Opening Statement

Law Council
OF AUSTRALIA

3 May 2018

Opening Statement to the Parliamentary Joint Committee on Intelligence and Security Hearing:

Review of the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018.

Morry Bailes, President, Law Council of Australia, 3 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 into the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018.

3. The focus of the Law Council's submission is on the Identity-matching Services Bill. If enacted, this Bill would enable the sharing of identification information of a majority of individuals living in Australia.

4. The Law Council supports reasonable and proportionate measures aimed at combatting identity crime and effective information-sharing for the purposes of facilitating law enforcement and protecting Australia's national security, protective security, community safety, road safety and identity verification. There are many elements within this Bill that are aimed at this legitimate objective and supported by measures that are intended to ensure that this legitimate objective is not achieved at unacceptable cost. Unacceptable cost should be measured by considering the impact of widespread use of identity-matching services to the vast majority of Australian citizens that do not engage in criminal behaviour and that expect Australian governments to assure a safe and secure lifestyle without excessive interference or oversight of their individual private lives, as conducted on the streets, anonymously in crowds, in public places and the apparent seclusion of parks, beaches, picnic areas and other shared areas.

5. The Intergovernmental Agreement envisaged 'robust privacy safeguards'. The Law Council submits that this reflects recognition by governments that Australian citizens expect that derogations from their right of privacy should be justified by governments as aimed at a legitimate objective, to be reasonable and proportionate. Reasonableness and proportionality is partly related to what the law says, but largely about how the law operates and in particular the level of transparency and accountability that is reliably assured and independently verifiable.

6. This is particularly important in the case of provision of a hub for an open system: in particular, provision of a capability for a diverse range of federal, state and territory government agencies to identify 'a face in a crowd'. Clearly, provision of such capability has been determined by government to be desirable to facilitate detection of would-be terrorists scoping a site for a potential terrorist attack. But that very same identity matching capacity might also be used for a range of activities that Australian citizens regard as unacceptable. Examples include access and use of CCTV footage to detect, investigate or prosecute particular young people who may (no 'reasonably believed to be' test applies in this case) engage in certain low-level unlawful conduct.

7. The line between (1) legitimate and proportionate uses of a hub, and (2) illegitimate and disproportionate uses should be clearly defined and assured by law. That line should also be assured by law to be fully transparent, understood and consistently applied by all relevant governments and their agencies, with clarity and stability of that line supported by appropriate accountability measures that are independently verifiable. If that line can creep towards broad social surveillance such as (to take but one of a myriad of possibilities) use of the system to detect and fine jaywalkers or litterers, that line can also creep further to a full social credit style system of government surveillance of Australian citizens. We respectfully submit that this legislation should entrench the principles that (1) this line will not creep without careful foresight of consequences of that creep and an engaged public debate about why that creep is justified, in essence to help close what is currently an open system and (2) that the stability of the line will assuredly be maintained through operation of the provisions of the Act itself.

8. Of course, any stable line must not only be clear and stable: it must also be seen to be clear and stable. Identity-matching services are legitimised through citizen trust of what governments are doing, and that trust is hard gained and in today's world, easily eroded and then hard to regain. What can go wrong often will go wrong, and the worst behaviour of one actor in a networked system can readily erode trust of citizens as to good behaviour by all other actors, and in the networked system itself. The Commonwealth will be seen to own the hub and what is done through it, even if the Commonwealth is not responsible for errors and misdeeds of others. The Explanatory Memorandum states the issue well (at page 55): "Accountability and transparency are also essential in data-sharing between government agencies. Members of the community have a right to understand how governments are using their identification information, and to have access to publicly available information about those uses. This is an essential aspect of a free and democratic society that supports trust in government processes and services". Of course, the Explanatory Memorandum then goes on to state that 'the limitation on the right to privacy as a result of provision of the IDSS is necessary and reasonable to achieve the legitimate objective of improving the efficiency, accountability and transparency of government data-sharing practices". We respectfully submit to this Committee that this assertion is an overstatement. Our submissions make targeted suggestions for amendments that would enable this assertion to be properly grounded.

9. The other important factor for consideration by this Committee is the reality or otherwise of consent by affected citizens. The Bill refers to the need for consent of citizens as a relevant safeguard, in particular in relation to use of the identity-matching service by individuals dealing with local government authorities. Consent can be a problematic concept in relation to provision of government services to citizens. Many government services are required to participate fully in communities and therefore essential in practice, whether or not legally required to be taken by relevant individuals. Where consenting to identity matching is 'bundled' with other matters and the impact of giving consent is not fully understood by the citizen, is the alleged consent valid? Current regulatory guidance by the Australian Information Commissioner (OAIC) and a number of other legal developments would say 'no'.

10. Subsequent to providing our written submissions to the Committee, the Law Council has had the benefit of reading the written submission of the Acting Australian Information Commissioner and Acting Privacy Commissioner. The Law Council generally agrees with the Commissioner's submission and the recommendations aimed at improving accountability and transparency as to use of identity-matching services and the operation of the hub.

11. 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