Chapter 4

Responding to the encryption challenge

4.1 As discussed in Chapter 1, the increasing prevalence of encrypted data and communications represents a significant challenge to current investigative and interception capabilities in law enforcement. As the Australian Securities and Investments Commission (ASIC) stated:

> While encryption has clear benefits in safeguarding the privacy and security of sensitive data, it poses challenges for law enforcement agencies in obtaining access, in appropriate cases, to the encrypted content and devices.[1]

4.2 The Australian Criminal Intelligence Commission (ACIC) and Australian Institute of Criminology (AIC) emphasised the increasing role of encrypted communication devices and applications in criminal activities:

> Increasingly, criminal activities are committed with the assistance of technology either via the online environment or through advances in technological capabilities, such as secure communications which include but are not limited to communication devices with military grade encryption, remote wipe capabilities, duress passwords and secure cloud-based services…The online environment enables crime to be committed with relative anonymity, a characteristic that is attractive to serious and organised crime groups and other motivated individuals, making the identification and prosecution of offenders more difficult.[2]

4.3 Similarly, ISACA noted that nations across the world have been grappling with the encryption challenge for several years, and submitted that the most effective way to address this challenge is to focus law-enforcement efforts on research and development.[3]

4.4 Drs Monique Mann, Adam Molnar, Ian Warren and Angela Daly, Australian Privacy Foundation, Digital Rights Watch Australia, Electronic Frontiers Australia and Future Wise noted that governments continue to argue for greater powers to address the encryption challenge:

> The rationale behind this argument is that encrypted messaging apps are having detrimental impacts on their ability to prevent, detect and investigate serious crimes such as terrorism and the distribution of child exploitation

---

1 Australian Securities and Investments Commission (ASIC), *Submission 11*, p. 6.

2 Australian Criminal Intelligence Commission (ACIC) and Australian Institute of Criminology (AIC), *Submission 29*, p. 4.

3 ISACA, *Submission 13*, [p. 7].

> material. Accordingly, these agencies insist that further powers are needed to enable access to encrypted communications.[4]

4.5 Dr Mann et al rejected this claim, instead arguing that:

> In spite of any claims that end-to-end encryption tools introduce insurmountable obstacles for intelligence gathering and criminal investigation, we insist that our present digital age offers an unparalleled opportunity for intelligence gathering and criminal investigation compared with any previous point in history. Australian authorities already have extensive technical and legal capabilities at their disposal to gather, store, and analyse social and geolocational data to facilitate operations.[5]

Five Eyes Alliance Statement of Principles

4.6 As outlined in Chapter 2, the Five Eyes Alliance is an intelligence alliance formed in 1946 and now comprising the United Kingdom (UK), United States (US), Canada, Australia and New Zealand (NZ).

4.7 On 26 June 2017, the Five Country Ministerial Meeting of the Five Eyes Alliance partners discussed the shared challenge of encryption, noting that it can severely undermine public safety efforts by 'impeding lawful access to the content of communications during investigations into serious crimes'. In response, the partners committed to engaging with communications and technology companies to explore shared solutions which 'proportionately balance the cybersecurity and the rights and freedoms of individuals'.[6]

4.8 On 29 August 2018, a joint meeting was held between the Attorneys-General and Interior Ministers from the Five Eyes nations to further discuss encryption and the problem of 'going dark'. This meeting resulted in the development of a framework for discussion with industry to resolve the challenge of encryption 'while respecting human rights and fundamental freedoms'.[7]

4.9 The agreement was set out in the Five Eyes Alliance *Statement of Principles on Access to Evidence and Encryption* (Statement of Principles), affirming:

> (i) a mutual public safety responsibility between governments and technology providers that obliges assistance, while recognising the need to 'ensure the ability of citizens to protect their sensitive data';

---

4 Dr Monique Mann, Dr Adam Molnar, Dr Ian Warren and Dr Angela Daly, Australian Privacy Foundation, Digital Rights Watch Australia, Electronic Frontiers Australia and Future Wise, *Submission 23*, p. 11.

5 Dr Monique Mann et al, *Submission 23*, p. 12.

6 Department of Home Affairs (DHA), Attorney-General's Department (AGD) and Australian Border Force (ABF), *Submission 28*, p. 17.

7 DHA, 'Five Country Ministerial 2018: official communiqué', *Media release*, 30 August 2018, p. 3.

(ii) the primacy of the rule of law and due process protections to ensure that 'lawful access should always be subject to oversight by independent authorities and/or subject to judicial review'; and

(iii) '[f]reedom of choice for lawful access solutions' so that technology providers can 'voluntarily establish…customised solutions, tailored to their individual system architectures that are capable of meeting lawful access requirements'.[8]

4.10 The Statement of Principles explain that 'appropriate government authorities should be able to seek access to otherwise private information when a court or independent authority has authorised such access based on established legal standards', similar to the principle that allows government authorities to search homes, vehicles, and personal effects with valid legal authority.[9]

4.11 The Statement of Principles notes the 'increasing gap between the ability of law enforcement to lawfully access data and their ability to acquire and use the content of that data'. It indicates that each of the Five Eyes jurisdictions will consider how best to implement the principles, including with the voluntary cooperation of industry partners.[10]

Five Eyes encryption laws

4.12 Of the Five Eyes partners, the UK and New Zealand have existing laws obliging industry to assist with access to encrypted communications, whereas the US and Canada have not as yet amended existing provisions to impose comparable requirements on technology providers.[11]

4.13 The *Investigatory Powers Act 2016* (UK) extends the Secretary of State's power to issue 'technical capability notices to require telecommunications operators to

8 Five Country Ministerial/Quintet Meeting of Attorneys-General Australia 2018, 'Statement of principles on access to evidence and encryption', DHA, 30 August 2018, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22media%2Fpressrel%2F6345572%22 (accessed 21 January 2019).

9 DHA, 'Statement of Principles on Access to Evidence and Encryption', https://web.archive.org/web/20180925154820/https://www.homeaffairs.gov.au/about/national-security/five-country-ministerial-2018/access-evidence-encryption (accessed 22 January 2019).

10 DHA, 'Statement of Principles'.

11 *Investigatory Powers Act 2016* (UK), http://www.legislation.gov.uk/ukpga/2016/25/contents; and *Telecommunications (Interception Capability and Security) Act 2013* (NZ), http://www.legislation.govt.nz/act/public/2013/0091/latest/DLM5177923.html (all accessed 21 January 2019).

maintain the capability to provide data in an intelligible format where it is proportionate, technically feasible and reasonably practicable to do so'.[12]

4.14 New Zealand's powers are broadly analogous to technical capability notices under the UK's legislation, whereby the New Zealand government can 'compel assistance from service providers to decrypt information in response to a warning provided by a "surveillance agency"'.[13]

Australia's new encryption laws

4.15 Australia was the first of the Five Eyes Alliance to introduce encryption legislation since the release of the Statement of Principles.

4.16 The Minister for Home Affairs, the Hon Peter Dutton MP, introduced the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 on 20 September 2018. The Explanatory Memorandum outlined the purpose of the legislation as follows:

> National security and law enforcement agencies already work cooperatively with industry and other partners in relation to a range of telecommunications interception matters. The Bill will enhance cooperation by introducing a new framework for industry assistance, including new powers to secure assistance from key companies in the communications supply chain both within and outside Australia (Schedule 1). It will also strengthen agencies' ability to adapt to a digital environment characterised by encryption by enhancing agencies' collection capabilities such as computer access (Schedules 2, 3, 4 and 5).
>
> The computer access powers in Schedules 2 to 5 will enable domestic law enforcement agencies to better assist international law enforcement partners by undertaking these powers on behalf of those partners where approved through Australia's mutual assistance framework. These powers recognise the fact that computers, communications and encryption are now global and perpetrators of crimes and terrorist acts have a global reach through these mediums. This will be based on the principle of reciprocity—that Australia will work with those who work with Australia—and any other conditions the Attorney-General deems appropriate.[14]

4.17 The Attorney-General, the Hon Christian Porter MP, referred the Bill to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) for consideration.

---

12 DHA, AGD and ABF, *Submission 28*, p. 17; see also Ms Esther George, Lead Cybercrime Consultant, International Association of Prosecutors, *Committee Hansard*, 29 March 2018, p. 46.

13 DHA, AGD and ABF, *Submission 28*, p. 17.

14 House of Representatives, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, *Explanatory Memorandum*, pp. 2−3, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6195 (accessed 12 December 2018).

4.18 Following a government request to expedite the inquiry, the Chair and Deputy Chair of the PJCIS issued a statement pointing to the committee's reviews of previous national security laws, stating that its reports had 'been carefully developed to ensure that new powers are proportionate and appropriately balanced with human rights and privacy, and that commensurate oversight and accountability is provided'.[15]

4.19 On 22 November 2018, the committee received advice from the Minister for Home Affairs that 'there was an immediate need to provide agencies with additional powers and to pass the Bill in the last sitting week of 2018'.[16]

4.20 The Minister explained that the request for acceleration of the committee's consideration of the Bill was made 'in light of the recent fatal terrorist attack in Melbourne and the subsequent disruption of alleged planning for a mass casualty attack by three individuals', and concern that Australia's agencies could not rule out the possibility that others may have been inspired to plan and execute terrorist attacks in the forthcoming Christmas-New Year period.[17] The committee stated in its Advisory Report that it accepted:

> …that there is a genuine and immediate need for agencies to have tools to respond to the challenges of encrypted communications. The absence of these tools results in an escalation of risk and has been hampering agency investigations over several years. As the uptake of encrypted messaging applications increases, it is increasingly putting the community at risk from perpetrators of serious crimes who are able to evade detection.[18]

4.21 The committee recommended that the Parliament immediately pass the Bill, following inclusion of amendments recommended by the committee in its Advisory Report. The committee also recommended that, once the Bill (as amended) was passed by the Parliament, the committee undertakes a review of the new legislation to be completed by 3 April 2019.[19] The Bill, with amendments, passed both Houses on 6 December 2018.

---

15 Parliamentary Joint Committee on Intelligence and Security (PJCIS), Joint statement by Chair and Deputy Chair, *Media release*, 22 November 2018, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/TelcoAmendmentBill2018/Media_Releases (accessed 21 January 2019).

16 PJCIS, *Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, December 2018, pp. 1−2, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/TelcoAmendmentBill2018/Report_1 (accessed 13 December 2018).

17 PJCIS, *Advisory Report*, p. 2.

18 PJCIS, *Advisory Report*, p. 2.

19 PJCIS, *Advisory Report*, Recommendation 1, p. 3 and Recommendation 16, p. 8. The Independent National Security Legislation Monitor is required to review its operation, effectiveness and implications after 18 months.

4.22 On 6 December 2018, the Senate referred the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (TOLA Act) to the PJCIS for review and report by 3 April 2019.[20]

Balancing privacy and risk

4.23 The provisions of the new legislation attracted debate in Australia and overseas. Some technology experts warned, for example, that despite the last-minute amendments, the legislation has the potential to damage the credibility of the ICT industry as a result of its provision for voluntary and mandatory industry assistance to help government access the content of encrypted communications.[21]

4.24 The credit ratings group Fitch observed that the new encryption laws would weaken the security of messages, and could harm Australia's flourishing tech sector as well as global operations of tech giants such as Google, Facebook and Apple.[22]

4.25 The Inspector-General of Intelligence and Security (IGIS) submitted to the PJCIS review of the TOLA Act that she had a number of outstanding concerns relating to the scope of IGIS oversight of the new and expanded powers contained in Schedules 2 and 5 to the Act.[23]

4.26 However, Mr Mike Burgess, Director-General of the Australian Signals Directorate (ASD), argued that the new legislation provided 'significant checks and balances' on law enforcement agencies, and was designed to target terrorists, paedophiles and criminals, not law-abiding Australians.[24]

---

20 See Review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/ReviewofTOLAAct (accessed 11 February 2019).

21 See, for example, P Smith, Y Redrup and A Tillett, '"As bad as Huawei": Australian encryption bill slammed after passing House of Reps', *Financial Review*, 6 December 2018, https://www.afr.com/technology/web/security/as-bad-as-huawei-australian-encryption-bill-slammed-after-passing-parliament-20181206-h18tk3; A Bogle, '"Outlandish" encryption laws leave Australian tech industry angry and confused', *ABC News*, 7 December 2018, https://www.abc.net.au/news/science/2018-12-07/encryption-bill-australian-technology-industry-fuming-mad/10589962 (all accessed 11 February 2019).

22 C Kruger, '"Negative for tech": Fitch slams encryption laws, *Sydney Morning Herald*, 13 December 2018, https://www.smh.com.au/technology/negative-for-tech-sector-fitch-slams-australia-s-new-encryption-laws-20181213-p50m55.html (accessed 20 December 2018).

23 Inspector-General of Intelligence and Security (IGIS), *Submission 1.1*, PJCIS, Review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, pp. 6−8. The overarching purpose of the IGIS's activities is to ensure that each intelligence agency acts legally and with propriety, complies with ministerial guidelines and directives, and respects human rights.

24 Mr Mike Burgess cited in A Probyn, 'Spy chief argues encryption laws target terrorists, not everyday Australians, in "myth-busting" missive', *ABC News*, 12 December 2018, https://www.abc.net.au/news/2018-12-12/encryption-laws-mike-burgess-australian-signals-directorate/10612570 (accessed 20 December 2018).

4.27 The Department of Home Affairs (DHA), Attorney-General's Department (AGD) and Australian Border Force (ABF) also pointed out—in their submission to this inquiry—that domestic carriers are already required under the *Telecommunications Act 1997* to provide 'reasonable assistance' to agencies seeking to implement warrants and enforce the law, and noted that the Australian government has stated that companies would not be required to build so-called 'backdoors'. In other words, encryption would continue to secure the private and sensitive information of businesses, governments and individuals.[25]

4.28 Several submitters and witnesses outlined what they saw as potential implications of the new encryption laws. Some raised broader concerns about 'bans', 'backdoors' or other 'weakening' of encryption technologies, and whether it was feasible to facilitate decryption by law enforcement agencies without also making it easier for criminals and foreign spy agencies to access the data.[26]

4.29 Others argued that weakening encryption tools will weaken security of digital communications generally, 'criminalising activities that are important for maintaining public safety, cyber security and digital innovation', as well as having a negative impact on individual privacy and freedom of expression.[27]

4.30 Drs Mann, Molnar, Warren and Daly stated that:

> While it might be the case that such proposals may facilitate law enforcement access to communications at a network-level scale, they will similarly do so for criminal hackers, organised criminals, or foreign state actors who acquire access. Computer scientists have noted that any introduction of a 'backdoor' vulnerability for law enforcement and security intelligence will similarly do so for malicious actors.[28]

4.31 They noted that Australian officials already have a range of selective and targeted technical and legal powers to address the issue of 'going dark'. These include existing powers, via amendments to the *Cybercrime Act 2001* (Cth) that introduced a new section 3LA under the *Crimes Act 1914* (Cth) to provide for lawful authorities to compel passwords, as well as existing powers to facilitate targeting hacking of end-point devices.[29]

---

25 DHA, AGD, and ABF, *Submission 28*, p. 16.

26 See for example, Dr Vanessa Teague, Melbourne School of Engineering, The University of Melbourne, *Submission 2*, [p. 3]; Dr John Coyne, *Submission 4*, p. 5; Pirate Party Australia, *Submission 16*, [pp. 6−7]; Dr Monique Mann, Co-Chair, Surveillance Committee, Board of Directors, Australian Privacy Foundation and Dr Adam Molnar, Vice-Chair, Australian Privacy Foundation, *Committee Hansard*, 29 March 2018, p. 16.

27 Dr Monique Mann et al, *Submission 23*, p. 12.

28 Dr Monique Mann et al, *Submission 23*, p. 13.

29 Dr Monique Mann et al, *Submission 23*, p. 14.

4.32 Mr Nathan White, Senior Legislative Manager, Access Now warned that enabling law enforcement agencies to bypass encryption poses security threats and is unlikely to solve law enforcement's problems, and advocated other means to assist law enforcement in dealing with cybercrime:[30]

> …undermining encryption hurts security. Every proposal for a mechanism to allow law enforcement to bypass encryption has been found to have security flaws that could, if deployed, cause great damage to people, governments and infrastructure. It could also have knock-on effects that we cannot anticipate today…undermining encryption will not solve law enforcement's problems. Principles of sovereignty and criminal incentives will likely drive law enforcement targets toward tools and technologies that are beyond the reach of any mandated access mechanism, leaving those who are less technically sophisticated or financially privileged to bear the brunt of any insecurity caused by the mandate.[31]

4.33 Dr John Coyne similarly argued that:

> …the idea that you can legislate your way out of the encryption challenge is deeply flawed….The bigger debate on this—and the public needs to know this—is that by wiring in back doors and by doing those sorts of approaches, we weaken and undermine all the benefits that come from encryption. It's part of our everyday life. It's what facilitates ease.[32]

4.34 The Law Council of Australia expressed concern that proposed powers contained in the Australian government's new encryption laws could have unintended consequences for the 'privacy and cybersecurity of individuals and regulation of the telecommunications sector'.[33] The Law Council considered that:

> …any restrictions on encryption and online anonymity must be provided for by law and are precise, public and transparent, must only be imposed for legitimate grounds under Article 19(3) of the ICCPR, and must conform to the strict tests of necessity and proportionality. This includes consideration of the possibility that encroachments on encryption and anonymity may be exploited by the same criminal and terrorist networks that the limitations deter.[34]

4.35 Dr Vanessa Teague, Melbourne School of Engineering, The University of Melbourne, stated that compliance to the new laws will only apply to encryption implemented by the company that owns the system, and that it is possible for a user to

---

30 Mr Nathan White, Senior Legislative Manager, Access Now, *Committee Hansard*, 11 May 2018, p. 2.

31 Mr Nathan White, Senior Legislative Manager Access Now, *Committee Hansard*, 11 May 2018, p. 2.

32 Dr John Coyne, *Committee Hansard*, 29 March 2018, p. 5.

33 Law Council of Australia, *Submission 21*, p. 11.

34 Law Council of Australia, *Submission 21*, p. 8.

install some encryption software from elsewhere and use it to encrypt files on that company's system.[35]

4.36 In response to the question as to whether it is possible to 'facilitate decryption by legitimate law enforcement, without also making it easier for bad actors such as criminals and foreign spy agencies to access the data too', Dr Teague responded 'No':

> The reason is simply that the legitimate law enforcement operatives are doing (for good reasons) exactly what criminals and other bad actors do: exposing someone else's data without their consent. Any change that makes this easier is likely, unfortunately, to make malicious hacking easier too. There are numerous examples of tools or weaknesses that were employed first for legitimate law enforcement and intelligence purposes, but were later shown to be exploitable by everyone (FREAK/Logjam, Dual-EC-DRBG, Wannacry).[36]

4.37 Ms Lizzie O'Shea and Ms Elise Thomas noted that overseas governments have had little success in regulating encryption, most recently in the UK where the *Investigatory Powers Act 2016* (UK) required technology companies to assist the government to decrypt messages where 'technically feasible':

> Approaches proposed or used in other countries include outright prohibitions on encryption, escrow of encryption keys, or limitations on the strength of encryption. Each of these has been demonstrated to have serious risks…Built-in weaknesses in encryption systems are not features that can be exploited only by the government; they can also be used by criminals and foreign enemies. Information about any backdoor will be highly valuable, and a honeypot for hackers, making it hard to keep safe.[37]

4.38 The Digital Industry Group Incorporated (DIGI) argued that great care must be taken in developing government policy around investigatory powers to ensure that the effectiveness of encryption technology is not comprised, stating that other countries have chosen alternative approaches to legislated intervention:

> A number of governments around the world have rejected such legal and market interventions in favour of a broader policy response which embraces international engagement, technical training for agencies, investment in new investigatory techniques and enhanced company engagement.[38]

4.39 The Law Council also noted that regulation of encryption by other nations has not been shown to be necessary when considering 'the breadth and depth of other tools, such as traditional policing and intelligence and transnational cooperation, that

---

35 Dr Vanessa Teague, Melbourne School of Engineering, The University of Melbourne, *Submission 2*, [p. 2].

36 Dr Vanessa Teague, Melbourne School of Engineering, The University of Melbourne, *Submission 2*, [p. 3].

37 Ms Lizzie O'Shea and Ms Elise Thomas, *Submission 15*, pp. 1−2.

38 Digital Industry Group Incorporated (DIGI), *Submission 20*, p. 6.

may already provide substantial information for specific law enforcement or other legitimate purposes'.[39]

4.40 DHA, AGD and ABF stated that legal frameworks need to be monitored regularly in order to keep pace with community expectations in this rapidly changing environment. Legal frameworks must 'balance the legitimate needs of law enforcement with the privacy, rights and freedoms of individuals'.[40]

4.41 DHA, AGD and ABF also noted that the legislative response will only ever address some of the law enforcement issues posed by encryption, and predicted that the continuing challenges posed by end-to-end encrypted communications mean that agency powers will need to be continually reviewed:[41]

> In this environment, it will be increasingly important for law enforcement agencies to utilise alternative methods to investigate serious crimes and combat threats to public safety and national security. For this purpose, the range of powers available to agencies must continually be examined.[42]

Committee view

4.42 Over recent years, the Australian government has introduced a series of legislative reforms with the aim of supporting law enforcement in their ability to respond to the threats posed by new and emerging ICTs.

4.43 The government's response to the challenges arising from new and emerging ICTs must balance the needs of law enforcement with the civil rights and liberties of Australians. The committee acknowledges there is an inherent tension between these and those engaged in this debate have, at times, strongly held and opposing views. It is for this reason that where the appropriate balance lies between law enforcement needs and civil rights and liberties must be resolved by the Australian government together with the Australian public, and not just by one or the other.

4.44 The committee accepts that there are cogent arguments put by government and law enforcement agencies for legislative reform to occur expeditiously. However, that need for swift enactment of law enforcement powers should not come at the expense of public engagement and debate on these issues.

4.45 The committee is aware that the UK government ran a seven week formal consultation process on its proposed amendments to the Investigatory Powers Act and the associated draft communications data code of practice, which provided 'more detail on how the new regime will work in practice'. The UK government stated that it 'does not normally consult on such regulations' but 'given the ongoing public interest

---

39 Law Council of Australia, *Submission 21*, p. 7.

40 DHA, AGD and ABF, *Submission 28*, p. 9.

41 DHA, AGD and ABF, *Submission 28*, p. 16.

42 DHA, AGD and ABF, *Submission 28*, p. 16.

in investigatory powers we consider it important to consult on potential changes to the legislative regime in order to inform the legislative response and subsequent Parliamentary debate'.[43]

4.46 The UK process was not without criticism, but the committee acknowledges the UK government's efforts to engage the public in the debate about the extent and appropriateness of certain investigatory powers for law enforcement in the cyber environment. The committee urges the Australian government to ensure that public consultation is undertaken when investigatory powers to tackle cybercrime are similarly amended or introduced in this country.

4.47 The committee acknowledges the public debate that has occurred in relation to the TOLA Act, and the range of different views amongst policymakers, law enforcement agencies, legal and technology experts, and users of ICTs, as to the most appropriate balance between law enforcement powers and human rights. The committee expects that the Australian government will carefully consider the views put and these will be appropriately reflected in the legislation.

4.48 The committee recognises that Australia's new encryption laws represent the first legislation to be introduced by a Five Eyes Alliance member since the release of the Alliance's Statement of Principles, and that the new legislation is entering new territory in extending law enforcement powers to access otherwise private information. The committee reiterates the view expressed by the DHA, AGD and ABF that the relevant legislative and regulatory regimes need to be continuously monitored and reviewed in order to identify, in a timely manner, gaps and constraints that may be limiting the ability of Australian law enforcement agencies to respond to the challenges of new and emerging ICTs.

4.49 The committee also considers that the powers given to law enforcement agencies must be subject to regular monitoring to ensure that the legislative and regulatory framework is keeping pace with new and emerging ICTs while respecting the human rights and fundamental freedoms of Australians.

4.50 To this end, the committee suggests that a task force would be an effective and flexible mechanism for monitoring the development of new and emerging ICTs and identifying gaps and vulnerabilities in Australia's law enforcement legislative and regulatory framework, as well as consulting and advising on the balance between investigatory powers and civil rights and liberties.

4.51 The committee envisages that such a task force would comprise ICT, legal, law enforcement and security experts (including academia), and be responsible for reporting to the Australian government at regular intervals on aspects of the legislative

43 Gov.UK, *Consultation outcome: Investigatory Powers Act 2016*, available: https://www.gov.uk/government/consultations/investigatory-powers-act-2016 (accessed 19 March 2019).

and regulatory framework that may require amendment in order for law enforcement to keep pace with this rapidly changing environment.

Recommendation 2

4.52 The committee recommends that the Australian government considers establishing a task force comprising information and communications technology (ICT), legal, law enforcement and security experts, including from academia, to:

- **monitor the development, and examine and advise on the impact of new and emerging ICTs on Australian law enforcement;**
- **identify specific gaps and vulnerabilities in the current legislative and regulatory frameworks that may be limiting the ability of Australian law enforcement agencies to investigate, disrupt or otherwise deal with cybercrime, including encryption services and encrypted devices;**
- **consult and advise on the balance between investigatory powers to tackle cybercrime and their impact on civil rights and liberties;**
- **report to the Australian government at regular intervals on the appropriateness of current legislative and regulatory frameworks; and**
- **recommend any changes that may be necessary to ensure that law enforcement agencies are keeping pace with and capable of tackling new cyber challenges as they arise.**