Submission by Professor Dan Jerker B. Svantesson to the Parliamentary Joint Committee on Law Enforcement's inquiry into:

The impact of new and emerging information and communications technology

January 2018

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

Summary of major points

- 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.
- Any examination of the challenges facing Australian law enforcement agencies arising from new and emerging ICT must consider the difficulties associated with ensuring effective law enforcement access to cloud-stored data held by private parties, while maintaining appropriate safeguards, e.g. for fundamental rights such as privacy.
- Australia must seek to address these challenges – both through domestic initiatives and through international cooperation.
- One obvious arena for moving this matter forward is the important work of the Council of Europe on providing further guidance on how its *Cybercrime Convention* can address these concerns.
- Australia could also consider engaging more actively with the work carried out on this topic by the Internet and Jurisdiction Policy Network.
- A key challenge in designing a functioning international system ensuring effective law enforcement access to cloud-stored data held by private parties, while maintaining appropriate safeguards, is to determine when law enforcement has jurisdiction to request data held by a foreign company, or indeed, held by a domestic company but stored on servers in another country. In this context, we need to move away from territoriality as a core principle of jurisdiction, in favour of a framework that fits better with the world we live in today.

1. General remarks

1. I welcome the initiative taken by the Parliamentary Joint Committee on Law Enforcement to seek input on the impact of new and emerging information and communications technology.

2. These submissions are intended to be made public.

3. These submissions deal only with a small selection of the relevant issues.

2. Well-known problems

4. Any examination of the challenges facing Australian law enforcement agencies arising from new and emerging ICT must consider the difficulties associated with ensuring effective law enforcement access to cloud-stored data held by private parties, while maintaining appropriate safeguards, e.g. for fundamental rights such as privacy.

5. The difficulties involved are well-known and have been documented in detail elsewhere:[1]

- Effective law enforcement carried out in accordance with fundamental rights is a State obligation.
- To be effective, law enforcement needs adequate access to evidence. Such access is essential both for the conviction of criminals and for the protection of those wrongly accused.
- 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.
- Ascertaining the location of the data may be difficult. To give just two examples, the problems that arise include situations where:
    - the location of the data cannot be ascertained within a reasonable timeframe and with reasonable measures; and
    - the data required is split over servers in more than one location.

[1] Dan Svantesson, Preliminary Report: Law Enforcement Cross-Border Access to Data (November 22, 2016). Available at SSRN: https://ssrn.com/abstract=2874238.

- Even where the location of data may be ascertained, the mobility of data makes it possible to manipulate the location so as to complicate or hinder law enforcement measures.
- The private parties that hold the data – often the major Internet companies – are, due to their presence in multiple markets, often exposed to the requirements of multiple legal systems.
- Relevant law, and how the law is applied, differs between various legal systems.
- The requirements a State sets for when its law enforcement agencies may access cross-border data are often different to the requirements States impose on foreign law enforcement agencies seeking access to data stored by private parties in that same State's jurisdiction.
- Being exposed to multiple legal systems with varying rules means that the private parties that hold the data may be put in a position where compliance with one State's laws unavoidably results in a direct violation of another State's law. Such situations are clearly harmful and should be minimised or, if possible, eliminated.
- The Mutual Legal Assistance (MLA) system – while the principal mechanism for law enforcement cross-border access to evidence – cannot cope with the number of requests, and even if improved, it does not alone represent the solution to the challenges we are facing.
- While commonplace, alternative means for law enforcement cross-border access to data – such as direct request to private parties – are currently controversial and associated with a sense of uncertainty both for law enforcement and for the private parties that hold the data.
- While they form an important part of the discussions to be had, the relevant (public) international law rules and concepts are not well understood and are often phrased in unjustifiably absolutist terms.
- This is a pivotal time as several important projects are underway to address the noted complications.

3. The current climate

6. It is widely recognised that, because of the noted difficulties, law enforcement agencies have felt forced to resort to unilateral actions to access cross-border

evidence where necessary in order to investigate criminal offences. Such actions are often characterised as "rogue" actions and are typically condemned.

7. However, we must recognise such actions as symptoms of a systems failure, and while unilateral actions do not work as a good path forward, we are unlikely to see such actions cease until we have fixed what is broken in the system.

8. The slowness of the MLAT system is one part of the problem,[2] and while the MLAT system alone does not represent the solution, practical steps can be taken to speed it up.

9. Another important problem stems from how we view the implications of territorial sovereignty. Put simply, it is commonly assumed that where a law enforcement agency in State A gains access to evidence held on a server in State B, this somehow violates State B's sovereignty, regardless of whether State B: (a) is aware of the data, (b) can access the data, or (c) has any discernible interest in the data. This overzealous interpretation of territorial sovereignty is surprising and is out of line with how similar situations are dealt with in other areas of law.

10. In the light of this, Australia must – both through domestic initiatives and through international cooperation – work towards a functioning international system ensuring effective law enforcement access to cloud-stored data held by private parties, while maintaining appropriate safeguards, e.g. for fundamental rights such as privacy.

11. One obvious arena for moving this matter forward is the important work of the Council of Europe on providing further guidance on how its *Cybercrime Convention* can address these concerns.

12. In parallel to the work undertaken by the Council of Europe, the Internet and Jurisdiction Policy Network[3] – a Paris-based global multi-stakeholder policy network addressing the tension between the cross-border internet and national jurisdictions – has brought together a Contact Group[4] consisting of experts from academia, industry, government, policy groups and law enforcement. That Group – of which I had the privilege of being a member – has recently produced a Report[5] canvassing a

---

[2] See further: Council of Europe, T-CY Cloud Evidence Group, *Criminal justice access to data in the cloud: Recommendations for consideration by the T-CY* [TCY(2016)5] (16 September 2016) http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e, at 9.

[3] https://www.internetjurisdiction.net/.

[4] https://www.internetjurisdiction.net/news/data-jurisdiction-contact-group-members.

[5] https://www.internetjurisdiction.net/uploads/pdfs/Papers/Data-Jurisdiction-Policy-Options-Document.pdf.

range of policy options. Australia could consider engaging more actively with the work of the Internet and Jurisdiction Policy Network.

4. A complex matrix of overlapping and competing considerations

13. Any work towards a functioning international system ensuring effective law enforcement access to cloud-stored data held by private parties, while maintaining appropriate safeguards, must be carried out with a clear understanding of the complex matrix of overlapping and competing considerations that are relevant. Together with Lodewijk van Zwieten (Public prosecutor specialised in cybercrime, The Netherlands), I have identified the following 25 considerations that must be taken into account in this context:[6]

1) Cloud providers have a duty to comply with appropriate legal process, resulting in an obligation to comply with or endure legitimate law enforcement measures.

2) Cloud providers have a duty to be respectful of the human rights (such as privacy) of their customers.

3) Cloud providers have a duty to be respectful of the human rights (such as privacy, protection of personal data and reputation, protection against crime etc.) of non-customers.

4) Cloud providers cannot comply with conflicting obligations.

5) The idea of territorial sovereignty as the primary nexus for establishing and enforcing jurisdiction is increasingly at odds with the realities of our interconnected world, which is characterised by constant and fluid cross-border interaction.

6) In approaching the question of jurisdiction, investigative measures cannot be handled under the strict rules governing enforcement jurisdiction.

7) Where a Cloud provider enjoys rights in a State where it has a corporate presence and where that State has a legitimate interest in the Cloud provider, those rights and interests must be considered when an assessment is made as to whether the Cloud provider should comply with duties, conflicting with those rights and interests, stemming from another country.

[6] Dan Svantesson & Lodewijk van Zwieten, Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution, *Computer Law & Security Review* 32 (2016) pp. 671-682

8) Different rules are needed for different types of data as the degree of data privacy sensitivity varies.

9) A distinction between access to stored (historical) data and live data is necessary.

10) Digital evidence stored on foreign servers is frequently relevant in relation to completely domestic crimes.

11) Where fully respected, anonymity – an articulated component of some data protection frameworks – undermines the identification of factors such as the relevant person's location, nationality and residence.

12) Cloud providers must be transparent as to how many requests for access they get, from where those requests originate, what those requests relate to, how many requests result in access being granted etc.

13) Cloud providers need to be transparent in their terms of use as to how they interact with law enforcement agencies, including how they treat the information they receive as part of data requests.

14) Cloud providers need to be transparent in informing the affected user where data is in fact communicated to law enforcement agencies, unless there are strong reasons not to inform the user.

15) The urgency of data access will vary from case to case.

16) Individuals have an interest in their data protection rights.

17) Individuals have a general interest in crimes being detected, investigated and prevented and in criminal justice being served.

18) Victims of crime have a particular interest in crimes being detected, investigated and prevented and in criminal justice being served.

19) States have a duty to be good world citizens so as to help legitimate law enforcement actions in other countries.

20) States have a duty to act against criminal activities within their jurisdiction so as to prevent those criminal activities affecting other States or their citizens.

21) States have a duty to be respectful of and to protect human rights (such as the right to privacy, data protection, etc.).

22) It is not always possible to ascertain the geographical location of the server on which data resides.

23) In the context of Cloud computing, data is frequently distributed over more than one server, either as duplicates or simply by the fact that it is broken into small parts.

24) Appropriate procedural safeguards ensuring legitimacy of data request must be established.

25) The proper substantive rules, scope, structure and nature of any framework for facilitating lawful law enforcement access to evidence via direct contact with Cloud providers will need to reflect the differences in the legal traditions of the countries covered by the framework, but with a minimum standard to be met.

5. The jurisdiction problem

14. A key challenge in designing a functioning international system ensuring effective law enforcement access to cloud-stored data held by private parties, while maintaining appropriate safeguards, is to determine when law enforcement has jurisdiction to request data held by a foreign company, or indeed, held by a domestic company but stored on servers in another country (consider the ongoing *Microsoft warrant case* coming before the Supreme Court of the United State).

15. The approach to date has been to focus on territoriality.

16. In the context of jurisdiction, territoriality essentially is meant to fulfil two functions, and it fails at both. The first is that territoriality is meant to be a criterion for when a state can claim jurisdiction. But especially online it is too easy to find territorial anchor-points for jurisdictional claims. The second function of territoriality is that it is meant to act as a stop sign providing a warning when you are entering the exclusive domain of another State. But again, territoriality fails since it is simply unrealistic to think that a State will be connected to the global community and still enjoy traditional exclusiveness in the Westphalian sense.

17. To move forward on designing a functioning international system ensuring effective law enforcement access to cloud-stored data held by private parties, while maintaining appropriate safeguards, we must move away from the outdated territorial thinking on this matter.[7]

[7] For a detailed discussion of this, see further: Dan Svantesson, *Solving the Internet Jurisdiction Puzzle* (Oxford University Press, 2017).

6. Time for solutions

18. An alternative to territoriality can be found in the three principles that I elsewhere have suggested as the core principles for jurisdiction more broadly.[8] Adopted to the present context they 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.*

19. It should be noted that none of these three principles lend themselves to single-factor short cuts such as merely focusing on the location of the data, the nationality of the suspect etc.

20. Much work obviously 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 are precedents to draw upon such as the system under which one country can proceed, for example in regard to the wiretapping, without seeking prior consent from another country. And if we can agree that it is the challenges associated with fleshing out the framework for investigate jurisdiction canvassed above that we should focus on, we have already made tremendous progress towards a framework for tackling the issue of cross-border access to electronic evidence.

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.

[8] See further: Dan Svantesson, A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft, 109 *American Journal of International Law Unbound* 69 (2015) https://www.asil.org/blogs/new-jurisprudential-framework-jurisdiction-beyond-harvard-draft.

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.