Submission by Professor Dan Jerker B. Svantesson to the Department of Infrastructure, Transport, Regional Development, Communications and the Arts regarding:

Statutory Review of the Online Safety Act 2021 Issues paper

June 2024

Professor Dan Jerker B. Svantesson
The Centre for Space, Cyberspace & Data Law
Faculty of Law, Bond University
Gold Coast, Queensland, 4229
Australia
[redacted]

Summary of major points

- The *Online Safety Act 2021* plays an important role for Australia.
- Several amendments may be useful to equip it to better serve Australia.
- The review should also ensure that increased clarity is provided in relation to key issues such as the issue of 'scope of jurisdiction' for orders made under the *Online Safety Act 2021*.
- The recent matter in *eSafety Commissioner v X Corp* [2024] FCA 499 highlights the need for clarity on what is meant by "all reasonable steps" and "be accessed by end users in Australia" under s. 109 of the *Online Safety Act 2021*.
- These submissions outline ten principles that can helpfully assist in the drafting of a detailed interpretation of the requirement that "the material can be accessed by end-users in Australia" and the limitation imposed by the reference to "all reasonable steps" in s. 109.

1. General remarks

1. I welcome the initiative taken to seek input on the *Online Safety Act 2021* as per the Issues Paper.

2. These submissions are intended to be made public. They express the view of the author alone.

3. These submissions deal only with a selection of issues. No views are expressed on any other matters.

4. The *Online Safety Act 2021* and the eSaftey Commissioner play important roles for Australia.

5. The useful Issues Paper shows that several amendments may be useful to equip the *Online Safety Act 2021* to better serve Australia in the light of challenges we face. The review should also ensure that increased clarity is provided in relation to key issues such as the issue of 'scope of jurisdiction' for orders made under the *Online Safety Act 2021*.

2. The issues addressed in these submissions

6. 'Scope of jurisdiction' relates to the appropriate geographical scope of a content-related decision such as a court order. Such issues arise under the *Online Safety Act 2021*. This was on display in the recent action against X Corp.[1] As that matter related to s. 109, that provision will be in focus here as an illustration of the 'scope of jurisdiction' issues that arise under the *Online Safety Act 2021*. In particular, as far as s. 109 is concerned, the question of 'scope of jurisdiction' depends on the interpretation of "all reasonable steps" and of "be accessed by end-users in Australia".

7. The 'scope of jurisdiction' issues discussed in these submissions are directly relevant for several of the specific questions raised in the Issues Paper. See in particular questions:

> 6. To what extent should online safety be managed through a service providers' terms of use?
>
> 15. Does the Commissioner have sufficient powers to address harmful material that depicts abhorrent violent conduct? Other than blocking access, what measures could eSafety take to reduce access to this material?
>
> 17. Does the Act need stronger investigation, information gathering and enforcement powers?
>
> 19. What more could be done to enforce action against service providers who do not comply, especially those based overseas?

[1] *eSafety Commissioner v X Corp* [2024] FCA 499.

20. Should the Commissioner have powers to impose sanctions such as business disruption sanctions?

26. Are additional safeguards needed to ensure the Act upholds fundamental human rights and supporting principles?

31. What features of the Act are working well, or should be expanded?

3. Section 109

8. Section 109 of the *Online Safety Act 2021* reads as follows:

> **Removal notice given to the provider of a social media service, relevant electronic service or designated internet service**
>
> (1) If:
>
> (a) material is, or has been, provided on:
>
> (i) a social media service; or
>
> (ii) a relevant electronic service; or
>
> (iii) a designated internet service; and
>
> (b) the Commissioner is satisfied that the material is or was class 1 material; and
>
> (c) the material can be accessed by end-users in Australia; and
>
> (d) the service is not:
>
> (i) an exempt Parliamentary content service; or
>
> (ii) an exempt court/tribunal content service; or
>
> (iii) an exempt official - inquiry content service;
>
> the Commissioner may give the provider of the service a written notice, to be known as a removal notice , requiring the provider to:
>
> (e) take all reasonable steps to ensure the removal of the material from the service; and
>
> (f) do so within:
>
> (i) 24 hours after the notice was given to the provider; or
>
> (ii) such longer period as the Commissioner allows.
>
> (2) So far as is reasonably practicable, the material must be identified in the removal notice in a way that is sufficient to enable the provider of the service to comply with the notice.

9. Thus, Australia's *Online Safety Act 2021* gives the eSafety Commissioner powers to issue a 'removal notice' requiring the provider to "take all reasonable steps to ensure the removal

of the material from the service" provided that certain conditions are met. The key condition in the discussion of 'scope of jurisdiction' is that the eSafety Commissioner can only do so if "the material can be accessed by end users in Australia".

10. In drafting s. 109, it would have been appropriate for the lawmaker to clearly and directly engage with the scope of jurisdiction issues that inevitably arise, as was illustrated in the X Corp. dispute.[2] Guidance is needed on what is meant when the *Online Safety Act* speaks of "all reasonable steps" and whether "the material can be accessed by end users in Australia".

11. It is regrettable that lawmakers in Australia have consistently taken a 'head-in-the-sand' approach to the question of 'scope of jurisdiction'. The failure to address it in the *Online Safety Act 2021* is only one example. A more current example is found in the recent reform to Australia's defamation law which gave courts the power to order a digital intermediary, such as a social media platform, to take access prevention steps or other steps the court considers necessary in the circumstances to prevent or limit the continued publication or republication of the matter.[3] Also here the lawmakers refused to engage with the question of 'scope of jurisdiction' resulting in a failure to set any limitations preventing, or provide guidance for, orders with global effect.[4]

12. The fact that this 'head-in-the-sand' approach to the question of 'scope of jurisdiction' is problematic was, as noted, on display in the recent X Corp. dispute.[5] The current review represents an excellent opportunity to finally provide guidance, at least as far as the *Online Safety Act 2021* is concerned.

4. The 'scope of jurisdiction' function of s. 109

13. Put simply, the 'scope of jurisdiction' function that needs to be incorporated in a provision such as s. 109 of the *Online Safety Act 2021* has two sides. First, it needs to ensure that the power to make orders under s. 109 is far-reaching enough to be effective. Second, it needs to ensure that the orders made under s. 109 do not have unnecessary and unjustified 'spillover' effects impacting foreign parties.

[2] *eSafety Commissioner v X Corp* [2024] FCA 499.

[3] https://pcc.gov.au/uniform/2023/pcc-584-d05b.pdf.

[4] https://dcj.nsw.gov.au/documents/about-us/engage-with-us/public-consultations/review-model-defamation-provisions/stage-2/professor-dan-svantesson-submission.pdf.

[5] *eSafety Commissioner v X Corp* [2024] FCA 499.

14. As alluded to, the two feature of s. 109 that can help achieve this balance are the requirement that "the material can be accessed by end-users in Australia" and the limitation imposed by the reference to "all reasonable steps".

5. Ten principles for scope of jurisdiction

15. It is not my ambition in these submissions to provide a detailed interpretation of the requirement that "the material can be accessed by end-users in Australia" and the limitation imposed by the reference to "all reasonable steps" in s. 109. Rather, building on a framework for scope of jurisdiction I have developed earlier, I here present ten principles that ought to guide how courts and regulators approach scope of jurisdiction in situations such as when interpreting the noted aspects of s. 109 of the *Online Safety Act 2021*.[6]

The fact that laws vary matters

Posting a satirical message that, by any imputation, innuendo, or insinuation, directly or indirectly, defiles the sacred name of the Holy Prophet Muhammad will, for example, violate Pakistan's strict blasphemy rules.[7] Comparing the appearance of Chinese leader Xi Jinping with that of Winnie the Pooh may result in censorship in China.[8] The diversity is great and the risks of unintentionally violating a foreign law can neither be predicted, nor be ignored.

Courts must take account of this indisputable diversity. As noted by Louis D Brandeis: "If we desire respect for the law, we must first make the law respectable."[9] Thus, while a worldwide scope of jurisdiction can be justified in certain circumstances, it must be recognised that the legitimacy of speech-restricting laws is, as default, limited in geographical scope.

[6] These ten principles were first presented in: D. Svantesson, "Scope of Jurisdiction" – A Key Battleground for Private International Law Applied to the Internet, Yearbook of Private International Law, Volume 22 (2020/2021), pp. 245-274.

[7] Pakistan Penal Code (Act XLV of 1860), § 295-C.

[8] S. McDonell, Why China censors banned Winnie the Pooh. BBC (2017, 17 July). Retrieved from https://www.bbc.com/news/blogs-china-blog-40627855 on 29.5.2021.

The fact that the application of laws varies matters

Fundamental human rights such as the protection of expression, privacy, and reputation, apply worldwide. But the instruments in which those important rights are articulated merely set a baseline. Different countries reconcile and balance those fundamental human rights in different manners. Thus, a court adopting a far-reaching scope of jurisdiction must consider, not just the balance it has struck between competing fundamental rights, but the fact that clashes between human rights (such as clashes between the freedom of expression and the right of reputation) may be balanced differently in other states affected by the order. States should generally avoid imposing their balance of those rights on other states.

Legitimacy outweighs efficiency

In the context of fundamental human rights such as freedom of expression, legitimacy must always be given greater weight than is given to procedural efficiency. In fact, any situation where the court in one state is entrusted with jurisdiction to adjudicate – on a speech matter – for other states, represents fairness, accuracy and the values of the individual states being sacrificed on the altar of procedural efficiency.

There is a link between scope of jurisdiction and the legitimacy of claims of jurisdiction

Whether a court ought to claim jurisdiction or not will frequently depend on what that court will do if it does claim jurisdiction. For example, if we know that a court is likely to seek to impose its will on the world at large – e.g., by ordering the global removal of certain Internet content – we may not favour that the court jurisdiction in the first place. This shows that the question of jurisdiction and the question of scope of jurisdiction are intrinsically linked.

There is a link between the strength of the claim of jurisdiction and the scope of jurisdiction

The legitimacy of a broad scope of jurisdiction (such as a worldwide order) increases with the strength of the connection between the forum and the dispute and the parties as assessed e.g., in the analysis of *in personam* jurisdiction, subject matter jurisdiction and territorial competence. In general terms, a court has greater legitimacy in granting a worldwide injunction in a domestic dispute between two domestic parties than it has in making an order against a foreign party in an international dispute.

In the light of how the strength of the connection between the forum and the dispute and the parties impact the legitimacy of the scope of jurisdiction, it is not appropriate for courts to 'compartmentalise' their assessment of jurisdiction and scope of jurisdiction. Finding a

weak but sufficient ground for jurisdiction should impact the reasoning on the scope of jurisdiction.

There is a link between the strength of the defendant's connection to the forum and scope of jurisdiction

There is a link between the strength of the defendant's connection to the forum and scope of jurisdiction. Relatedly, there is a difference between an order against a party to the dispute and an order against a non-party. Even in a situation where all other factors point to a broad scope of jurisdiction being legitimate, an order with a broad scope may not necessarily be legitimate against a non-party even where it is legitimate against a party to the dispute.

Perhaps it may even be argued that, where an order is directed at a party that is at fault in some sense, the legitimacy of a broad scope of jurisdiction increases with the degree of fault attributable to that party. Correspondingly then, where the party at which the order is directed is not at fault it is more difficult to justify a broad scope of jurisdiction. This may perhaps justify an approach under which plaintiffs are directed to first seek removal/blocking by the original poster before being allowed to request removal/blocking by intermediaries.[10]

The scope of jurisdiction must be guided by the potential impact on other countries and persons in other countries

The reality is that with an interconnected world – not least online – it is quite simply impossible to avoid situations where court orders in one country have an effect in other countries. In other words, some 'collateral damage' may be unavoidable.

However, as acknowledged e.g., by AG Szpunar and by the Court of Appeal in the *Google Canada* matter, any order that impacts the sovereignty of another country must be carefully assessed as to whether it is nevertheless appropriate: "[C]ourts should be very cautious in making orders that might place limits on expression in another country. Where there is a realistic possibility that an order with extraterritorial effect may offend another state's core values, the order should not be made."[11]

[10] See further: D. SVANTESSON, Limitless borderless forgetfulness? Limiting the geographical reach of the 'right to be forgotten', *Oslo Law Review* 2015/2 (2), p. 116 *et seq*.

[11] Decision of the Court of Appeal of British Columbia dated June 11, 2015 [92]. See also: *eSafety Commissioner v X Corp* [2024] FCA 499.

Thus, the greater the impact on foreign countries, and persons in foreign countries, the stronger the reason to limit the scope of jurisdiction. This is particularly so where the impact relates to (1) strangers to the lawsuit and/or (2) the fundamental human rights, such as privacy, reputation, and freedom of expression, of the persons in foreign countries.

The scope of jurisdiction must be legitimate by reference to the principle of scalability

In international law, much weight is given to state practice.[12] This ought to create a strong incentive for countries to pursue scalable universal approaches given that a broad uptake of their approaches legitimacies those approaches. However, scalability does not seem to have been considered much in the context of scope of jurisdiction assessments.

Rather, states base their claims solely on domestic law and needs with the occasional reference to vague principles of international law. *De lege ferenda*, they should also take into account of what will be the effect if other countries adopt the same approach;[13] that is the question of scalability.

The scope of jurisdiction must be legitimate by reference to the principles of necessity and proportionality

The appropriateness of granting an order with a broad scope of jurisdiction is affected by factors such as the cost of complying with that order, whether the order is limited in time, the availability of less onerous alternative measures and the effectiveness of the order (both in an absolute sense, and as compared to alternative measures).[14]

Like it is in so many other settings, assessing the necessity and proportionality in the context of scope of jurisdiction matters is complex. Yet, there are some guidance to be had. Elsewhere, I have, for example, argued that one matter — a rule of thumb — that will be helpful in determining whether certain content justifies a broader scope of jurisdiction is whether the nature of the content is such that a reasonable person would legitimately be concerned or offended about a random third person viewing that content. The availability of

[12] See in particular: *Statute of the International Court of Justice*, Article 38(1)(b).

[13] Compare to the 'global south impact assessment' advocated in D. SVANTESSON, *Internet & Jurisdiction Global Status Report 2019*, Paris, Internet & Jurisdiction Policy Network 2019, p 64: "it is arguably reasonable to expect lawmakers in those countries that commonly influence policy and law developments globally to conduct what may be termed a 'global south impact assessment', assessing: (1) what impact their approaches will have in the global south, and (2) what will happen if the global south adopts their approaches."

[14] For this factor, I draw upon Justice Arnold's reasoning in *Cartier International AG et al v British Sky Broadcasting Ltd et al* [2014] EWHC 3354 (Ch).

the sort of negative financial information at issue in the well-known *Google Spain* – right to be forgotten – case[15] may only legitimately trouble a reasonable person where it is accessed by either a person who knows the data subject or may enter into dealings or contact with the data subject. In contrast, a reasonable person may legitimately feel uncomfortable about so-called 'revenge porn' content depicting the sexual activities of the data subject even where that content is accessed by a random third person. Similarly, the potential harm that may stem from confidential details that expose the data subject to a serious risk of fraud or theft may, of course, be a legitimate concern also where that content is accessed by a random third person.

One size does not fit all

When it comes to scope of jurisdiction, we cannot work on the assumption that one size fits all. Rather, appropriate solutions will be context-specific, and we need to adopt what I elsewhere have termed a 'consequence focused approach';[16] that is, rather than restricting ourselves to a blind adherence to the exact wording of the law (a literal interpretation), we must seek to identify the consequences of the various possible interpretations of the law.

When we do so, it is obvious that, as I have argued since 2014, 'one size does not fit all'.[17]

[15] Case C-131/12 Google Spain SL, Google Inc v Agencia Española de Protección de Datos, Mario Costeja González.

[16] D. SVANTESSON, 'What is "Law", if "the Law" is Not Something That "Is"? A Modest Contribution to a Major Question' (2013) 26(3) Ratio Juris 456. For a useful illustration of this 'consequence focused approach' being applied, see e.g.: Opinion of Advocate General Jääskinen in Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD) (Case C-131/12) at [30]-[31].

[17] D. SVANTESSON, Delineating the Reach of Internet Intermediaries' Content Blocking – 'ccTLD Blocking', 'Strict Geo-location Blocking', or a 'Country Lens Approach'?, *SCRIPT-ed* 11/2 (2014) pp. 153-170, at 168. See further: D. SVANTESSON, *Internet & Jurisdiction Global Status Report 2019*, Paris, Internet & Jurisdiction Policy Network 2019, pp. 151-152; J. DASKAL, Speech Across Borders, 105 VA. L. REv. 1605, 1625 (2019).

Professor Dan Jerker B. Svantesson

Dan Jerker B Svantesson is a Professor at the Faculty of Law in Bond University where he is a co-director for the Centre for Space, Cyberspace & Data Law. He is a Senior Fellow with the Social Cyber Institute, and specialises in international aspects of the IT society, a field within which he has authored or co-authored more than 280 publications, and given presentations in Australia, Asia, Africa, North America, and Europe. Dan is an Associated Researcher at the Swedish Law & Informatics Research institute, Stockholm University, he held an ARC Future Fellowship (2012-2016) and was the inaugural Managing Editor for International Data Privacy Law, published by Oxford University Press. He is a Member of the Editorial Boards for several journals, including the Commonwealth Cybercrime Journal, the International Cybersecurity Law Review, the International Journal of Law and Information Technology, the Commonwealth Law Bulletin, the International Review of Law Computers and Technology, the Masaryk University Journal of Law and Technology and the Computer Law and Security Review. Professor Svantesson has authored and contributed to commissioned reports by several international organisations including the UNODC, OECD, UNCTAD, the Commonwealth Secretariat, and the Internet & Jurisdiction Policy Network. He has been identified as the Field Leader for "Technology Law" in studies published by League of Scholars together with The Australian for four years (2021, 2020, 2019, 2018), and has given expert opinions before leading courts such as the Court of Justice of the European Union.