T 03 9607 9311
F 03 9602 5270
president@liv.asn.au

5 September 2018

Dr Natasha Molt
Acting Director of Policy
Policy Division
Law Council of Australia
19 Torrens Street
Braddon ACT 2612

By email: natasha.molt@lawcouncil.asn.au

Dear Dr Molt

Exposure Draft Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

Executive summary

The Law Institute of Victoria (**LIV**) welcomes the opportunity to provide input to the Law Council of Australia's (**LCA**) submission to the Department of Home Affairs' (the **Department**) Consultation on the Exposure Draft Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the **Exposure Draft Bill**).

The LIV is Victoria's peak body for lawyers and those who work with them in the legal sector, representing around 19,000 members. The LIV advocates on behalf of our profession and the wider community, leads the debate on law reform and policy, lobbies and engages with government and provides informed and expert commentary.

While the LIV recognises the Exposure Draft Bill's aim to increase public safety by providing faster access to encrypted data and supports many of the proposed safeguards, including requiring agencies to seek a warrant or authorisation, and for that warrant or authorisation to meet the same threshold as a surveillance device warrant, the LIV has identified some concerns with the operation of the proposed enhanced powers of law enforcement agencies.

Summary of recommendations

The summary of the LIV's recommendations are set out in the table below. Most relate to the scope of the proposed law going far beyond its stated rationale in the commentary provided by the Department.

TOPIC	RECOMMENDATION
Purpose of the Exposure Draft Bill	• Limit the enforcement of criminal law within Australia only, with the potential addition of investigating and prosecuting acts or omissions occurring overseas.
The scope of the Exposure Draft Bill as it relates to entities	• Limit the types of entities which have control over encrypted information and are able to access and decrypt it.

Law Institute of Victoria ABN 32 075 475 731
T: 03 9607 9311 F: 03 9602 5270
E: lawinst@liv.asn.au
470 Bourke Street, Melbourne 3000 Australia
DX 350 Melbourne, GPO Box 263 Melbourne 3001
W: www.liv.asn.au

The scope of the Exposure Draft Bill as it relates to activities	• Limit the scope of cooperation to decrypting the content of encrypting communications and providing them to one of the three designated agencies.
Managing compliance costs	• Provide an upper limit for non-compliance fines for small businesses and clearly define what a 'per case' basis means in relation to the attraction of non-compliance fines; • Clearly explain how Technical Capability Notices will apply to entities outside Australia when the warrant giving the authority to issue the Technical Capability Notice does not apply outside of Australia; and • Require granting authority to take into account the size and economic impact on the recipient of the warrant or authorisation.
Protection of individual privacy	• Expressly include individual privacy as a consideration in the public interest test.[1]
Accountability/ oversight	• Expressly include a percentage breakdown of the types of notices issued and for what purpose they were issued in each annual report; and • Grant the OAIC direct oversight to ensure adherence to the Australian Privacy Principles.
Comparison with other jurisdictions	• Consider the lack of a privacy cause of action in Australia.

Context of issues

According to the Department, the Exposure Draft Bill has been developed to address threats by terrorists, child sex offenders and criminal organisations who use encryption and other forms of electronic protection to mask illegal conduct. The Exposure Draft Bill intends to address these threats by introducing a suite of measures that will improve the ability of agencies to access intelligible communications content and data. According to the Exposure Draft Bill's Explanatory Memorandum, three distinct reforms will help achieve improved access:

1. Enhancing the obligations of domestic providers to give reasonable assistance to Australia's key law enforcement and security agencies and, for the first time, extending assistance obligations to offshore providers supplying communications services and devices in Australia;

2. Introducing new computer access warrants for law enforcement that will enable agencies/authorities to covertly obtain evidence directly from a device; and

3. Strengthening the ability of law enforcement and security authorities to overtly access data through the existing search and seizure warrants.

LIV responses to issues

The LIV considers that the primary issues that arise from the Exposure Draft Bill relate to:

- The purpose of the Exposure Draft Bill;

- The scope of the Exposure Draft Bill as it relates to entities;

[1] For example, s 317ZK(2) of the Exposure Draft Bill.

- The scope of the Exposure Draft Bill as it relates to activities;
- Managing compliance costs;
- Protection of individual privacy;
- Accountability/oversight; and
- Comparison with other jurisdictions.

The LIV has considered the positive and negative aspects of the Exposure Draft Bill in relation to each of the primary issues that it suggests arise from the Exposure Draft Bill, and provides the following comments:

The purpose of the Exposure Draft Bill

In relation to the purpose of the Exposure Draft Bill, the LIV acknowledges that there is significant value to public safety in allowing law enforcement authorities faster access to encrypted information where there are threats to national security or in order to prevent the commission of serious criminal offences. The LIV also acknowledges that there is merit in international cooperation to deal with cybercrimes which occur across multiple jurisdictions, and that Australia has ratified the European Convention on Cybercrime.

The LIV echoes the guiding principle that the "protection of privacy should continue to be a fundamental consideration in and the starting point for any legislation providing access to telecommunications for security and law enforcement purposes".[2]

The protection of individual privacy should be weighed against the expansion of purposes (or "relevant objectives" as variously defined in the Exposure Draft Bill) which are used to carve out exclusions to the prohibition on access to communications. The traditional main exceptions to the prohibition on interception broadly are:

- Enforcing the criminal law and laws imposing pecuniary penalties;
- Protecting the public revenue; and
- Safeguarding national security.

In the Exposure Draft Bill:

- In addition to the traditional main exceptions, the purpose of "assisting the enforcement of the criminal laws in force in a foreign country"[3] is included, which was relatively recently introduced into the *Telecommunications Act 1997* (Cth) pursuant to the *Cybercrime Legislation Amendment Act 2012* (Cth);
- In the context of technical assistance requests (**TARs**) only, the purpose relating to "safeguarding national security" is broadened to include "the interests of Australia's foreign relations or the interests of Australia's national economic well-being"; and[4]

[2] A S Blunn, 'Report of the Review of the Regulation of Access to Communications, Attorney-General's Department', 2005, page 5. Similar guiding principles are reiterated by the Law Council of Australia's submissions on the 'Inquiry on the Impact of New and Emerging ICT on Australian law enforcement agencies', 6 February 2018, page 7.

[3] See relevant objectives defined in s 317G(5)(b) of the Exposure Draft Bill with respect to requirements under TARs (per s 317G(2)); specified purposes for TANs under s 317L(2)(c)(ii); and relevant objectives defined in s 317T(3)(b) with respect to requirements for TCNs under s 317T(2).

[4] Compare s 317L(2)(c) of the Exposure Draft Bill for TANs: "safeguarding national security"; s 317T(3)(d) for TCNs: "safeguarding national security"; and 317G(5)(d) for TARs: "the interest of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being".

- In the context of technical assistance notices (**TANs**) and technical capability notices (**TCNs**), the four primary purposes (or relevant objectives as defined in the *Telecommunications Act Act 1977* (Cth)) is further expanded to include any matter that facilitates, or is ancillary or incidental to, primary purposes or relevant objectives, whichever is applicable (the **Ancillary Purposes**).[5]

The LIV submits that given the extensive powers already available to law enforcement authorities to access stored communications, metadata, and computer networks, it would be more reasonable and proportionate that the purposes for which the TAR, TCN, and TANs can be given should be utilised only for matters of law enforcement involving serious offences.[6]

If "assistance to foreign law enforcement" is to remain as a basis for giving a TAR/TAN/TCN, the LIV submits that prior to a TAR/TAN/TCN being given, and where the relevant purpose relates to "assisting the enforcement of the criminal laws in force in a foreign country", the relevant decision-maker ought be required to give consideration to the mandatory and discretionary grounds for refusing a mutual assistance request under s 8 of the *Mutual Assistance in Criminal Matters Act 1987* (Cth). The LIV also suggests that it may be appropriate for costs of compliance to be an additional matter for consideration by the decision-maker, particularly with respect to TAN/TCNs, where the mandatory aspects mean that Australian intelligence services may compel Australian service providers to undertake extensive and potentially resource-draining activities in response to assistance requests from foreign law enforcement agencies.

The rationale behind the third purpose, "protecting the public revenue", has not been discussed in the commentary around the Exposure Draft Bill, and could potentially give the Australian Taxation Office (ATO), through cooperation with an interception agency, near-unlimited access to all encrypted communication on the basis that it might be evidence of a transaction giving rise to a tax liability. Although the purpose of "protecting the public revenue" has been a part of the *Telecommunications Act 1997* (Cth) since its inception, it is unclear why such purpose should also be included in the Exposure Draft Bill given the significant enlargement of interception agency powers being proposed.

The LIV suggests further that the purpose of "safeguarding national security" has an extremely broad scope given that no actual laws need to be identified for it to apply. In the circumstances, where this appears to be a supplementary "top up" power for law enforcement, and will have a significant effect on individuals' privacy, the LIV submits that this should be aligned with the current definition of serious offences in the *Telecommunications (Interception and Access) Act 1979* (Cth) which would cover most critical matters of national security.

The LIV submits that the Exposure Draft Bill may not take into account the realities of technology, in particular, the speed with which targeted criminals will shift platforms or adopt new technology.

<u>The scope of the Exposure Draft Bill as it relates to entities</u>

The LIV understands that the Exposure Draft Bill is intended to capture all types of entities which may have control over encrypted information of value to law enforcement.

LIV notes that the Exposure Draft Bill applies to "eligible activities" of a "designated communications provider", pursuant to s 317C. These include the provision of a service "ancillary or incidental to, the supply of a listed carriage service", the provision of "an electronic service that has one or more end-users in Australia", the manufacturing and operation of a facility, and the manufacture of components used in a facility. The LIV considers that many of these providers will have little or no control over encrypted information which will be of value to law enforcement, and it is unclear why they have been captured in the Exposure Draft Bill. This would make the Exposure Draft Bill a compliance concern for

[5] See s 317(L)(2)(d) of the Exposure Draft Bill for TANs and s 317T(2)(a)(ii) and s 317T(2)(b)(ii) for TCNs.
[6] The definition of serious offences in s 5D of the *Telecommunications (Interception and Access) Act 1979* (Cth) is useful here, as it includes acts of terrorism, sabotage, espionage, foreign interference, and other serious criminal offences as well as offences which would prejudice national security.

overseas companies operating in Australia, even if they have no control over encrypted communications.

The scope of the Exposure Draft Bill as it relates to activities

The LIV notes with agreement that:

- Agencies must obtain a warrant or authorisation, and that warrant or authorisation must meet the same threshold as a surveillance device warrant;
- There are requirements for practicability and technical feasibility;
- No systemic weaknesses can be built into products;[7] and
- Some of the recommendations from the LIV submission relating to the 'Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014' have been adopted.[8]

However, the LIV is concerned:

- The Exposure Draft Bill can potentially require designated communications providers (**DCP**) to undertake a wide range of activities unrelated to decrypting information, including installing, maintaining, testing or using software or equipment (s 317E(c)), assisting with the testing, modification, development or maintenance of a technology or capability (s 317E(f)), and modifying, or facilitating the modification of, any of the characteristics of a service provided by the designated communications provider (s 317E(h));
- The terms "practicability" and "technical feasibility" are not defined. The LIV understands that any provider who believed a notice required them to undertake something unfeasible would need to seek judicial review; a time-consuming and expensive process, particularly for a small business; and
- While the scope of notices is limited to core agency functions, these are very wide.[9]

Managing compliance costs

The LIV considers that the advantages of the Exposure Draft Bill in relation to managing compliance costs include:

- Enforcement on a no profit/no loss principle; and
- Immunity from civil liability for cooperating providers.[10]

However, the LIV is concerned:

- There may be potentially unnecessary regulatory costs on providers. The LIV notes that it can be burdensome for small businesses, in particular, with non-compliance fines of up to $10 million for companies and fines of up to $50,000 for individuals *per case,* where "case" is not clearly defined*;*

[7] s 317ZG of the Exposure Draft Bill.
[8] Namely, that "The agencies which can access telecommunications data must be exhaustively set out in the legislation". In the Exposure Draft Bill, there is an exhaustive list of applicable agencies.
[9] s 317G(3) and s 317T(3) of the Exposure Draft Bill.
[10] s 317ZJ and s 317G of the Exposure Draft Bill.

- Agencies can issue TCNs to companies outside of Australia but within its "nexus". Agencies also require a warrant to undertake surveillance activities under the Exposure Draft Bill. These warrants have no application outside of Australia. The LIV considers that it is unclear how this will operate; and

- More broadly than "protecting the public revenue" should perhaps be considerations of the economic impact of the regime. Where warrants or authorisations are issued to innocent holders of encrypted data, there is a risk that part of the investigative cost will be transferred to those holders. Where the holders are small businesses, the LIV is concerned about the risk of government bodies requiring the holders of the data to utilise their own resources to make the data "intelligible" to the relevant government body beyond merely de-encrypting the data.

Protection of individual privacy

The LIV considers that one of the Exposure Draft Bill's primary advantages regarding protection of individual privacy is that it provides for unauthorised disclosure of information being punishable by up to five years' imprisonment.[11]

However, the LIV understands that the "public interest" test does not require decision makers to have regard to individual privacy[12] when making a TAN or TCN.

A related issue is the exposure of recipients of warrants and authorisations to claims by parties the subject of the data sought by the warrant. Where data holders have contracted to protect such information, such as via the use of encryption, the LIV is concerned that in complying with the warrant or authorisation, they may be exposing themselves to contractual claims. Most contracts allow carve outs for the provision of confidential information "where required by law". However, where there is an obligation to encrypt data and a warrant requires the recipient to de-encrypt such data, it is less clear that such steps would fall within such a contractual carve out.

Accountability/oversight

Regarding accountability and oversight under the Exposure Draft Bill, the LIV notes:

- The proposed safeguards that require warrants and strict threshold tests; and

- Only the Attorney General or the head of an interception agency can issue a TCN.

However, the LIV is concerned that:

- The Exposure Draft Bill does not impose the same requirements for warrant or authorisation on a TAR, so there is less oversight compared to TAN and TCNs;

- Annual reporting requirements and company transparency reports are arguably insufficient given the proposed scope of the Exposure Draft Bill; and

- Heads of interception agencies can delegate powers to SES employees.[13]

[11] s 317ZF of the Exposure Draft Bill.
[12] s 317ZK(2) of the Exposure Draft Bill.
[13] s 317ZP to s 317ZR of the Exposure Draft Bill.

Comparison with other jurisdictions

The LIV is concerned that restrictions on encryption by other nations disproportionately affect the right to freedom of expression.

The LIV notes that the United Kingdom's *Investigatory Powers Act 2016* (**the UK Act**) is broader in scope than the Exposure Draft Bill. The UK Act introduces a new system for the lawful interception and examination of information, authorisations for obtaining and retaining data, and new powers to issue notices to compel communications providers to do certain things, such as remove electronic protection by or on behalf of that operator from any communications or data, or disclose certain information.

In relation to the "Assistance" aspect of the Exposure Draft Bill, the LIV notes the following differences between the UK Act and the Exposure Draft Bill:

- **Oversight**

  The Exposure Draft Bill has "limited oversight and accountability structures and processes in place. The Director-General of Security, the chief officer of an interception agency and the Attorney-General can issue [technical capability] notices without judicial oversight. This differs from how it works in the UK, where a specific judicial oversight regime was established, in addition to the introduction of an Investigatory Powers Commission".[14] Under the Exposure Draft Bill, a TAN or TCN will have no effect to the extent (if any) to which it would require a designated communications provider to do an act or thing for which a warrant or authorisation under a range of laws is required.[15]

- **Limitations**

  In the Exposure Draft Bill, the requirements imposed by a technical capability notice must be reasonable and proportionate, and compliance must be practicable and technically feasible.[16] The UK Act specifically considers the cost to providers of complying with a notice: "The UK's *Investigatory Powers Act* authorises the UK Government to compel communications providers to remove 'electronic protection' applied to communications or data in its control. In requiring a person to remove such electronic protection, which would include encryption, the Government must in particular take into account the technical feasibility, and likely cost, of complying with those obligations''.[17]

- **Preventing creation of 'back-doors'**

  The Exposure Draft Bill includes a provision that designated communications providers must not be required to implement or build a systemic weakness or systemic vulnerability into their systems.[18] The LIV notes that it does not appear that such a provision exists in the UK Act.

- **Types of notices**

  The UK Act sets out two types of notices that compel assistance: national security notices and technical capability notices. National security notices require a telecommunications operator to take "such specified steps as the Secretary of State considers necessary in the interests of

[14] Monique Mann, 'The Devil is in the Detail of Government Bill to enable Access to Communications Data', The Conversation, 15 August 2018 (https://theconversation.com/the-devil-is-in-the-detail-of-government-bill-to-enable-access-to-communications-data-96909); see also s 253(1) and s 254 of the UK Act.
[15] s 317ZH of the Exposure Draft Bill.
[16] s 317V of the Exposure Draft Bill.
[17] Allens, 'Code Breakers – Australian Government Flags Forced Decryption Reforms', (https://www.allens.com.au/pubs/priv/pulse-1805/article-01.htm); see also s 255(3) of the UK Act.
[18] s 317ZG of the Exposure Draft Bill.

national security"[19] and technical capability notices impose on a relevant operator any obligations specified in the notice. This differs from the Exposure Draft Bill, which allows for technical capability notices to be issued to enforce domestic laws, assist the enforcement of the criminal laws of foreign countries, and in the broader interests of national security, or to protect the public revenue. These have been described as "vague and unclear limits on these exceptional powers".[20]

- **Broad application**

  The LIV understands that, in the UK Act, technical capability notices may be given to a "relevant operator", meaning "a postal operator, a telecommunications operator, or a person who is proposing to become a postal operator or telecommunications operator".[21] In the Exposure Draft Bill, the term "provider" is very broad and might include telecommunication companies, internet service providers, email providers, social media platforms and a range of other "over-the-top" services. It also covers those who develop, supply or update software, and manufacture, supply, install or maintain data processing devices.[22]

The LIV notes the following similarities between the UK Act and the Exposure Draft Bill in relation to the "Assistance" aspect of the Exposure Draft Bill:

- Both the UK Act and the Exposure Draft Bill put the onus on telecommunication providers to give security agencies access to communications;[23] and

- In both the UK Act and the Exposure Draft Bill, there are unclear outcomes for end-to-end encryption security. In Australia, "providers will be required to develop new ways for law enforcement to collect information. As in the UK, it is not clear whether a provider will be able to offer true end-to-end encryption and still be able to comply with the notices".[24]

Regarding the differences between the UK Act and the Exposure Draft Bill in relation to the "Access" aspect of the Exposure Draft Bill, in the UK Act, there are safeguards in place for members of parliament, items subject to legal privilege, confidential journalism material and sources of journalistic information in relation to the issuing of warrants to intercept and examine information.[25] It does not appear that similar safeguards are contained in the Exposure Draft Bill.

While the Exposure Draft Bill does not concern data retention, the LIV notes that recent legal challenge may lead to the UK having to amend the UK Act to the extent that "it was inconsistent with EU law because access to retained data was not limited to the purpose of combating 'serious crime' and was not subject to prior review by a court or other independent body".[26]

In considering the similarities and the differences between the Exposure Draft Bill and similar legislation found within the rest of the "Five Eyes" intelligence community, the LIV notes the following:

---

[19] s 252 of the UK Act.
[20] Monique Mann, 'The Devil is in the Detail of Government Bill to enable Access to Communications Data', The Conversation, 15 August 2018 (https://theconversation.com/the-devil-is-in-the-detail-of-government-bill-to-enable-access-to-communications-data-96909).
[21] s 253(3) of the UK Act.
[22] Monique Mann, 'The Devil is in the Detail of Government Bill to enable Access to Communications Data', The Conversation, 15 August 2018 (https://theconversation.com/the-devil-is-in-the-detail-of-government-bill-to-enable-access-to-communications-data-96909).
[23] Monique Mann, 'The Devil is in the Detail of Government Bill to enable Access to Communications Data', The Conversation, 15 August 2018 (https://theconversation.com/the-devil-is-in-the-detail-of-government-bill-to-enable-access-to-communications-data-96909).
[24] Ibid.
[25] Part 2 of the UK Act.
[26] Ian Cobain, 'UK has six months to rewrite snooper's charter, high court rules', (https://www.theguardian.com/technology/2018/apr/27/snoopers-charter-investigatory-powers-act-rewrite-high-court-rules), 28 April 2018.

- "The enforcement of criminal laws in other countries may mean international requests for data will be funnelled through Australia as the 'weakest-link' of our Five eyes allies. This is because Australia has no enforceable human rights protections at the federal level";[27]

- In New Zealand, "the *Telecommunications (Interception Capability and Security) Act* was introduced in 2013. It provides for the issuing to NZ surveillance agencies of warrants, under which they may require a telecommunications service to decrypt a telecommunication on its service if it has provided the encryption";[28] and

- In the United States, "the Trump administration and FBI officials have publicly canvassed the possibility of cracking down on the use of encryption technology. This follows the 2016 legal battle between the Obama administration and tech giant Apple over whether Apple should be compelled to develop software allowing it to break into its own iPhone devices, in response to a terrorist attack in California. The FBI withdrew its request the day before the hearing of this dispute, claiming it had found a third party who was able to assist in unlocking the iPhone. Similarly to the situation in Australia, concerns in the US revolve around the inability to guarantee the security of decryption keys stored in a central location. This is why providers of encrypted communication services generally do not hold keys themselves. It is also unclear how the UK and NZ laws will work in circumstances where service providers are unable to decrypt, or have great difficulty in decrypting, communication".[29]

Recommendations

The LIV makes the following recommendations in relation to the Exposure Draft Bill:

The purpose of the Exposure Draft Bill

Primary recommendation

In relation to the purpose of the Exposure Draft Bill, the LIV suggests that the Exposure Draft Bill be limited to the enforcement of the criminal laws of Australia, with the potential addition of the investigation or prosecution of acts or omissions committed overseas which would also be a crime under Australian law. This would allow, if necessary, Australian law enforcement agencies/authorities to access encrypted information to assist overseas agencies in dealing with terrorism, child sex offences, and the other types of conduct which the Exposure Draft Bill is designed to address.

Secondary recommendations

If "assistance to foreign law enforcement" is to remain as a basis for giving a TAR/TAN/TCN, the LIV submits that prior to any one being given, and where the relevant purpose relates to "assisting the enforcement of the criminal laws in force in a foreign country", the relevant decision-maker must give consideration to the mandatory and discretionary grounds for refusing a mutual assistance request under s 8 of the *Mutual Assistance in Criminal Matters Act 1987* (Cth).

The LIV also suggests that costs of compliance should be an additional matter for consideration by the decision-makers, particularly with respect to TAN/TCNs.

The LIV suggests further that s 317(L)(2)(d) of the Exposure Draft for TANs and s 317T(2)(a)(ii) and s 317T(2)(b)(ii) for TCNs be removed to balance the protection of privacy with the proportionate purposes by which the powers under the Exposure Draft Bill are exercised.

---

[27] Monique Mann, 'The Devil is in the Detail of Government Bill to enable Access to Communications Data', The Conversation, 15 August 2018 (https://theconversation.com/the-devil-is-in-the-detail-of-government-bill-to-enable-access-to-communications-data-96909).
[28] Allens, 'Code Breakers – Australian Government Flags Forced Decryption Reforms', (https://www.allens.com.au/pubs/priv/pulse-1805/article-01.htm).
[29] Ibid.

The scope of the Exposure Draft Bill as it relates to entities

In relation to the scope of the Exposure Draft Bill as it applies to entities, the LIV suggests that the entities to which the Exposure Draft Bill could apply should be limited to entities which have control over encrypted information and are able to access and decrypt it.

The scope of the Exposure Draft Bill as it relates to activities

In relation to the scope of the Exposure Draft Bill as it applies to activities, the LIV suggests:

- Limiting the scope of cooperation required to decrypting the content of encrypted communications and providing them to one of the three agencies; and

- Limiting the scope of application to companies with direct control and access to encrypted information.[30]

Managing compliance costs

In relation to managing compliance costs, the LIV suggests:

- Establishing an upper limit for non-compliance fines, particularly for small businesses, in addition to the maximum established per case;

- Clearly explaining how TCNs will apply to entities outside of Australia when the warrant giving the authority to issue the TCN does not apply;

- Including, in the requirements for practicability and technical feasibility, a requirement that the granting authority weigh the significance of the issue to which the warrant or authorisation relates with the economic impact on the party to whom the warrant or authorisation is being issued. A minor issue with significant compliance cost to the recipient that is a small business might not justify the granting of the warrant, whereas a more important issue might; and

- Providing limits on the extent to which the bodies seeking the warrant or authorisation can transfer data filtering or data organisation tasks onto the recipient.

Protection of individual privacy

In relation to protection of individual privacy, the LIV considers that the reasonable/proportionate test[31] should explicitly include a required to consider the right to individual privacy.

The scope of the immunity should be considered in light of potential contractual and other consequences to the recipients of warrants and authorisations regarding the parties to which any data the subject of the warrant relates.

[30] The Exposure Draft Bill allows ASIO, ASIS and the ASD to issue TANs and TCNs. These notices can require a designated communications provider to undertake an extremely broad range of activities going beyond simply accessing encrypted data, including: Installing, maintaining, testing or using software or equipment (s 317E(c)); Assisting with the testing, modification, development or maintenance of a technology or capability (s 317E(f)); and Modifying, or facilitating the modification of, any of the characteristics of a service provided by the designated communications provider (s 317E(h)).

[31] Namely, that "the decision-maker must be satisfied that requirements in a technical assistance notice and technical capability notice must be reasonable and proportionate and compliance with the notice is practicable and technically feasible".

Accountability/oversight

In relation to accountability/oversight, the LIV suggests that:

- Annual reports should include a percentage breakdown of types of notices issued and whether they were for terrorism, child sex offences, organised criminal activity or otherwise;

- When assistance has been provided under a TAR/TAN/TCN, subjects of an interception warrant or a TAR be notified of the fact once there is no prejudice to an investigation;[32] and

- The LCA's previous recommendation that the OAIC has direct oversight to ensure the Australian Privacy Principles under the *Privacy Act 1988* (Cth) are complied with be adopted.[33]

Comparison with other jurisdictions

The LIV notes that many jurisdictions have enacted, or are considering similar legislation. The LIV suggests it is important to consider the lack of an invasion of a privacy cause of action in Australia, in contrast to jurisdictions such as the United States. The lack of a privacy cause of action increases the Exposure Draft Bill's potential negative impact to personal privacy for which individuals will have little recourse.

Conclusion

There is significant value to public safety in allowing law enforcement agencies/authorities faster access to encrypted information where there are threats to national security, or in order to prevent the commission of serious criminal offences. However, the LIV supports the guiding principle that the "protection of privacy should continue to be a fundamental consideration in and the starting point for any legislation providing access to telecommunications for security and law enforcement purposes".[34]

The recommendations above seek to balance the need for the protection of individual privacy with the overarching aims of the Exposure Draft Bill. They primarily revolve around limiting the scope and purpose of the Exposure Draft Bill so that individual freedoms are not unnecessarily and unintentionally encroached. Amending the Exposure Draft Bill in accordance with the LIV's recommendations will assist in achieving such balance.

Please do not hesitate to contact me or Patrick Fong via PFong@liv.asn.au if you wish to discuss any aspect of this letter further.

Yours sincerely

Belinda Wilson
President
Law Institute of Victoria

[32] See similar recommendation in the 'Report on the Review of the Cybercrime Legislation Amendment Bill 2011', Joint Select Committee on Cyber-Safety, (http___www.aphref.aph.gov.au_house_committee_jscc_cybercrime_bill_report_chapter5.pdf), pages 45-57.
[33] Law Council of Australia, 'Policy Statement: Rule of Law Principles (March 2011)', (https://www.lawcouncil.asn.au/resources/policies-and-guidelines), page 4.
[34] A S Blunn, 'Report of the Review of the Regulation of Access to Communications, Attorney-General's Department', 2005, page 5. Similar guiding principles are reiterated by the Law Council of Australia's Submissions on the 'Inquiry on the Impact of New and Emerging ICT on Australian law enforcement agencies', 6 February 2018, page 7.