author or a government, all users of that kind of device should, from that point, consider it vulnerable.

ThoughtWorks wishes to underline recommendations for amendments that would:

- **Repeal the legislation** and commence a democratic process towards an alternative;

- **Introduce a warrant-based system with judicial consent to Technical Assistance Notices (TANs) and Technical Capability Notices (TCNs)** and their respective variations. We concur with others that it is only appropriate that the far-reaching powers granted by the legislation are supervised by an eligible judge;

- **Adequately define the terms 'systemic weakness/vulnerability' and 'target technology'.** The current definitions, particularly of what constitutes a 'class of technology' are incoherent and ambiguous. As experts in cryptography, Dr Chris Culnane and Associate Professor Vanessa Teague, have stated, the current definition of a systemic weakness "...allows law enforcement to demand modifications that undermine the cybersecurity of millions of people, as long as something less than 'a whole class of technology' is affected."

- **Increase the threshold triggers for the legislation to that of a serious offence to be consistent with other interception and access regimes.** Currently this legislation is triggered by any "serious crime" including those punishable by a period of 3 years or more of imprisonment. This is inconsistent with the Telecommunications (Interception and Access) Act. This legislation should be triggered by serious crimes with stated targets or offences punishable by imprisonment for life or for a period, or maximum period, of at least 7 years;

- **Appoint sufficiently-independent assessors, with whom the Attorney General is obliged to engage.** It compromises the independence of the assessors to be appointed by the Attorney General, who currently need only 'have regard' to their recommendations. We concur with others that this is a weakened safeguard.

- **Repeal the insufficiently precise provisions that compel a person with knowledge of a computer or a computer system to assist** with providing access to a computer (s 114, the new s 64A of the *Surveillance Devices Act*). ThoughtWorks concurs with others that a limit on the use of this power is necessary, as well as clarification of what a technologist can be required to do while also protecting the public interest in security of digital infrastructure. We remain deeply concerned that those technologists who feel morally compelled to withhold their assistance could be jailed for 5 years.

- **Recognise the full costs of compliance.** While the new Explanatory Memorandum of the legislation acknowledges that the cost of compliance might not be reasonable, there is no recognition that while companies can be compensated for work done, there is no provision for compensation for damage of reputation and standing of products and services that may be perceived as broken by the market.