Australian Government
Department of Home Affairs

Joint Submission to the Inquiry into the Impact of New and Emerging Information and Communications Technology

Department of Home Affairs
Attorney-General's Department
Australian Border Force

Table of Contents

Glossary

Unless otherwise stipulated, the below definitions do not constitute official Australian Government definitions and should be considered for the purposes of this submission.

5G	The next cellular communications standard in development to replace existing 4G technology. Most commonly associated with providing wireless internet services to electronic devices. 5G is predicted to be in common use by 2020.
ABF	Australian Border Force
ACORN	Australian Cybercrime Online Reporting Network
AFP	Australian Federal Police
AGD	Attorney-General's Department
AI	Artificial Intelligence, Artificial intelligence is the simulation of intelligence processes by machines, especially computer systems. These processes include learning (the acquisition of information and rules for using the information), reasoning (using the rules to reach approximate or definite conclusions), and self-correction. Particular applications of AI include threat identification, expert systems, speech recognition and machine vision.
AML/CTF	Anti-money laundering and counter-terrorism financing
AMLCTFA Act	*Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017*
ASD	Australian Signals Directorate
ASIO	Australian Security Intelligence Organisation
AUSTRAC	Australian Transaction Reports and Analysis Centre
Bitcoin	A digital currency and payment system underpinned by blockchain technology. Bitcoins can be used for online purchases, or converted into traditional currency. Considered to be the first digital currency and as of January 2018 the largest by transaction volume and market capitalisation. Bitcoin also pioneered blockchain technology.
Blockchain	A distributed database that maintains a continuously growing list of records, called blocks, secured from tampering and revision. Each block contains a timestamp and a link to a previous block. By design, blockchains are inherently resistant to modification of the data — once recorded, the data in a block cannot be altered retroactively.
Dark web	The dark web is made up of sites that are not indexed by search engines and are only accessible through specialty networks such as Tor. Often, the dark web is used by website operators who want to remain anonymous. The ‘dark web’ is a subset of the ‘deep web’.
Deep web	The part of the internet that is not indexed by search engines. Includes websites that are password-protected and pay walled, encrypted networks and databases, and dynamic data such as social media feeds. Also includes the dark web.
Digital currency	Defined by the Financial Action Task Force on Money Laundering as: a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the digital currency.
Encryption	The conversion of electronic plaintext data into unreadable cipher text using algorithms. Encryption protects the confidentially of data at rest and in transit. Both encryption and decryption are functions of cryptography.
End to End Encryption	A method of secure communication where only the communicating users can read data transferred from one end system or device to another.

ICT	Information and Communications Technology, refers to any device that can process, store or communicate electronic information, for example; computers, mobile phones, etc.
Internet	The global system of interconnected computer networks that use standardised communication protocols to link devices and provide a variety of information and communication facilities.
IP	Internet Protocol (IP) is the technology which allows computers and other electronic devices to connect to the internet.
IPv6	Internet Protocol version 6
ISP	Internet Service Provider, a company that provides subscribers with access to the internet.
Mesh Network	A wireless mesh network combines multiple routers into a single and larger local network.
MLA	Mutual legal assistance
NPCC	National Plan to Combat Cybercrime
Over-the-top	Refers to when a telecommunication service provider delivers its services over or across an IP network.
PJCLE	Parliamentary Joint Committee on Law Enforcement
Router	A networking device that forwards data packets between computer networks.
SD Act	*Surveillance Devices Act 2004*
Silk Road	A now defunct illicit marketplace located on the dark web.
TIA Act	*Telecommunications (Interception and Access) Act 1979*.
Tor	'The Onion Router' (Tor) is free software used to anonymise access to the internet by routing data through multiple anonymised networks. Tor permits users to mask their usage and location, making it difficult to trace their activity. It is the most commonly used means to access the dark web.
Tumbler	A service whereby cryptocurrency is 'mixed' with additional funds in order to obfuscate the identity of those making the transaction. Tumblers were pioneered to enable purchases on the dark web.

Preface

1. The Department of Home Affairs, Australian Border Force and Attorney-General's Department (hereinafter 'the departments') welcome the opportunity to provide this joint submission ('the submission') to the Parliamentary Joint Committee on Law Enforcement ('the Committee') Inquiry into the impact of new and emerging information and communications technology (ICT) ('the inquiry'). The content of this submission is unclassified and suitable for public release.
2. On 20 December 2017, the Department of Home Affairs (Home Affairs) was formally established. Some policy areas of the Attorney-General's Department (AGD) with responsibility for national security and criminal law policy transferred to the new department. At the time of making this submission, AGD retains responsibility for encryption, electronic surveillance policy and aspects of child exploitation. These functions will transfer to Home Affairs in the first half of this year.
3. This submission responds to all the Terms of Reference of the inquiry (see Attachment A).
4. This submission is divided into two parts: Part 1 includes the introduction, background and context; Part 2 is divided as per the Terms of Reference.
5. The submission was jointly drafted by the departments. Responses particular to a department, agency or specific issue have been delineated under a sub-heading where necessary.
6. The departments note that the Australian Federal Police (AFP), Australian Criminal Intelligence Commission (ACIC) and Australian Transaction Reports and Analysis Centre (AUSTRAC) have provided separate submissions to the Committee.

Part 1: Introduction and background

Introduction

7. Australia's ability to harness the potential of digital technologies depends on the extent to which we can trust the internet and cyberspace. Strong cyber security is fundamental to our economic growth and is vital for our national security. Continued success in making the online environment safer will require partnerships between government, the private sector and the community. Within these partnerships, law enforcement and regulators play a particularly important and specialist role in enforcing the law, protecting our national interests, and protecting the community.

8. Cybercrime is attractive to criminals due to the relatively low costs of entry and the increasingly user-friendly nature of illicit services. Cybercrime now operates on an industrial scale, driven by the global commercialisation of cybercrime, the ability of sophisticated cyber criminals to adapt to technological advancements, and the rapid pace of technological change. With the prolific global rise of cybercrime, estimates suggest that it costs Australians between $1 billion to $17 billion annually. Cybercrime does not respect geographic or jurisdictional boundaries and this has made the challenges of keeping up with technological advancement a universal issue for law enforcement, regulators and national security agencies in Australia and overseas.

9. The Australian Government has recognised these challenges and has invested over $230m over four years to enhance Australia's cyber security capability. It has also appointed a National Cyber Security Adviser to lead cyber security policy, and head the Australian Cyber Security Centre (ACSC). Recognising the need to engage with our regional neighbours and international counterparts on cyber security, Australia's first Cyber Ambassador has been appointed within the Department of Foreign Affairs and Trade. The 2016 Cyber Security Strategy, and the 2017 International Cyber Engagement Strategy provide a high level policy framework to guide government, including law enforcement, contributions to a safer and more secure online environment.

10. Through the establishment of the Department of Home Affairs ('Home Affairs'), the Government has brought together the national security, emergency management and criminal justice functions from across government. In addition, Australian Federal Police (AFP), Australian Border Force (ABF), Australian Criminal Intelligence Commission (ACIC) and the Australian Transaction Reports and Analysis Centre (AUSTRAC) all now sit within the broader Home Affairs portfolio contributing to coordinated strategy across the portfolio. ASIO will join the portfolio in 2018.

11. Law enforcement agencies operate in an increasingly complex technological environment. Terrorists, child sex offenders, cyber criminals and organised crime syndicates are exploiting new technologies to communicate, commit and enable crimes. Technology is also increasingly used as an enabler of crime, with the majority of serious and organised crime using ICT for a variety of crime types. Technology is no longer limited to high tech crime types.

12. This is not solely a technology challenge. Domestic and international legal frameworks must also keep pace with rapid changes and technology and organisational cultures, policy and procedures must enable agencies to adapt more rapidly to changes in criminal behaviour.

13. Significant challenges also exist for the development and maintenance of an adequately skilled workforce. This is not a challenge faced by law enforcement in isolation. There are a range of difficulties in recruiting and retaining adequately trained staff, particularly in relation to ICT and cyber security disciplines. The Government is currently investing in education and training to increase the supply of skilled workers to the cyber security industry. This is an important step, but it is likely to take some time for supply to catch up with current and future demand. Governments will have to consider carefully how

the ICT and cyber security workforce and capabilities can be most effectively utilised across, rather than simply within, agencies.

14. Cybercrime continues to be a serious challenge for law enforcement. The 2016 Cyber Security Strategy includes a commitment to enhance the law enforcement capabilities to combat cybercrime, including: increasing the capabilities of the ACSC; a new multi-use facility for the ACSC scheduled to be opened in June 2018; additional funding for the AFP and ACIC; engaging our regional partners to shut down 'safe havens' for cyber criminals to name a few.

15. Criminals can simultaneously attack multiple victims across multiple states and territories, often from overseas. To have a real impact, law enforcement, regulatory and other agencies, both here and overseas, will need to work in close collaboration to make a real impact on cybercrime. A new National Plan to Combat Cybercrime, currently under development, will provide shared national priorities for law enforcement to enhance collaboration in the fight against cybercrime.

16. This submission should provide the Committee with an overview of the broader context within which many of the challenges of technology law enforcement, as well as a number of specific issues and experiences which form part of the responsibilities of the Attorney-General's Department, the Department of Home Affairs and Australian Border Force.

17. Individual agencies, including the AFP, ACIC and AUSTRAC have provided separate submissions to the Committee.

Background

The Department of Home Affairs

18. On 18 July 2017, the Prime Minister announced significant reforms to Australia's national security and intelligence arrangements, including the establishment of a Department of Home Affairs ('Home Affairs') and a Home Affairs Portfolio. These reforms were needed to preserve the operational focus and strength of frontline agencies engaged in the fight against terrorism, organised crime and other domestic threats.

19. On 20 December 2017, Home Affairs, including the Home Affairs portfolio, was formally established. Home Affairs is a central policy agency, providing coordinated strategy and policy leadership for Australia's national and transport security, federal law enforcement, criminal justice, cyber security, border, immigration, multicultural affairs, emergency management and trade related functions.

20. Home Affairs has an integral role in working with government, industry and law enforcement to ensure risks from emerging ICT are managed appropriately while simultaneously enabling the realisation of benefits from advances in technology. Among other things, Home Affairs is responsible for cyber security and cybercrime, transport security, domestic national security, serious and organised crime, anti-money laundering and counter-terrorism financing, immigration and border security. Technology is critical to the work of the entire Home Affairs portfolio. It plays a vital role in supporting our response to increasingly complex supply chains, the growing data and business volumes and the delivery of timely and accurate national security intelligence to respond to changes in the global environment.

21. The ABF operates in a unique, diverse and complex environment. The Australian border is not considered to be a purely physical barrier separating nation states, but a complex continuum stretching offshore (pre-border) and onshore (at and post-border), including the international, maritime, physical border and domestic dimensions of the border ('the border continuum'). The ABF provides the Government a mechanism to control people and goods that may enter, stay or exit Australia and under what conditions.

Attorney-General's Department

22. AGD delivers policies and programs to maintain and improve Australia's law and justice framework. The department supports the Attorney-General in his role as First Law Officer of the Commonwealth and in his oversight role of Australia's intelligence community and the agencies in the Home Affairs Portfolio.

23. On completion of the machinery of government changes, the Attorney-General's portfolio will incorporate the Inspector-General of Intelligence and Security and the Independent National Security Legislation Monitor. In addition, the portfolio will house the Commonwealth Ombudsman, which will remain an independent statutory body. Strong oversight and accountability is important to give the public confidence that our agencies not only safeguard our nation's security, but do so respecting the rights and liberties of all Australians.

Part 2: Response to the Parliamentary Terms of Reference

24. This section of the submission is structured against the Terms of Reference.

Challenges to law enforcement arising from new and emerging ICT

25. The evolution and emergence of new ICT presents unique challenges for Australian law enforcement as well as intelligence agencies. The evolving digital environment provides criminals with new avenues to commit a range of serious and complex crimes, including terrorism, firearms and drug trafficking, human trafficking and child sexual abuse. Extremist individuals and terrorist organisations are increasingly using social media and other online tools to facilitate and promote their activities. Similarly, online platforms provide unprecedented connection and storage for the easy sharing, promotion and discussion of child sexual abuse material. New technologies are also making these crimes more complex for law enforcement agencies to investigate. The use of cyber elements for criminal purpose is growing, creating unprecedented risks for both individuals and businesses. For example, according to the Australian Cybercrime Online Reporting Network (ACORN), reports of ransomware attacks doubled between 2016 and 2017.

26. Crimes can be committed across state and national borders, with the perpetrator located in one jurisdiction and the victim in another. This makes investigations more protracted, expensive and reliant on cooperation between multiple jurisdictions. Investigations into less serious cross-border crimes, where the impact on the victim may be relatively small, become less viable. Regardless of the jurisdiction in which a crime is committed, evidence is frequently located offshore due to the range of international companies now supplying communications services to Australians – for example, over the top voice and messaging applications, email and cloud storage.

27. Technologies also provide new methods for criminals to mask their activities. People can act anonymously by using software which hides their IP addresses, and use digital currencies to obfuscate transactions. Additionally, widespread encryption of communications and devices, while important for the digital economy and privacy, makes it difficult, and frequently impossible, to decipher legally intercepted communications. Agencies must allocate considerable resources to successfully investigate many cases and use a range of investigative techniques to gather information. IPv6, 5G and mesh networks will heighten these challenges and provide criminals with greater anonymity.

28. In the emerging technological landscape, agencies will need to build and adapt their ICT capabilities and investigative techniques to operate effectively. It will be important for law enforcement agencies to build closer relationships with each other, foreign counterparts and private sector players.

29. New technologies also provide the potential for improved investigative and operational outcomes. The goal is to ensure law enforcement agencies are well-positioned to harness these opportunities, by being nimble and ‘ahead of the curve’, as well as being capable of tackling new challenges as they arise.

30. Legal frameworks must also keep pace with community expectations in this changing environment and balance the legitimate needs of law enforcement with the privacy, rights and freedoms of individuals.

Emerging Technologies

Internet Protocol version 6 (IPv6)

31. IP information is invaluable to law enforcement investigations, as it provides a way for law enforcement to lawfully access a person's network traffic under the authority of the *Telecommunications (Interception and Access) Act 1979* (TIA Act).

32. The implementation of IPv6 will make it significantly more difficult for law enforcement to use interception powers. The framework will include a native IP security system, which encrypts the content of network communications as a matter of course. These encryption technologies are currently available, however users require detailed knowledge of networks and configuring these systems is relatively complex. The implementation of IPv6 will make these encryption services easily accessible and transparent to consumers, and significantly increases the amount of encrypted content over internet services.

33. IPv6 will also significantly increase the number of new IP addresses. These addresses will be available to internet service providers, as well as other foreign and domestic entities, such as social media providers. There are no legal regimes to regulate how these addresses will be assigned to consumers. Consequently, a single user may have numerous IP addresses when operating online. This will degrade law enforcement's ability to attribute information to a particular person. For example, a person communicating on one social media platform may not necessarily use the same IPv6 address when browsing the internet, or when communicating on another social media platform.

34. At present, legislative provisions under Part 5-1A of the TIA Act require domestic service providers to maintain records linking IP addresses and a subscriber for a session. This regime is part of the Australian Government's commitment to ensuring that appropriate information is available to law enforcement and intelligence agencies and allows them to attribute individuals to a particular service and identify criminals. This information will remain critical for law enforcement, but IPv6 will potentially make record keeping more complex particularly in cases involving offshore providers.

35. According to Google Statistics, from the period January 2009 to December 2017, the worldwide use of IPv6 increased from approximately 0.1% to over 20% of Google users.

5G Network Technologies

36. At present, law enforcement agencies rely on the unique identifiers associated with an electronic device to lawfully obtain information about the user of said device, including location-based data. Identifiers allow devices to establish a connection with different network towers. 5G will replace the permanent identifier with one which is temporary, destructing after connection to a tower is made. This will make it more difficult for law enforcement to gain information about a person.

37. Traditionally, a device transfers data through a single medium such as Wi-Fi or a mobile network tower. However, under 5G it will be possible for a device to obtain some data from a network tower and some through another means, such as connecting to a Wi-Fi hotspot, satellite, or internet service provider. Communications using 5G are not guaranteed to follow any particular path making interception challenging. 5G networks may allow a person to restrict data transfers to local networks and bypass telecommunications providers entirely.

38. Existing technologies that switch communications between Wi-Fi and cellular networks already present a problem for agencies – a significant amount of lawfully collected data is already incomplete. 5G will further exacerbate these intelligence gaps and make it harder for law enforcement to identify the appropriate access point to communications data. In order to gain the data from one communication platform, law enforcement may be required to intercept information from a number of sources. This raises issues for the current telecommunications interception framework which was developed in an environment that assumed that:

i. data will eventually travel across a particular point on a provider network (where the entirety of the communication may be lawfully intercepted);

ii. a particular user is only associated with a single telecommunications service or device; and

iii. telecommunications providers will be in a position to facilitate lawful access to communications.

Mesh Networks

39. Mesh networks allow devices in the network to have a strong Wi-Fi signal regardless of their location or direct connection to the internet. For example, a mesh network may involve a person's personal router being 'meshed' with the networks of surrounding neighbours, allowing that person to access the internet through their neighbour's connection in the event of an outage or other adverse circumstance. The primary network technology may be Wi-Fi, while some other devices can be connected with one another via Bluetooth, or a mixture of new wireless technologies. Commercial mesh products are still within their developmental stages, however personal mesh networks between smart phones, watches and other devices are increasingly prevalent.

40. Future adoption of mesh network technologies makes it imperative for legislation to enable law enforcement agencies to investigate offences over more than just carrier networks. These technologies raise questions about traceability and attribution that underpin current interception frameworks. For example, it may appear that the owner of the router directly connected to the internet sent a communication, rather than the actual sender. Additionally, mesh networks will not typically establish one direct path for a communication to travel over. Mesh networks self-configure and will establish the most efficient route for a communication to travel over at a given time.

Modernisation of telecommunications interception laws

41. Law enforcement agencies must be supported by clear and facilitative legal frameworks which appropriately balance the legitimate requirements of law enforcement with the privacy, rights and freedoms of individuals. Legislation provides important powers to law enforcement to access information for investigative purposes. For example, telecommunications interception under the TIA Act and electronic surveillance under the *Surveillance Devices Act 2004* (SD Act) are vital tools for agencies in their investigations of a range of criminal offences, both online and offline. The TIA Act and SD Act recognise that law enforcement and intelligence agencies should have access to the content of communications where certain preconditions are met. However, changes in the technological environment are undermining that access. Although the TIA Act has been subject to a number of legislative changes, it is nevertheless largely anchored to the technological environment that existed in 1979 when it was enacted.

42. To the extent possible, legislative frameworks in which agencies must operate should be capable of applying to unforeseen technologies while still providing agencies appropriate clarity with regard to their powers and obligations. Explicit protections for individuals will assist in ensuring the powers entrusted to law enforcement and intelligence agencies are used appropriately.

43. The Government has committed to progressively revising the TIA Act in response to parliamentary committee inquiries over time, to better enable law enforcement and security agencies to respond to the magnitude of changes which have taken place and those that are anticipated to take place in the near future. This is an opportunity to better reflect the current use of communications networks and the wider range of providers in the communications supply chain.

44. Key issues include streamlining and reducing complexity across the TIA Act, as well as reforming the systems of warrants, oversight and accountability measures and information sharing provisions.

The ICT capabilities of Australian law enforcement agencies

45. The departments note that the AFP, ACIC and AUSTRAC have provided separate submissions to the Committee.

Department of Home Affairs

46. The increasing interdependence of global economies, complex and evolving trade, trends in travel and the more sophisticated border threats are forcing Home Affairs to innovate and adopt new capabilities, particularly in the area of ICT. The border environment is changing rapidly with increasing volumes of travellers, migration, trade and greater geographical dispersion of entry and exit.

47. Home Affairs uses a large number of operational technology capabilities to support its front-line activities, including the delivery and support of x-ray, radios and satellite communications. These technologies are required to operate in our office, at ports, at sea and in the air. Home Affairs' technology will need to adapt to the changing global threat environment to protect Australia's interests from terrorism, illicit materials, illegal migration and organised crime. Home Affairs will adopt leading-edge operational technology to drive innovation in surveillance, examination, inspection and detection. This will improve the ability to maximise the value of information generated by operational technologies.

48. In conjunction with other processes to manage the clearance of goods, in particular the 'near real time' visibility provided by blockchain would, significantly improve the information available for risk analysis. This could eventuate provide safety and security, as well as greater efficiency in border inspection clearance procedures.

49. AI might usefully assist further automation and seamless decision making across the border continuum, particularly in the automated resolution of identity to enable seamless visa assessment and cargo and passenger clearance.

Workforce planning

50. ICT capabilities also include the capacity, materials and expertise an organisation needs to achieve its business objectives.

51. There is also evidence that Year 11 and 12 students in Australia show a lack of interest in STEM (Science, Technology, Engineering and Mathematics) careers and ICT. This may lead to a smaller pool of graduates when recruiting for technologically capable professionals in the medium to long term.

52. Law enforcement also need to develop and maintain an adequately skilled workforce. Many agencies encounter difficulties recruiting and retaining adequately trained staff, particularly in relation to our cyber security workforce. A multi-agency approach to ICT workforce planning could provide opportunities to build a workforce that has the required skills to respond and adapt to emerging technologies.

Australian Border Force

53. The challenges of new and emerging ICT to the ABF are significant and multifaceted. The ABF is reliant on key ICT border management systems to manage cargo and passenger movements. This information enables the identification of goods and passengers, movement information, revenue collection and statistical collection. These systems also provide the information that the ABF and partner agencies use to identify a range of border threats.

54. The dependency on extremely large external facing systems introduces an inherent range of complexities and risk. Maintaining older technologies and aged software platforms, as well as accommodating compatibility with emerging ICT, creates resourcing and security challenges. In turn, this may inhibit the ABF's ability to fully adopt new and emerging technologies. These issues naturally flow on to impact internal corporate ABF systems, potentially limiting ABF's effectiveness.

55. ABF has finite resources and utilises an intelligence-led risk based approach. The exploitation of contemporary ICT can assist with both the processing of passengers and minimising the need for intervention and intrusive searches. This technology assists the ABF to protect passengers, particularly Australian citizens (while transitioning our border continuum as expeditiously as possible).

56. ABF has the unique and difficult job to identify and interdict those at our borders who pose a threat to the Australian community. At the frontline, the detection and response to threats needs to occur in real-time. Those threats include national security risks, those who wish to incite violence, persons involved in child exploitation crimes as well as more traditional criminal threats such as drug importation. The ABF's limitation in accessing and searching electronic devices reduces its opportunity to intervene and collect information and evidence. This may enable a person to enter Australia undetected and without appropriate disruption.

57. At the border, electronic information presents unique challenges. Challenges include encryption, security and the simple refusal for entities and/or people to cooperate and facilitate access to devices, such as withholding passwords when trying to access electronic information. It is now commonplace for information to be stored at a different geographical location to where the device is being used or accessed.

Engagement by Australian law enforcement agencies in our region

58. Ongoing collaboration with both regional and international partners will be important to meet the shared challenges that arise from new ICT. Countries across the world are grappling with the impact of new technologies on crime and the ability for law enforcement to detect and deter criminal activity. Continuing to build strong partnerships and information-sharing arrangements will strengthen our collective ability to respond to the technical environment as it evolves. Cooperation is particularly important given the transnational nature of many crimes threatening Australian public safety and national security. It is in our interest that regional partners have a strong capacity to conduct investigations and prosecutions, as well as assist Australian authorities where required.

59. The 2017 International Cyber Engagement Strategy provides a high level policy framework to guide government, including law enforcement, contributions to a safer and more secure online environment.

60. Commonwealth law enforcement and intelligence agencies have developed and grown international networks and engagement in our region. The departments note these respective agencies have provided separate submissions to the Committee.

Electronic evidence in terrorism cases

61. While electronic evidence is often vital to the successful investigation and prosecution of a range of offences, the process of accessing this evidence can be complex and protracted. Difficulties include identifying where the records are held and taking appropriate steps to have them preserved. Obtaining records from overseas-based ISPs can also cause delay and be affected by jurisdictional challenges.

62. There is substantial regional engagement across government on both a ministerial and agency level. For example, Home Affairs engages with key regional partners to build the capacity of law and justice officials to use electronic evidence in terrorism-related investigations and prosecutions.

63. In April 2017 AGD and AFP partnered with the Indonesian Attorney General's Office and Indonesian National Police to deliver a regional workshop on using electronic evidence in terrorism cases with officials from Indonesia, Australia, Malaysia, Thailand, Singapore and the Philippines attending.

64. Recent terrorism prosecution action has been reliant on the evidence, intelligence and information physically collected by the ABF through the interrogation of electronic devices at the border from devices of inbound and outbound persons. Case information on devices collected both on departure and re-entry from Australia has been pivotal in prosecution action, and providing intelligence for Australian intelligence agencies and their international counterparts.

The role and use of the dark web

65. The dark web facilitates a range of criminal activity, including firearms and drug trafficking, human trafficking, terrorism and online child abuse. Illicit marketplaces located on the dark web allow criminals to anonymously buy and sell drugs, weapons, malware and stolen identities. Illicit forums allow terrorists to communicate and recruit.

Online child abuse

66. Predators have increasingly moved online to forge relationships with children as a first step to luring them for sexual abuse, and onto dark web platforms to discuss, share and promote child sexual abuse and child sexual abuse material. Online forums, websites and other storage and exchange platforms play an increasing role in enabling the global exchange of child abuse material and are often hosted on the dark web.

67. To respond to the increasing use of the dark web for the sharing and promotion of child sexual abuse material, the Government recently introduced the *Crimes Legislation Amendment (Sexual Crimes*

Against Children and Community Protection Measures) Bill 2017. This Bill introduces a new offence into the Criminal Code that targets the provision of electronic services to facilitate dealings in child abuse material. The new offence will address the increasing role played by electronic services in enabling the exchange of child abuse material.

68. The offence will address a gap in Commonwealth law, legislating that individuals can be prosecuted for providing electronic services to facilitate dealings with child abuse material if it can be proven that they are also accessing child abuse material or encouraging others to do so. Where this cannot be proven, there is currently limited criminal recourse against the individual.

69. The maximum penalty for this new offence is 18 years' imprisonment. The offence is also a serious offence for the purposes of the TIA Act, which means that law enforcement will have access to the range of investigatory powers under that Act.

Digital currency

70. The use of digital currencies on the dark web allows buyers and sellers of illicit goods to hide their transactions. This is discussed further in response to '(f) Other relevant matters' of the inquiry's Terms of Reference.

Australian Border Force

71. The dark web poses a range of national security and criminal threats across the ABF's remit. The dark web provides a market place that supports these types of activities. For example, the sale of fake travel documents facilitates attempts to circumvent our border controls, providing a direct threat to the Australian community.

The role and use of encryption, encrypted services and encrypted devices

72. Encryption is a vital part of internet, computer and data security, supporting Australian economic growth and national security. Encryption enables Australians to confidently engage in activities online such as banking, shopping, communications and other services. Encryption also forms part of a suite of measures the Government uses to secure government and citizen information, critical infrastructure and networks.

73. Encryption in devices and applications is also having a serious impact on criminal and national security investigations and prosecutions. Serious criminals are exploiting encryption technologies to communicate, commit offences and operate 'in the dark'. While the use of computers and smartphones is not new, the trend towards ubiquitous encryption being enabled on devices and applications by default means that encryption is no longer the tool of specialists. Like the general public, criminals are taking advantage of this technology.

74. Lawfully intercepted or accessed communications are difficult or impossible to be decrypted and used operationally. Over 65 per cent of data being lawfully intercepted by the AFP now uses some form of encryption. Encryption impacts at least nine out of every 10 of ASIO's priority cases. ABF activities to disrupt and deter organised criminal activities, such as the importation of drugs and pre-cursor chemicals as well as systematic revenue evasion, often encounters sophisticated methodologies using ICT. It is estimated that by 2020 all electronic communications of investigative value will be encrypted.

75. In most instances encryption is incapable of being overcome, limiting the possible avenues for law enforcement to investigate a criminal operation. In some instances, law enforcement agencies may have to employ expensive and time-consuming techniques to access a decrypted device or decipher encrypted communications. Not only does this increase the cost of operations, any delay in agencies' operations substantially raises the risk of harm or loss of life.

76. There are cases where encryption has the potential to be overcome, such as the relatively low levels of protection found on many devices intercepted at the border. However, inconsistent capabilities across different law enforcement agencies inhibit this from taking place. Law enforcement agencies could pool these resources together to capitalise on economies of scale.

Legislative response

77. On 14 July 2017, the Prime Minister and the then Attorney-General announced the Government's intention to address the challenges posed by ubiquitous encryption.

78. It is a well-established principle that, with appropriate authority, law enforcement and intelligence agencies should be able to access people's communications. Under section 313 of the *Telecommunications Act 1997*, domestic carriers are already required to provide 'reasonable assistance' to agencies seeking to implement warrants and enforce the law.

79. The Government has committed that companies will not be required to build so-called 'backdoors'. This will mean that encryption will continue to secure the private and sensitive information of businesses, governments and the general public.

80. While a legislative response can address some of the challenges posed by encryption, it is likely that agencies will continue to face challenges accessing end-to-end encrypted communications. 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.

International experiences and responses

81. On 26 June 2017, at the Five Country Ministerial Meeting between Australia, Canada, New Zealand, the United Kingdom and the United States (‘five country partners’) in Ottawa, Ministers and Attorneys-General discussed the shared challenge of encryption and noted that encryption can severely undermine public safety efforts by impeding lawful access to the content of communications during investigations into serious crimes.

82. To address these issues, the five country partners committed to develop engagement with communications and technology companies to explore shared solutions which proportionately balance the cybersecurity and the rights and freedoms of individuals.

83. In 2016, the UK Parliament passed the Investigatory Powers Act 2016 (UK IPA Act). The UK IPA Act extends a Secretary of State's power to issue 'technical capability notices to require telecommunications operators to maintain the capability to provide data in an intelligible format where it is proportionate, technically feasible and reasonably practicable to do so.

84. New Zealand has powers that are broadly analogous to technical capability notices under the UK IPA Act. The New Zealand Government can compel assistance from service providers to decrypt information (whether or not that provider is located in New Zealand) in response to a warrant provided by a ‘surveillance agency’.

Other relevant matters

Cross-border access to data

85. The global communications supply chain, and the fact that many Australians use communications services provided by overseas providers, has implications for law enforcement officers seeking to access communications information and highlights the importance of working effectively with international partners.

86. The process by which law enforcement agencies may lawfully access stored communications and telecommunications data held by Australian carriers and carriage service providers is relatively straight-forward and efficient under the TIA Act. However, the TIA Act does not provide the same process for information held outside Australia's jurisdiction. Agencies can request telecommunications data directly from some overseas providers, however to obtain communications content, agencies must engage the Mutual Legal Assistance (MLA) process, even if the content is relevant to persons located within Australia. As the MLA process may take considerable time, this may seriously impact agencies' ability to resolve criminal cases or progress cases in a timely manner. Where an investigation continues to move quickly once a MLA request has been made, delays could have serious consequences for public safety and national security.

87. AGD is considering how arrangements for law enforcement agencies to access telecommunications information held by foreign providers may be improved.

88. In June 2017, the Council of Europe Convention on Cybercrime Committee agreed to develop a Second Additional Protocol to the Convention on transborder access to data. The main objective of the Convention on Cybercrime is to pursue a common policy aimed at the protection of society against cybercrime by adopting appropriate legislation and fostering international cooperation. It is expected the Second Additional Protocol will further promote the use and sharing of data and information across jurisdictions to combat cybercrime by establishing more effective formal mutual legal assistance between parties, establishing informal cooperation mechanisms, providing a framework for direct cooperation with service providers, and providing a basis for transborder access to data by law enforcement. Australia is a party to the convention and sits on the drafting group for the Second Additional Protocol which is expected to be open for signature by 2020.

89. At the 2017 Quintet of Attorneys-General, the Five Country partners of Australia, Canada, New Zealand, the United Kingdom and the United States agreed to engage proactively with service providers to facilitate transborder access to non-content data (telecommunications data).

90. In February 2016, the US and UK governments began negotiating a bilateral agreement, under which providers could disclose data directly to the government in the other jurisdiction for serious criminal investigations. For example, the agreement would allow the UK government to serve a UK warrant on a US based telecommunications provider. This would alleviate pressure on the MLA process and hasten law enforcement investigations. US Congress is currently considering the required legislative amendments to enable the bilateral agreement. A similar bilateral agreement between Australia and the US would be beneficial to Australian law enforcement agencies.

Digital currencies

92. Recent reforms to Australia's anti-money laundering and counter-terrorism financing (AML/CTF) regime in relation to digital currencies provide a useful example of how the Government has adapted legislative frameworks to address the regulatory challenges brought by new ICT technologies.

93. The Statutory Review of Australia's AML/CTF regime highlighted that while digital currencies offer the potential for cheaper, more efficient and faster payments, their use gives rise to a number of money laundering and terrorism financing risks including:

    i. greater anonymity (or pseudonymity) compared with traditional payment methods

    ii. transactions are made on a peer-to-peer basis, generally outside the regulated financial systems

    iii. different components of a digital currency system may be located in many countries and subject to varying degrees of regulatory oversight

94. These risks have only been heightened by the use of 'Tor', 'tumblers' and the creation of anonymity-focused digital currencies. For example, the infamous dark web marketplace, the 'Silk Road', was able to flourish due to a combination of Tor and the use of tumblers to allow buyers and sellers of illicit goods to obfuscate their transactions made in bitcoin.

95. Since the closure of the first Silk Road, there has also been the creation of digital currencies specifically designed to enhance anonymity. Europol's Internet Organised Crime Risk Assessment of 2017 found that such privacy-enhancing currencies are increasingly being accepted on the dark web as part of cyber-related extortion attempts such as ransomware, and dark web markets.

Regulation of digital currencies in Australia

96. Recently the Government passed legislation to regulate digital currency exchanges and provide law enforcement with vital financial intelligence to combat the criminal exploitation of digital currencies. The *Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017* (AMLCTFA Act) regulates digital currency exchanges at the point of intersection between the existing regulated financial system and unregulated digital currencies. In doing so, the AMLCTFA Act covers the exchange of fiat currency to digital currencies, such as bitcoin, and vice versa.

97. The measures in the AMLCTFA Act require digital currency exchange businesses in Australia to:

    i. enrol with the AUSTRAC and register on the Digital Currency Exchange Register

    ii. adopt and maintain an AML/CTF program to identify, mitigate and manage the money laundering and terrorism financing risks they may face

    iii. identify and verify the identities of their customers and undertake ongoing customer due diligence

    iv. report suspicious matters, and transactions involving physical currency that exceed $10,000 or more to AUSTRAC

    v. keep certain records for seven years.

98. Digital currency exchanges will have to register on the Digital Currency Exchange Register. This requirement brings with it powers for the AUSTRAC CEO to refuse an application for registration or to tailor a business' registration according to its money laundering, terrorist financing or other serious crime risk. Pursuant to section 76G, the AUSTRAC CEO can impose conditions on its registration.

99. These conditions could allow the AUSTRAC CEO to prevent a digital currency exchange from exchanging a particular digital currency. Furthermore, the AUSTRAC CEO is able to enforce any conditions through the power to suspend or cancel a business' registration on the Digital Currency Exchange Register if a business breaches a condition of registration or the business involves, or may involve, a significant money laundering, terrorist financing or other serious crime risk. The information

registered, reported and kept by digital currency exchanges will be beneficial to AUSTRAC, and partner law enforcement and regulatory agencies across the Commonwealth, states and territories and internationally. The data may assist agencies to conduct analysis and track activity with potential links to dark web, ultimately supporting efforts to prevent the criminal exploitation of digital currencies.

ATTACHMENT A – Terms of Reference

Pursuant to subsection 7(1) of the Parliamentary Joint Committee on Law Enforcement Act 2010, the committee will examine the impact of new and emerging information and communications technology (ICT) with particular reference to:

a) challenges facing Australian law enforcement agencies arising from new and emerging ICT;
b) the ICT capabilities of Australian law enforcement agencies;
c) engagement by Australian law enforcement agencies in our region;
d) the role and use of the dark web;
e) the role and use of encryption, encryption services and encrypted devices; and
f) other relevant matters.