Law Council
OF AUSTRALIA

Inquiry on the impact of new and emerging information and communications technology on Australia law enforcement agencies

Parliamentary Joint Committee on Law Enforcement

6 February 2018

Telephone +61 2 6246 3788 • *Fax* +61 2 6248 0639
Email mail@lawcouncil.asn.au
GPO Box 1989, Canberra ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.asn.au

Table of Contents

About the Law Council of Australia

The Law Council of Australia exists to represent the legal profession at the national level, to speak on behalf of its Constituent Bodies on national issues, and to promote the administration of justice, access to justice and general improvement of the law.

The Law Council advises governments, courts and federal agencies on ways in which the law and the justice system can be improved for the benefit of the community. The Law Council also represents the Australian legal profession overseas, and maintains close relationships with legal professional bodies throughout the world.

The Law Council was established in 1933, and represents 16 Australian State and Territory law societies and bar associations and the Law Firms Australia, which are known collectively as the Council's Constituent Bodies. The Law Council's Constituent Bodies are:

- Australian Capital Territory Bar Association
- Australian Capital Territory Law Society
- Bar Association of Queensland Inc
- Law Institute of Victoria
- Law Society of New South Wales
- Law Society of South Australia
- Law Society of Tasmania
- Law Society Northern Territory
- Law Society of Western Australia
- New South Wales Bar Association
- Northern Territory Bar Association
- Queensland Law Society
- South Australian Bar Association
- Tasmanian Bar
- Law Firms Australia
- The Victorian Bar Inc
- Western Australian Bar Association

Through this representation, the Law Council effectively acts on behalf of more than 60,000 lawyers across Australia.

The Law Council is governed by a board of 23 Directors – one from each of the constituent bodies and six elected Executive members. The Directors meet quarterly to set objectives, policy and priorities for the Law Council. Between the meetings of Directors, policies and governance responsibility for the Law Council is exercised by the elected Executive members, led by the President who normally serves a 12 month term. The Council's six Executive members are nominated and elected by the board of Directors.

Members of the 2018 Executive as at 1 January 2018 are:

- Mr Morry Bailes, President
- Mr Arthur Moses SC, President-Elect
- Mr Konrad de Kerloy, Treasurer
- Mr Tass Liveris, Executive Member
- Ms Pauline Wright, Executive Member
- Mr Geoff Bowyer, Executive Member

The Secretariat serves the Law Council nationally and is based in Canberra.

Acknowledgement

The Law Council acknowledges the assistance of its National Criminal Law Committee and the Law Society of New South Wales in preparation of this submission.

Executive Summary

1. The Law Council welcomes the opportunity to provide this submission to the Parliamentary Joint Committee on Law Enforcement's (**the Committee**) inquiry into the impact of new and emerging information and communications technology (**ICT**) on Australian law enforcement agencies (**the Inquiry**).

2. The Law Council acknowledges that the Inquiry follows the legislative changes in comparable jurisdictions which sought to address ICT challenges of law enforcement agencies. This includes the *Investigatory Powers Act 2016* (UK) and the *Telecommunications (Interception Capability and Security) Act 2013* (NZ).

3. The Law Council notes that the Terms of Reference for this inquiry are very broad, and do not provide any specific policy proposals for consideration and comment. Further, the matters outlined in the Terms of Reference are themselves very broad and do not reflect the nuanced nature of the 'challenges' identified or the potential issues that these forms of technology may pose to law enforcement agencies. As such, the Law Council offers the following general comments.

4. The first part of this submission will outline the guiding principles that the Committee should have regard to when considering the adequacy of existing ICT capabilities of Australian law enforcement agencies. This includes certain rule of law principles and human rights obligations in regard to ensuring that any expansion of law enforcement capabilities are necessary and proportionate to rights of privacy and freedom of opinion and expression, security of personal information and client legal privilege.

5. Identifying these principles at the outset may assist to identify the different interests involved in relation to the impact of new and emerging ICT on Australian law enforcement agencies, and to resolve in a principled manner the tensions which may arise when seeking to determine the most appropriate legislative responses.

6. The second part of this submission will provide further general comments in relation to the use of certain types of technology by Australian law enforcement agencies and a proposal for a principled consideration of privacy and data security issues when developing new policy and legislation in this area.

7. The Law Council recommends that:

    a. any Australian Government response to challenges facing Australian law enforcement agencies arising from new and emerging ICT, such as the use of encrypted communications and devices by persons involved in serious criminal conduct, should ensure that any limitations on individuals' rights are necessary, reasonable and proportionate;

    b. any legislative reform must consider whether, and if so to what extent, restrictions may be placed on the use of technologies that promote and protect the rights to privacy and freedom of opinion and expression;

    c. any expansion of law enforcement capabilities to access personal information should be subject to meaningful oversight by the Parliament, judiciary and the Office of the Australian Information Commissioner (**OAIC**);

    d. any legislative reform should be accompanied by a Privacy Impact Assessment (**PIA**) in accordance with the *Privacy Act 1988* (Cth) (**the Privacy Act**);

e. any proposed legislative amendments to enhance the ICT capabilities of law enforcement agencies which involves the collection of personal information should be accompanied by an Information Security Impact Assessment;

f. any proposed legislation must have regard to the principle of client legal privilege and include safeguards to protect this principle where law enforcement may access client/lawyer communication;

h. the Government release an exposure draft of any proposed legislation on accessing encrypted material, to ensure proposed amendments do not have serious unintended consequences for privacy and cybersecurity of individuals and regulation of the telecommunications sector;

i. consideration should be given to:

- development of an appropriate regime to detect, audit, report on, respond to and guard against events that may breach biometric data security; and
- methods for assessing the implications of any security breach and communicating the breach to both the general public and the technical, privacy and security communities;

j. additional technical information about the nature of the facial matching scheme and the process for ensuring that there are not false matches should be released publicly to inform the public about the operation of the National Facial Biometric Matching Capability (**Capability**) and allow informed debate about its use; and

k. clarification be provided on what other databases will link to the Capability.

Guiding principles

Necessity and proportionality

8. Any Australian Government response to challenges facing Australian law enforcement agencies arising from new and emerging ICT, such as the use of encrypted communications and devices by persons involved in serious criminal conduct,[1] should ensure that any limitations on individuals' rights are necessary, reasonable and proportionate.

9. Law enforcement has expressed concern that new and emerging ICT make it difficult for governments to investigate and prevent illegal activities such as terrorism, the illegal drug trade, organised crime and child pornography, as well as harassment and discrimination against members of vulnerable groups.[2] Before there is an expansion of ICT capabilities of law enforcement powers to gather information, Parliament should

[1] Prime Minister Malcolm Turnbull, 'Press conference with Attorney-General, Senator the Hone. George Brandis QC and the Acting Commissioner of the Australian Federal Police, Mr Michael Phelan APM, (transcript, 14 July 2017, AFP Headquarters, Sydney). Available online at: https://www.pm.gov.au/media/press-conference-attorney-general-and-acting-commissioner-australian-federal-police.

[2] David Kaye, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' Human Rights Council, 29th session (22 May 2015), p. 6; Prime Minister Malcolm Turnbull, 'Press conference with Attorney-General, Senator the Hone. George Brandis QC and the Acting Commissioner of the Australian Federal Police, Mr Michael Phelan APM, (transcript, 14 July 2017, AFP Headquarters, Sydney). Available online at: https://www.pm.gov.au/media/press-conference-attorney-general-and-acting-commissioner-australian-federal-police.

firstly consider the adequacy of current laws that enable law enforcement to access individuals' personal information through ICT. For example, the Law Council notes that the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) allows law enforcement agencies power to gather information concerning an individual's identity through metadata analysis. Further, judicial warrants are available to States to request the disclosure of stored communications information.[3] Other tools currently available to law enforcement to prevent illegal activity include wiretapping, geo-location and tracking, data-mining, and traditional physical surveillance.[4]

10. The Law Council notes that the regulation of encryption by other nations has not been shown to be necessary to meet a legitimate interest, when considering 'the breadth and depth of other tools, such as traditional policing and intelligence and transnational cooperation, that may already provide substantial information for specific law enforcement or other legitimate purposes'.[5]

11. Further, any expansion of the ICT capabilities of law enforcement agencies, such as, legal reform to access encrypted information, must be considered in light of its important role in protecting the security and privacy of information shared through common applications on smartphones, personal computers and network servers. Encryption is also a fundamental tool for providing security across banking, financial, securities, medical, legal and e-commerce sectors as well as general messaging, communications, data protection, intellectual property protection and the secure transfer and storage of sensitive information.

12. Noting the tensions which exist between the competing interests involved, any legislative reform should seek to balance these interests in a manner which ensures that any limitations on individuals' rights are proportionate.

Recommendation

- **Any Australian Government response to challenges facing Australian law enforcement agencies arising from new and emerging ICT, such as the use of encrypted communications and devices by persons involved in serious criminal conduct, should ensure that any limitations on individuals' rights are necessary, reasonable and proportionate.**

Privacy and freedom of opinion and expression

13. In the context of new and emerging ICT, such as encryption and online anonymity, it is necessary to consider the rights to privacy and freedom of opinion and expression. A person's right to be protected from arbitrary or unlawful interference with their privacy, family, home or correspondence is protected under Article 17 of *the International Covenant on Civil and Political Rights* (**the ICCPR**).[6] The right to freedom of opinion and expression is protected by Article 19 of the ICCPR.[7] The right to freedom of opinion is the right to hold opinions without interference, and cannot be limited in any way. The right to freedom of expression can only be subject to certain restrictions as are provided by

[3] *Telecommunications (Interception and Access) Act 1979,* Part 3-3.
[4] David Kaye, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' Human Rights Council, 29th session (22 May 2015), p. 6.
[5] Ibid 13.
[6] *International Covenant on Civil and Political Rights* opened for signature 16 December 1966, 993 UNTS (entered into force 3 January 1976), Art 17(1).
[7] Ibid Art 19.

law and are necessary for the respect of the rights or reputations of others, or for the protection of national security or of public order.[8]

14. Privacy is enabled through encryption and online anonymity, which enables freedom of expression and opinion by allowing individuals to seek, receive and impart information without the risk of repercussions, disclosure, surveillance or other improper use.[9] These individuals include journalists, researchers, lawyers, civil society organisations, members of ethnic or religious groups, or those persecuted because of their sexual orientation or gender identity.[10] Encryption and online anonymity have been identified as crucial to enable individuals their rights to freedom of opinion and expression.[11]

15. Any legislative changes to respond to the challenges must consider whether, and if so to what extent, restrictions may be placed on the use of technologies that promote and protect the rights to privacy and freedom of opinion and expression.[12] Further, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, has observed that restrictions on encryption by other nations 'disproportionately impact the right to freedom of opinion and expression, because they deprive all online users in a particular jurisdiction of the right to carve out private space for opinion and expression, without any particular claim of the use of encryption for unlawful ends'.[13] Such restrictions may include requiring licences for encryption use, setting weak technical standards for encryption, controlling the import and export of encryption tools, and implementing back-door access in commercially available products.[14]

16. The Law Council considers 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.[15]

17. The Law Council further believes that to ensure no one's right to privacy is compromised, the use of powers by law enforcement to copy or seize information, or to intercept or access telecommunications or stored communications, should be subject to mechanisms to safeguard against the misuse or overuse of law enforcement powers.[16] This includes meaningful parliamentary and judicial oversight.[17] As discussed below, any expansion of law enforcement capabilities which involves the collection of personal information would also require, where appropriate, the oversight of the Office of the Australian Information Commissioner (**the OAIC**), to ensure relevant Australian Privacy Principles (**APPs**) under the *Privacy Act 1988* (Cth) (**Privacy Act**) are complied with.

---

[8] Ibid Art 19(3).
[9] David Kaye, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' Human Rights Council, 29th session (22 May 2015), p. 4.
[10] Ibid p. 3.
[11] Ibid.
[12] Ibid p. 6.
[13] Ibid p. 14.
[14] Ibid.
[15] Inter-American Commission on Human Rights, OEA/Serv.L/V/II.149, para. 134 cited in David Kaye, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' Human Rights Council, 29th session (22 May 2015), p. 12.
[16] Law Council of Australia, *Policy Statement: Rule of Law Principles* (March 2011), available online at https://www.lawcouncil.asn.au/resources/policies-and-guidelines, p. 4.
[17] Ibid.

Australian Privacy Principles

18. Any proposed legislative amendments to enhance the ICT capabilities of law enforcement agencies which involves the collection of personal information should be accompanied by a Privacy Impact Assessment (**PIA**) which evaluates the impact of the proposed reform on individual privacy.

19. A PIA would include an assessment of the consistency of proposed amendments with the APPs. This includes ensuring that where an APP entity holds personal information, they must take reasonable steps to protect the information from misuse, interference and loss; and from unauthorised access, modification or disclosure.[18] APP 11.2 also states that where an entity holds personal information, and they no longer need the information for any purpose for which it was used or disclosed by the entity, the entity must take reasonable steps to destroy the information and ensure it is de-identified.[19]

20. Further, the Law Council notes that most Australian Government law enforcement agencies, as agencies with existing personal information security obligations, are covered by the Privacy Act, and therefore will be subject to the Government's Notifiable Data Breaches (**NDB**) scheme, commencing on 22 February 2018. It introduces an obligation to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm.

Recommendations

- **Any legislative reform must consider whether, and if so to what extent, restrictions may be placed on the use of technologies that promote and protect the rights to privacy and freedom of opinion and expression;**
- **any expansion of law enforcement capabilities to access personal information should be subject to meaningful oversight by the Parliament, judiciary and the Office of the Australian Information Commissioner; and**
- **any legislative reform should be accompanied by a Privacy Impact Assessment in accordance with the Privacy Act.**

Security of data

21. Any proposed legislative amendments to enhance the ICT capabilities of law enforcement agencies which involves the collection of personal information should be accompanied an Information Security Impact Assessment (**ISIA**) which evaluates the potential impact on information and cyber security systems.

22. An ISIA involves ensuring that any legislative reform is consistent with the requirements of the *Australian Government Information Security Manual 2016-2017*. This is a key policy document produced by the Australian Signals Directorate as the standard which governs the security of government information and communication technology systems.

[18] *Australian Privacy Act 1988* (Cth) s 11.
[19] *Privacy Amendment (Enhancing Privacy Protection) Act 2012,* schedule 1, part 4, section 11.2 – security of personal information.

Recommendation

- **Any proposed legislative amendments to enhance the ICT capabilities of law enforcement agencies which involves the collection of personal information should be accompanied by an Information Security Impact Assessment.**

Client legal privilege

23. The Law Council regards client legal privilege as a fundamental civil right and a pillar of the Australian legal system. Lawyer-client communications should be regarded as confidential, except where lawyer and client are together engaged in conduct that is calculated to defeat the ends of justice or is otherwise in breach of the law.[20]

24. The Law Council considers that any proposed legislation must have regard to this principle where there is the potential to impact client legal privilege by allowing law enforcement to access telecommunications information, including encrypted data, which contains client/lawyer communications. Proposed legislation should also consider appropriate safeguards, such as notice to lawyers where potential communications will be accessed by law enforcement.

Recommendation

- **Any proposed legislation must have regard to the principle of client legal privilege and include safeguards to protect this principle where law enforcement may access client/lawyer communication.**

Use of certain types of technology

Encryption

25. The Law Council notes that many of the Government's responses to new and emerging technology are intended to strengthen the capacity of law enforcement agencies to meet new challenges. The area of encryption provides a relevant example. The Government has previously announced its intention to introduce new legislation to allow Australian law enforcement agencies to access the content of end-to-end encrypted information by imposing an obligation upon device manufacturers and service providers to assist intelligence and law enforcement agencies with a warrant to access encrypted information.[21]

26. The Law Council notes that encryption is a fundamental tool for protecting the security, authenticity and privacy of information shared through many common applications on smartphones, personal computers, communications systems, network servers and other devices. A wide range of digital services depend on encryption's continued proven effectiveness against attacks, including digital services used by many professional sectors and general messaging and communications applications used by many

[20] Law Council of Australia, *Policy Statement: Rule of Law Principles* (March 2011), available online at https://www.lawcouncil.asn.au/resources/policies-and-guidelines, p. 3.
[21] Prime Minister of Australia, 'Press Conference with the Attorney-General, Senator the Hon. George Brandis QC and the Acting Commissioner of the Australian Federal Police, Mr Michael Phelan APM', 14 July 2017, available at <https://www.pm.gov.au/media/press-conference-attorney-general-and-acting-commissioner-australian-federal-police>.

individuals. A number of risks have been identified with different approaches to accessing encrypted information. For example, there is a risk that the proposals may increase the possibility of unauthorised access to applications or devices by third parties. This would be an unwelcome consequence.

27. The Law Council is of the view that a thorough and considered review of the technical details of any such proposal is necessary to ensure that the proposed amendments do not have serious unintended consequences for the privacy and cyber security of individuals and regulation of the telecommunications sector. The Law Council has previously called upon the Government to release an exposure draft of this proposed legislation to enable such review, in line with the principles set out in the Department of Prime Minister and Cabinet's *Guidance Note on Best Practice Consultation*.[22]

28. There is also a need to consider how any proposed provisions will be enforced, particularly in cases where the service providers are located outside Australia.

Recommendation

- **The Government release an exposure draft of any proposed legislation on accessing encrypted material, to ensure proposed amendments do not have serious unintended consequences for privacy and cybersecurity of individuals and regulation of the telecommunications sector.**

Biometric data and facial recognition systems

29. For several years, the Government has planned to augment the existing Document Verification Service with the Capability to enable government agencies to use facial images to detect and prevent identity fraud.[23] The Capability is comprised of a central interoperability hub that acts as an exchange to facilitate information sharing on a query and response basis. The central hub will facilitate data sharing between agencies on a query and response basis, without storing any personal information; there will be no single database that holds all the images.[24] The Capability will also draw upon a National Driver Licence Facial Recognition Solution, with information shared by states and territories under the Intergovernmental Agreement on Identity Matching Services (**Intergovernmental Agreement**),[25] as well as providing a technical ability to use still images from other sources such as CCTV, surveillance photography, the internet or social media.[26]

[22] Department of Prime Minister and Cabinet, 'Best Practice Consultation Guidance Note' (February 2016) <https://www.pmc.gov.au/sites/default/files/publications/best-practice-consultation.pdf> 5, 9.
[23] Attorney-General's Department, "Preliminary Privacy Impact Assessment of the National Facial Biometric Matching Capability – Interoperability Hub: Attorney-General's Department Response" December 2015, available at <https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/AGD-response-privacy-impact-assessment.pdf.
[24] Attorney-General's Department, 'Fact Sheet: Face Matching Services', available at <https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Face-matching-services-fact-sheet.pdf>.
[25] Intergovernmental Agreement on Identity Matching Services, 5 October 2017, available at: <https://www.coag.gov.au/sites/default/files/agreements/iga-identity-matching-services.pdf>.
[26] Website of the Attorney-General's Department, "Face Matching Services" available at <https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/Face-verification-service.aspx.

30. Much of the public discussion around the development of the Capability has focused on the benefits to law enforcement agencies. However, the Capability will use information taken for a particular purpose for other purposes which individuals have not consented to – for example, individuals have consented to providing a photograph to obtain a passport or driver licence but have not consented to their biometric information being extracted from that image and being used for other purposes. The Law Council also notes that a previous PIA concluded that the Capability could collect more information than necessary and retain that data longer than necessary.[27] While the Attorney-General's Department indicated in response that only the minimum amount of transaction data required for audit and control purposes would be retained, it is unclear how this will work in practice.[28]

31. Within this context, we note that a number of privacy and data security issues arise in relation to the development of the Capability. Many similar issues would also arise in the development of other large government databases containing personal information. In brief, we note the following issues:

    a) The consequences of any potential security breach or unauthorised disclosures are significant. Given that any inadvertent release or breach in the security of biometric information is irrevocable, careful consideration should be given to matters such as:
        - development of an appropriate regime to detect, audit, report on, respond to and guard against events that may breach biometric data security both in the short and longer term, noting that in the long term many of the security measures currently in place may no longer be effective; and
        - methods for assessing the implications of any security breach and communicating the breach to both the general public (data subjects) and the technical, privacy and security communities.
    b) There remain flaws with existing facial recognition technologies, which create a risk that there may be false positive matches. The Law Council is of the view that additional technical information about the nature of the facial matching scheme and the process for ensuring that there are not false matches should be released publicly to inform the public about the operation of the Capability and allow informed debate about its use.
    c) At this stage it is unclear what other databases will link to the Capability. The Digital Transformation Agency is developing plans for the integration of biometrics to form the foundation of the new Trusted Digital Identity Framework, to be used for 'Govpass'. It is unknown how, and to what extent, the Capability and the National Driver Licence Facial Recognition Solution will interact with facial matching for Govpass.
    d) The Intergovernmental Agreement left open the possibility that in the future access to the Facial Verification Service may be made available to private organisations. There is currently very limited information on this proposed use of the Capability but careful consideration will need to be given to:

[27] Information Integrity Solutions 'National Facial Biometric Matching Capability: Privacy Impact Assessment – Interoperability Hub' dated August 2015, available at <https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Privacy-Impact-Assessment-National-Facial-Biometric-Matching-Capability.PDF>, Appendix 2.

[28] Attorney-General's Department, 'Preliminary Privacy Impact Assessment of the National Facial Biometric Matching Capability Interoperability Hub: Attorney-General's Department Response', December 2015, 3-4, available at <https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/AGD-response-privacy-impact-assessment.pdf>.

- how the private sector use of biometric data through the Capability will be regulated;
- the systems that will be put in place to control use of sensitive biometric data in the private sector;
- how consumers will be informed about use of their biometric data and provide consent for their biometric information to be used by private organisations, especially where the data was originally collected from the individual for another purpose;
- the penalties that will be put in place for unauthorised use;
- the safeguards that will be in place to protect individuals from identity fraud and/or theft; and
- whether private entities using the facial verification service will also be expected to contribute facial recognition/biometric data to government databases.

Recommendations

- **Consideration should be given to:**
  - **development of an appropriate regime to detect, audit, report on, respond to and guard against events that may breach biometric data security; and**
  - **methods for assessing the implications of any security breach and communicating the breach to both the general public and the technical, privacy and security communities.**
- **Additional technical information about the nature of the facial matching scheme and the process for ensuring that there are not false matches should be released publicly to inform the public about the operation of the Capability and allow informed debate about its use;**
- **Clarification be provided on what other databases will link to the Capability.**