Opening Statement

Law Council
OF AUSTRALIA

11 May 2018

Opening Statement to the Parliamentary Joint Committee on Law Enforcement:

Inquiry on the impact of new and emerging information and communications technology

Morry Bailes, President, Law Council of Australia, 11 May 2018

Opening Statement

1. My name is Morry Bailes and I am the President of the Law Council of Australia. As the Committee would be aware, the Law Council is the peak national body representing the legal profession in Australia.

2. I would like to thank the Committee for the opportunity to provide evidence to its inquiry on the impact of new and emerging information and communications technology.

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. As is customary, the Law Council does not comment as to whether possible policy is good or bad. We see the Law Council's role as assisting the legislature to ensure that laws and regulatory instruments:

    a. are clear, consistent, sustainable over a period of time and otherwise practical;

    b. reflect good practice in public administration; and

    c. take due account of human rights and other fundamental rights and legitimate expectations of citizens, and thereby do not erode citizen trust in government and its agencies. This is particularly important in the case of security and law enforcement legislation, where safe civil society can only be achieved over the longer term if citizens trust what government is doing necessarily under a cloak of confidentiality. Safe civil society should not be achieved at the expense of citizens being fully engaged in the digital economy and sharing the benefits of the digital economy. Getting this balance right is particularly difficult, as the legislature must speculate as to likely future developments in technology and its uses and the extent to which new statutory interventions may prompt users to work around these interventions or opt-out of targeted digital applications.

4. The Law Council would therefore like to highlight two areas for the Committee to have regard to when considering the adequacy of existing information and communications technology or ICT capabilities of Australian law enforcement agencies. Firstly, rule of law principles and human rights obligations, and secondly, recommendations in relation to certain types of technology, in particular encrypted communications and biometric data.

5. With regard to certain rule of law principles and human rights obligations, 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, and considers the extent to which restrictions may be placed on these

technologies that promote and protect the rights to privacy and freedom of opinion and expression. Such restrictions if required should be the subject of Parliamentary oversight.

b. 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 to assess the impact on individual privacy, a Regulation Impact Statement which evaluates the impact on business, and an Information Security Impact Assessment to evaluate the impact on information and cyber security systems. These should be conducted by appropriately experienced and independent privacy counsel and made available for independent review.

c. Any proposed legislative amendments to enhance the ICT capabilities of law enforcement agencies which involves the collection of data and of personal information should articulate:

- which agencies may have access to the information;
- when access (if any) is permitted to other entities (including private sector organisations); and
- when access is to be permitted, under what specified circumstances, with what transparency measures, and subject to what safeguards and oversight as to the form of access request, persons that may make a request, restrictions as to types of information to be provided and as to subsequent use of that information by the recipient after its provision.

d. Any proposed legislation must have regard to the principle of client legal privilege and whistle-blower protection and include safeguards to protect these principles where law enforcement may access client/lawyer communication.

6. In relation to the use of encrypted communications by Australian law enforcement agencies the Law Council recommends that 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. Indeed, we would ask that the Committee consider making that a recommendation, let us help the Parliament by examining an exposure draft and providing advice to the Parliament.

7. In relation to the use of biometric data by Australian law enforcement agencies the Law Council recommends that the Committee consider:

- 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.

8. The Law Council recommends that additional technical information about the nature of facial matching schemes 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 and allow informed debate about its use. May I add, the Law Council appeared before the Joint Committee on Security and Intelligence only last week, following a submission in respect of the *Identity-matching Services Bill 2018,* regarding facial recognition. I draw the Committee's attention to our evidence regarding that Bill.

9. Further recommendations are in our written submission.

10. My colleagues and I are happy to answer any questions the Committee may have. Thank you.

Contact:

Patrick Pantano: Public Affairs
P 02 6246 3715 (includes mobile)
E Patrick.Pantano@lawcouncil.asn.au

Sonia Byrnes: Communications
P 0437 078 850
E Sonia.Byrnes@lawcouncil.asn.au