Submission by Professor Dan Jerker B. Svantesson to the Department of Home Affairs' consultation regarding:

The Assistance and Access Bill 2018

September 2018

Professor Dan Jerker B. Svantesson
Co-director, Centre for Commercial Law
Faculty of Law, Bond University
Gold Coast, Queensland, 4229
Australia
[redacted]

Summary of major points

- The Bill adopts a complex, yet unsophisticated and blunt, approach to the delineation of its geographical scope of operation relating to the new framework for industry assistance.
- This approach lacks support in traditional international law notions of jurisdiction.
- The Bill's approach to the delineation of its geographical scope of operation also lacks support in contemporary and developing international law notions of jurisdiction.
- The Bill's approach to the delineation of its geographical scope of operation sets a dangerous precedent.
- Consequently, the Bill's approach to the delineation of its geographical scope of operation relating to the new framework for industry assistance must be substantially reworked.

1. General remarks

1. I welcome the initiative taken by the Department of Home Affairs to seek input on the impact of the Assistance and Access Bill 2018.

2. These submissions are intended to be made public.

3. These submissions deal only with one particular issue; namely that of the Bill's geographical scope of operation relating to the new framework for industry assistance.

2. The relevant fundamental considerations

4. The difficulties associated with ensuring effective law enforcement access to electronic evidence, while maintaining appropriate safeguards, e.g. for fundamental rights such as privacy, are well documented. Today, relevant data (evidence) – both in relation to specific "cybercrimes" and in relation to traditional crimes – is often stored in cloud structures outside the State of the law enforcement agency that needs access to the data in question. Thus, the need for law enforcement access to evidence is beyond debate. Such access is essential both for the conviction of criminals and for the protection of those wrongly accused.

5. However, despite its undeniable importance, the need for law enforcement access to evidence is best seen as one of four relevant fundamental considerations. The other three are (1) the need for protecting and promoting human rights, (2) the need to ensure a functioning international system, and (3) the need to support the digital economy.

3. The Bill's approach to the delineation of its geographical scope

6. The thinking behind the Bill's geographical scope of operation relating to the new framework for industry assistance is perhaps best explained in the assertion that: "Operating in the Australian market comes with obligations to assist in protecting Australian citizens from those using its marketed services and devices for serious crimes, including terrorism."[1]

[1] A new industry assistance framework (https://www.homeaffairs.gov.au/consultations/Documents/industry-assistance-factsheet.pdf).

7. This type of 'market-focused' ground for jurisdiction is not new,[2] and has a certain appeal.[3] However, as applied in the Bill's geographical scope of operation relating to the new framework for industry assistance it only establishes a weak nexus with Australia.

8. In fact, reading the definition of a "designated communications provider" (s. 317C) together with the definition of an "electronic service" (s. 317C), it is clear that, for example, anyone, anywhere in the world, who operates a website "that has one or more end-users in Australia" is subject to Australia's claim of jurisdiction.

4. The Bill's approach to the delineation of its geographical scope of operation lacks support in traditional international law notions of jurisdiction

9. Traditional thinking on jurisdiction is largely focused on the territoriality principle; a state has jurisdiction over its territory, but not beyond. Obviously, the territoriality principle does not provide support for a claim of jurisdiction over a foreign website operator merely based on the website having one or more end-users in Australia.

10. However, as far as legislative jurisdiction is concerned, international law is typically said to also recognise jurisdiction based on four other grounds. They are:

the nationality principle;

the protective principle;

the universality principle; and

the passive personality principle.[4]

11. Jurisdiction based on the mere fact that a foreign website is accessed by an end-user in Australia does not fit within any of these grounds of jurisdiction.

[2] Consider e.g. the focus on "doing business" found in various laws including the *Privacy Act 1988* (Cth), s. 5B(3).

[3] Svantesson, D.J.B. (2013). The extraterritoriality of EU data privacy law - its theoretical justification and its practical effect on U.S. businesses. *Stanford Journal of International Law*, 50(1), 53-117.

[4] 'Introductory Comment to the Harvard Draft Convention on Jurisdiction with Respect to Crime 1935' (1935) 29 Supp AJIL 443, 445.

5. The Bill's approach to the delineation of its geographical scope of operation lacks support in contemporary and developing international law notions of jurisdiction

12. It has long been recognised that the traditional focus on territoriality is a poor fit with the online environment.

13. Not least in the context of law enforcement cross-border access to digital evidence, there is emerging acceptance of an alternative jurisprudential framework for jurisdiction not anchored in territoriality.[5] Adopted to the present context that framework would dictate that, where an investigator seeks cross-border access to electronic evidence, (s)he needs to show that:

> 1) there is a substantial connection between the matter in relation to which the investigative measure is taken and the State seeking to exercise investigative jurisdiction;
>
> 2) the State seeking to exercise investigative jurisdiction has a legitimate interest in the investigative measures in question; and
>
> 3) the exercise of investigative jurisdiction is reasonable given the balance between the State's legitimate interests in the investigative measures in question and other interests.[6]

14. Much work lies ahead in defining, as precisely as we can, what we mean by "legitimate interest" and "substantial connection"; and the challenge of reaching consensus on the interests to be balanced as part of the third principle should not be underestimated. Nevertheless, there can be no doubt that, without more, jurisdiction based on the fact that a foreign website is accessed by one end-user in Australia does neither meet requirement of a substantial connection, nor does it prove a legitimate interest. Furthermore, such a weak nexus does not come close to meeting the requirement of interest balancing.

6. The Bill's approach to the delineation of its geographical scope of operation sets a dangerous precedent

[5] See, e.g., the approach to jurisdiction adopted in the US CLOUD Act, and the EU's Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings and the Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters.

[6] Svantesson, D.J.B., Solving the Internet Jurisdiction Puzzle (Oxford University Press, 2017), pp. 57-90; Polcak, R. and Svantesson, D.J.B., Information Sovereignty – Data Privacy, Sovereign Powers and the Rule of Law (Edward Elgar Publishing, 2017), pp. 188-206.

15. The Bill's approach to the delineation of its geographical scope of operation sets a dangerous precedent.

16. To see that this is so, we need only consider whether we would find it acceptable if all other states – including oppressive dictatorships – were free to seek the types of measures, catered for under the Bill, from all Australian designated communications providers.

17. This is not merely a theoretical risk.

7. Concluding remarks

18. To move forward on designing a functioning international system ensuring effective law enforcement access to digital evidence held by private parties, while maintaining appropriate safeguards, we must move away from the outdated territorial thinking on this matter.

19. However, that does not mean that we lower the thresholds.

20. The Bill's approach to the delineation of its geographical scope of operation lacks support in traditional international law notions of jurisdiction, as well as in more contemporary and developing international law notions of jurisdiction. Furthermore, it sets a dangerous precedent.

21. In the light of this, the Bill's approach to the delineation of its geographical scope of operation relating to the new framework for industry assistance must be substantially reworked.

Professor Dan Jerker B. Svantesson

Professor Svantesson is based at the Faculty of Law, and is a Co-director of the Centre for Commercial Law, at Bond University. He is also a Researcher at the Swedish Law & Informatics Research Institute, Stockholm University (Sweden), a Visiting Professor, Faculty of Law, Masaryk University (Czech Republic) and serves on the editorial board on a range of journals relating to information technology law, data privacy law and law generally.

Professor Svantesson held an ARC Future Fellowship 2012-2016, has written extensively on Internet jurisdiction matters and has won several research prizes and awards including the 2016 Vice-Chancellor's Research Excellence Award.

The views expressed herein are those of the author and are not necessarily those of any organisation Professor Svantesson is associated with.