Thursday 30 April 2020

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

BY EMAIL: pjcis@aph.gov.au

Google welcomes the opportunity to provide comments to the Parliamentary Joint Committee on Intelligence and Security on the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 ("the Bill").

The US Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") creates a concrete path for the U.S. government to enter into modern agreements with other nations that meet baseline privacy, human rights and rule of law standards. . The legislation enables law enforcement to investigate cross-border crime and terrorism in a way that avoids international legal conflicts.

Google has long advocated for international agreements and global solutions to protect our customers and Internet users around the world. We have always stressed that dialogue and diplomacy between and among countries, not conflict, is the best approach. Google encourages and supports efforts by the Australian government to negotiate an executive agreement authorised by the CLOUD Act. However there are certain elements of the Bill that give us cause for concern, especially when considering how the interception powers under this Bill could be used in tandem with technical capability notices under the controversial Telecommunications and Other Legislation (Assistance and Access) Act 2019, which is currently undergoing a statutory review by the Committee. Google has separately raised concerns about that legislation.

Definition of "designated communications provider"

The Bill broadly defines "designated communications provider" as;

i. a carrier; or
ii. a carriage service provider; or
iii. a message / call application service provider; or
iv. a storage / back-up service provider; or
v. a general electronic content service provider.

We suggest that the Bill should not apply to service providers in their capacity as infrastructure providers to corporations or government entities (arguably covered in the categories of a storage / back-up service provider and / or a general electronic content service provider). Corporations or government entities are best placed to produce the requested records themselves, save for a rare circumstance where the corporation is itself the subject of the criminal investigation. Any ambiguity on the issue, raising from unclear exceptions, should therefore be avoided in the text.

Centralising requests

Designated communications providers are instructed under Schedule 1 Part 6 of the Bill to provide any requested communications and data to the requesting agency or the Australian Designated Authority, depending on the directions of the IPO. Respectfully, our experience is that a better approach would be that all communications to and from an Australian law enforcement agency be channelled through the Designated Authority and that this Authority acts as a coordinator across multiple agencies. Putting in place a coordinating body will guard against the risk of duplication and will act as a single point of contact for training, education and access to designated communications providers.

Civil penalties for non-compliance with an International Production Order ("IPO")

Part 8 of the Bill establishes a framework for compliance with IPOs. If a designated communications provider receives a valid IPO and the designated communications provider meets the 'enforcement threshold' (a two step test that is, in practice, a relatively low bar to meet) when the IPO is issued, the designated communications provider must comply with the IPO. Failure to comply with an IPO may lead to a civil penalty of up to $10 million for body corporates. The imposition of a mandatory obligation to comply with an IPO is contrary to the purpose of the CLOUD Act which is to lift blocking statutes, but explicitly does <u>not</u> create a compulsory obligation on service providers. The authors of the Bill appear to be aware of this dichotomy as the Bill explicitly asserts that Australian service providers do not have to comply with reciprocal requests from international agencies. We are concerned by the attempt to impose a mandatory obligation on overseas based designated communications providers that exists only in the construct of an otherwise non-compulsory international agreement, and respectfully request that this be amended to reflect the intent of the CLOUD Act, which is that enforcement procedures be found in existing law, and that references to civil penalties be removed.

Approval of interception orders

We seek further information about the role that eligible judges will play in approving IPOs that involve the interception of communications. The Bill states that an interception agency "may" apply to an eligible judge or AAT member for approval, which suggests that this is a suggestion rather than a requirement. Given the invasive nature of these powers, we consider the role of an independent third party who can impartially assess and balance the criteria set out in sub-clause 30(5) to be critical to the approval process. Therefore, we

recommend amending the suggestion that an agency "may" apply to an eligible judge to read as strict obligation.

We note that the Bill identifies an additional approval step in the States of Queensland and Victoria whereby a Public Interest Monitor must approve any interception orders requested by one of their State based agencies. We see great merit in this secondary review and approval step and suggest that the Committee recommend to the Government that either a national Public Interest Monitor role be established to oversee the approval of International Production Orders, or that the remaining Australian States and Territories establish a similar role with equivalent functions (perhaps through the Council of Australian Governments).

Appealing IPOs

We respectfully suggest that the appeal options contained within the Bill could be strengthened. Deferring to existing appeal mechanisms is not satisfactory given the lack of appropriate merit based appeal processes in other relevant legislation such as the Telecommunications and Other Legislation (Assistance and Access) Act 2019. The reliance on existing law as the primary source for appeal procedures is especially problematic in light of the enforcement provision discussed above. In particular, overseas providers may be subject to other third-country laws, conflicts with which are not and cannot be lifted through the international agreement, yet no option would exist to raise such an impediment to compliance. This would create exactly the type of conflict of laws scenario that the CLOUD Act is designed to prevent.

Thank you once again for the opportunity to contribute towards this review.