Global content orders: A legal analysis of eSafety Commissioner

Professor Dan Jerker B. Svantesson

Abstract: The dispute between the Australian eSafety Commissioner and X Corp. (formerly Twitter) in relation to an order requiring global removal of certain footage of a stabbing has brought attention to the topic of 'scope of jurisdiction'. Scope of jurisdiction relates to the appropriate geographical scope of a content-related decision such as a court order. Australia has a mixed 'track-record' when it comes to dealing with scope of jurisdiction and this ongoing dispute represents an opportunity for Australia to lead the way by adopting a sophisticated framework for this type of matters.

Centre for Space, Cyberspace & Data Law 2024:1

7 May 2024

Global content orders: A legal analysis of eSafety Commissioner

Professor Dan Jerker B. Svantesson

Key points

This Paper discusses the legal issues arising in the dispute between the Australian eSafety Commissioner and X Corp. (formerly Twitter) in relation to an order requiring global removal of certain footage of a stabbing. Key points include:

- The disputed footage of the stabbing has no 'free speech' value.
- X Corp.'s terms of service should be read in the light of X Corp. being a supporter of the 'Christchurch Call'.
- X Corp. should have acted responsibly and maturely, removing the disputed footage voluntarily by reference to its terms of service and commitments under the Christchurch Call.
- The eSafety Commissioner's request for global removal is based on *Online Safety Act 2021* (Cth), section 109, and the key question in dispute is whether the disputed content "can be accessed by end users in Australia" even where X Corp. has used geo-location technologies to block Australian end users.
- The circumvention of geo-location technologies typically requires intent, and those who would have the intent to access

Briefly about the author

The author of this Paper – Dan Jerker B. Svantesson – is a Professor at the Faculty of Law and Co-director of the Centre for Space, Cyberspace & Data Law. Professor Svantesson is also a Senior Fellow at the Social Cyber Institute, a Researcher at the Swedish Law & Informatics Research Institute, Stockholm University (Sweden). He serves on the editorial board on a range of journals relating to information technology law, data privacy law, cybersecurity, and law generally.

Professor Svantesson has written extensively on Internet jurisdiction matters and has won several research prizes and awards.

The views expressed herein are those of the author alone.

the disputed footage by circumventing the 'geo-blocking' will be able to find the content on other sites on the Internet.

- Section 109 of the *Online Safety Act 2021* (Cth), must be interpreted as meaning that where geo-location technologies are used appropriately to block Australian end users, the material in question cannot "be accessed by end users in Australia" even where such geo-location technologies can be circumvented.

- Whenever a court makes a content-related decision, it must confront the matter of 'scope of jurisdiction'. Scope of jurisdiction relates to the appropriate geographical scope of a content-related decision such as a court order.

- Given that a broad scope of jurisdiction may significantly impact foreign countries and persons in foreign countries, a court determining the scope of jurisdiction in a particular matter is bound by both domestic (private international law rules as well as e.g., constitutional law) and international law.

- Orders with a global scope of jurisdiction may be justified in some circumstances but cannot be the default position.

- In approaching the question of scope of jurisdiction, a court may usefully adopt the framework outlined in this Paper.

The Paper draws, and expands, on:

Dan Svantesson, *Elon Musk vs Australia: global content take-down orders can harm the internet if adopted widely*, The Conversation (23 April 2024) https://theconversation.com/elon-musk-vs-australia-global-content-take-down-orders-can-harm-the-internet-if-adopted-widely-228494

Dan Svantesson, *Elon Musk, Australia, and global content take-down: A legal analysis*, LinkedIn (27 April, 2024) https://www.linkedin.com/pulse/elon-musk-australia-global-content-take-down-legal-svantesson-0ycdc/

Dan 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

Background

On 15 April 2024, a bishop in Sydney was stabbed during a church service. The stabbing was recorded and streamed as the service was live streamed. Following this event, Australia's eSafety Commissioner[1] worked cooperatively with leading tech companies, including, Google, Microsoft, Snap and Tik Tok, to remove the material.[2] On April 16, 2024, the eSafety Commissioner issued removal notices to Meta and X Corp. Meta removed the material identified in the notice. However, X Corp. did not. Instead, X Corp. used geo-location technologies to prevent Australian end-users from accessing the materials. The eSafety Commissioner "was not satisfied the actions it took constituted compliance with the removal notice and sought an interim injunction from the Federal Court."[3] The Court gave the interim injunction on 22 Aril 2024[4] and has since extended it via a new order on 24 April 2024.[5] A new hearing is scheduled for 10 May 2024.

What X Corp. should have done

In my view, the footage of the stabbing has no 'free speech value', and X Corp. ought to have acted maturely and responsibly and removed it voluntarily like other social media platforms did. My reading of X Corp.'s policies[6] suggests that they could, and should, have done so. After all, X Corp. specifically reserves "the right to remove Content that violates the User Agreement, including for example, […] unlawful conduct". This is further supported by the fact that X Corp. is a supporter of the so-called 'Christchurch Call'[7] that acts to eliminate terrorist and violent extremist content online. Under the Christchurch Call, X Corp. as an online service provider commits to:

> "Take transparent, specific measures seeking to prevent the upload of terrorist and violent extremist content and to prevent its dissemination on social media and similar content-sharing services, including its immediate and permanent removal, without prejudice to law enforcement and user appeals requirements"[8]

There can sometimes be real tension between free speech and the suppression of violent imagery. For example, some news reporting from military conflicts may be deemed too graphic by some, while others view it as a necessary tool to illustrate the level of violence being committed. Here, there are no such complex considerations.

---

[1] https://www.esafety.gov.au/.
[2] https://www.esafety.gov.au/newsroom/media-releases/statement-on-removal-of-extreme-violent-content.
[3] https://www.esafety.gov.au/newsroom/media-releases/statement-on-removal-of-extreme-violent-content.
[4] https://www.comcourts.gov.au/file/Federal/P/NSD474/2024/3979442/event/31767828/document/2267337.
[5] https://www.comcourts.gov.au/file/Federal/P/NSD474/2024/3979442/event/31770572/document/2268490; https://www.esafety.gov.au/newsroom/media-releases/statement-on-federal-court-order.
[6] https://twitter.com/en/tos.
[7] https://www.christchurchcall.com/.
[8] https://www.christchurchcall.com/about/christchurch-call-text.

The legal issues at the hearing 10 May 2024

X Corp. has made clear what it sees as the two core legal issues: "First, we believe that these posts should not have been banned in Australia at all. […] Second, we oppose the demand to globally remove this content from X".[9]

I do not imagine X Corp. will have much luck on its first point. The stabbing attack has been labelled as an act of terrorism, and the footage is likely to be classed as content that would be "refused classification under the National Classification Scheme".[10]

The second issue raised by X Corp. is more complex and will the topic in focus in the below.

The demand to globally remove the content – 'scope of jurisdiction'

Whenever a court makes a content-related decision, it must confront the matter of 'scope of jurisdiction'[11] or 'scope of remedial jurisdiction' as preferred by the Court of Appeal for British Columbia in the *Equustek* case.[12] Scope of jurisdiction relates to the appropriate geographical scope of a content-related decision such as a court order.

Thus, assuming that the Federal Court on May 10 decides to limit the distribution of the relevant footage, it must decide whether to order the relevant content to be limited only in Australia, globally, or somewhere in between these extremes. It goes without saying that this is a key question from the perspective of Internet governance. Indeed, while it remains an emerging area of study, it is a topic that will only increase in significance over the coming years.

Given that a broad scope of jurisdiction may significantly impact foreign countries and persons in foreign countries, a court determining the scope of jurisdiction in a particular matter is bound by both domestic (private international law rules as well as e.g., constitutional law) and international law. This is uncontroversial and indeed is frequently – but unfortunately not always – reflected in the judgments by courts.

[9] https://www.afr.com/companies/media-and-marketing/the-real-reason-elon-musk-is-taking-on-australia-20240425-p5fmi3.
[10] https://www.esafety.gov.au/sites/default/files/2022-03/Online%20Content%20Scheme%20Regulatory%20Guidance.pdf?v=1714186259819.
[11] DJB Svantesson, 'A Third Dimension of Jurisdiction', *LinkedIn*, 3 May 2015, available at https://www.linkedin.com/pulse/third-dimension-jurisdiction-dan-jerker-b-svantesson/ on 29.5.2021, followed by DJB Svantesson, Jurisdiction in 3D – "scope of (remedial) jurisdiction" as a third dimension of jurisdiction, *Journal of Private International Law* 2016/12:1, 60 *et seq.*
[12] *Equustek Solutions Inc v Google Inc* [2015] BCCA 265, [69].

Relevant domestic law

Australia's *Online Safety Act 2021* (Cth)[13] gives the eSafety Commissioner powers to issue a 'removal notice' requiring the provider (in this case X Corp.) to "take all reasonable steps to ensure the removal of the material from the service" (s. 109) provided that certain conditions are met. The key condition in this dispute is that the eSafety Commissioner can only do so if "the material can be accessed by end users in Australia". The key question for the Court on May 10 is then whether it can be said that the controversial footage can be accessed by end users in Australia even where X Corp. has used geo-location technologies to block Australians from accessing that content.

The eSafety Commissioner argues that the use of geo-location technologies to block Australians from accessing the content is insufficient to achieve a situation where the material cannot be accessed by end users in Australia since the blocking can be circumvented e.g. with the use of VPNs.

Of course, a court order requiring X to take down certain content globally is more effective than a court order requiring X to geo-block such content so that users in Australia cannot access it. But that efficiency argument applies equally to all laws around the world, and given the diversity of domestic laws we may ask what would be left online if only content that was lawful globally could be anywhere online.

Furthermore, even if X Corp. removed the content on a global basis, those Australians who are determined to view the footage in question would be able to find it somewhere else online. In other words, there is no realistic way to fully ensure the content cannot be accessed at all.

Ordering X to use geo-location technologies to block Australians from viewing the content would be sufficient to prevent the general Australian public from coming into contact with the footage.[14] Where the content can only be accessed by those determined enough to seek out the content by circumventing the 'geo-blocking', it cannot be said that the content "can be accessed by end users in Australia". Denying this is akin to saying that a locked door is not sufficiently locked if someone can break it open with certain tools.

To fully appreciate the matter before the Court, it may be helpful to remember that this is not the first time Australian courts have had to address the topic of whether our laws can decide what may be online globally. In 1999, in one of Australia's earliest Internet jurisdiction cases, the Court steered clear of claiming global scope of jurisdiction. Justice Simpson sensible noted:

> "An injunction to restrain defamation in NSW is designed to ensure compliance with the laws of NSW, and to protect the rights of plaintiffs, as those rights are defined by the law

[13] https://www.legislation.gov.au/C2021A00076/latest/text.

[14] https://www.linkedin.com/pulse/circumvention-geo-blocking-big-issue-content-blocking-svantesson/?trackingId=yA8980A1Q0GE23P4zsRsjw%3D%3D.

> of NSW. Such an injunction is not designed to superimpose the law of NSW relating to defamation on every other state, territory and country of the world. Yet that would be the effect of an order restraining publication on the Internet."[15]

This changed radically in 2017 in a case with a now rather amusing name. In *X v Twitter*[16] (X indicated an unnamed plaintiff, not the social media company), Justice Pembroke granted an order requiring Twitter to remove content posted by one of its users anywhere in the world. In fact, the order went as far as to requiring Twitter to prevent the offending user from ever posting any type of content on Twitter again even though it was possible that the offending user was not an Australian.[17] Remarkably, Justice Pembroke did so without even mentioning the international implications of such an order – the topic that is now so hotly debated.

Unfortunately, lawmakers in Australia have consistently taken a 'head-in-the-sand' approach to the question of scope of jurisdiction. The law that the eSafety Commissioner bases her claim on is an example of this. The relevant provision of the *Online Safety Act* speaks of whether "the material can be accessed by end users in Australia" without discussing what this means in practical terms.

Similarly, through the recent reform to Australia's defamation law, courts get 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.[18] However, the law drafters refused to engage with the question of scope of jurisdiction so they fail to set any limitations preventing, or provide guidance for, orders with global effect.[19]

The bigger picture – global consequences and international law

Hopefully the Court will also engage with the international law question of whether Australia has a right to make take-down orders with global effect. Looking at past experiences, outlined above, we can see a mixed experience with Justice Simpson acknowledging Australia's responsibilities on the global stage while Justice Pembroke displayed ignorance of, or contempt for, the international dimension of content-related orders. But perhaps the enormous attention that this matter has attracted in media will force the Court to engage ´with this 'bigger picture'.

[15] https://www8.austlii.edu.au/cgi-bin/viewdoc/au/cases/nsw/NSWSC/1999/526.html.
[16] https://www8.austlii.edu.au/cgi-bin/viewdoc/au/cases/nsw/NSWSC/2017/1300.html.
[17] https://www.linkedin.com/pulse/sydney-become-internet-content-blocking-capital-world-svantesson/?trackingId=yA8980A1Q0GE23P4zsRsjw%3D%3D.
[18] https://pcc.gov.au/uniform/2023/pcc-584-d05b.pdf.
[19] https://dcj.nsw.gov.au/documents/about-us/engage-with-us/public-consultations/review-model-defamation-provisions/stage-2/professor-dan-svantesson-submission.pdf.

The relevant international law is admittedly vague and unsettled. It will not be explored in detail here. However, what is clear is that courts cannot ignore international law in situations such as this.

Furthermore, courts ought to seek to apply domestic law in a manner that takes account of the global consequences. We can safely assume that there are countries in the world where this type of content is not illegal. In those countries people, thus, have a right to view it. We are then talking about foreign citizens in a foreign country access content on a foreign platform. If the Court is to conclude that Australian law somehow has the power to override their right to access the content, it must have a clear and convincing case for why that is so.

The Court will also have to confront the uncomfortable 'other side of that coin'; that is, if Australian courts have the right to decide what foreign citizens, located overseas, view online on a foreign platform are we equally happy for courts in other countries to determine what Australians can see and post online in Australia?

What is need is a full assessment and to assist with this, I have elsewhere developed a framework for scope of jurisdiction.

Ten 'commandments' for scope of jurisdiction

Building on a framework for scope of jurisdiction I have developed, I here present the ten commandments (or at least principles) that ought to guide how courts approach scope of jurisdiction.[20]

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.[21] Comparing the appearance of Chinese leader Xi Jinping with that of Winnie the Pooh may result in censorship in China.[22] The diversity is great and the risks of unintentionally violating a foreign law can neither be predicted, nor be ignored.

[20] 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.
[21] Pakistan Penal Code (Act XLV of 1860), § 295-C.
[22] 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.

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."[23] 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.

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 the court's 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. Subjecting a foreign defendant with a weak connection to the forum to an order with a global scope of jurisdiction is a more severe step than subjecting a local person or entity to such an order.

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.[24]

[24] 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*.

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."[25]

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.[26] 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;[27] that is the question of scalability.

[25] Decision of the Court of Appeal of British Columbia dated June 11, 2015 [92].
[26] See in particular: *Statute of the International Court of Justice*, Article 38(1)(b).
[27] 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."

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).[28]

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 the sort of negative financial information at issue in the well-known *Google Spain* – right to be forgotten – case[29] 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';[30] 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'.[31]

---

[28] 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).

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

[30] 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].

[31] 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.

Final remarks

The regulation of online content raises a range of complex questions with which courts and legislators typically must engage. Given the centrality of freedom of expression in any functioning democracy, the issues at stake are important indeed. But while the complexity of balancing – or preferably reconciling – fundamental rights in a domestic setting is obvious, it is greatly amplified where it is brought to an international level as often is the case with online content regulation. Put simply, there is no international consensus on online content regulation.

The question of scope of jurisdiction goes to the core of what we want the Internet to look like, both now and in the future. Its importance has been underestimated for far too long. But given the current debates, I am hopeful that lawmakers can no longer 'sweep it under the carpet', and that Australian courts finally must confront the misguided precedent set back in 2017 in *X v Twitter*.

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).

Additional resources:

For additional works, by the author of the Report, that expand upon the arguments raised here works, see:

Private International Law and the Internet 4th Ed, Kluwer Law International (2021)

Solving the Internet Jurisdiction Puzzle, Oxford University Press (2017)

Extraterritoriality in Data Privacy Law, Ex Tuto Publishing (2013)

Internet & Jurisdiction Global Status Report 2019, Internet & Jurisdiction Policy Network (November 2019) (184 pages)

A decision-making guide for online content regulation', Alternative Law Journal (2024), https://journals.sagepub.com/doi/10.1177/1037969X241231327 (Peer reviewed)

(With Michal Czerniawski) Challenges to the extraterritorial enforcement of data privacy law – EU case study, in Daniel Westman et al., (eds.), Dataskyddet 50 år – historia, aktuella problem och framtid (2023) pp. 127-154

Global speech regulation: extraterritoriality in the context of internet content blocking, removal, de-listing, and must carry orders, in Austen Parrish & Cedric Ryngaert (eds.), Research Handbook on Extraterritoriality in International Law, Edward Elgar Publishing (2023) pp. 459-476

(With Ioannis Revolidis) From eDate to Gtflix: Reflections on CJEU case law on digital torts under Art. 7(2) of the Brussels Ia Regulation, and how to move forward, in Paris Arvanitakis (ed.), National and International Legal Space: The Contribution of Prof. Konstantinos Kerameus in International Civil Procedure, Sakkoulas Publications (2022), pp. 319-372

Is International Law Ready for the (Already Ongoing) Digital Age: Perspectives from Private and Public International Law, in Preadviezen: International Law for a Digital World: Collected Papers 147, Asser Press (2020) pp. 113-155

Internet Jurisdiction and Intermediary Liability, in Giancarlo Frosio (ed.), The Oxford Handbook of Online Intermediary Liability, Oxford University Press (2020) pp. 691-708

Article 3. Territorial Scope, in Christopher Kuner et al. (eds), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press (2020) pp. 74-99

Are we Stuck in an Era of Jurisdictional Hyper-regulation?, in Peter Wahlgren (Ed.), Scandinavian Studies in Law: 50 Years of Law and IT Vol. 65 (2018) pp. 143-157

Cyberborders through 'Code': An All-or-Nothing Affair?, in Uta Kohl (ed.), The Net and the Nation State - Multidisciplinary Perspectives on Internet Governance, Cambridge University Press (2017); 110-124

Legal Theories of Private International Law: Overview and Practical Implications for Internet Regulation, in Patrik Lindskoug et al., (eds.), Essays in Honour of Michael Bogdan, Juristförlaget i Lund (2013); 539-555

Online cross-border defamation disputes, in Dan Jerker B. Svantesson & Stanley Greenstein (ed.), Nordic Yearbook of Law and Informatics 2010–2012: Internationalisation of Law in the Digital Information Society, Ex Tuto Publishing (2013); 195-215

Cross-border internet defamation conflicts and what to do about them: Two proposals, Journal of Private International Law Vol 19 No 2 (2023) (With Symeon C. Symeonides); pp. 137-185 (Peer reviewed)

Online Intellectual Property Disputes and Private International Law: A Swedish and Australian perspective, Lex&Forum, 2/2023 (2023), pp. 345-356 (Peer reviewed)

"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 (Peer reviewed)

Scope of jurisdiction online and the importance of messaging – lessons from Australia and the EU, Computer Law & Security Review 38 (2020) Article 105428 (Peer reviewed)

Grading Szpunar's Opinion in Case C-18/18 – A Caution Against Worldwide Content Blocking As Default, Masaryk University Journal of Law and Technology 13(2) (2019) pp. 389-400 (Peer reviewed)

European Union Claims of Jurisdiction over the Internet – an Analysis of Three Recent Key Developments, Journal of Intellectual Property, Information Technology and Electronic Commerce Law 9 (2018) pp. 113-125 (Peer reviewed)

'Lagom jurisdiction' – What Viking drinking etiquette can teach us about Internet jurisdiction and Google France, Masaryk University Journal of Law and Technology 12(1) (2018) pp. 29-47 (Peer reviewed)

Jurisdiction in 3D – "scope of (remedial) jurisdiction" as a third dimension of jurisdiction, Journal of Private International Law Vol 12 No 1 (2016); pp. 60-76 (Peer reviewed)

Limitless borderless forgetfulness? Limiting the geographical reach of the 'right to be forgotten', Oslo Law Review 2 (2) (2015) pp. 116-138 (Peer reviewed)

A Jurisprudential Justification for Extraterritoriality in (Private) International Law, Santa Clara Journal of International Law 13(2) (2015) pp. 517-571

The holy trinity of legal fictions undermining the application of law to the global Internet, International Journal of Law and Information Technology Vol. 23 No. 3 (2015); pp. 219-234 (Peer reviewed)

The Google Spain case: Part of a harmful trend of jurisdictional overreach, EUI Working Paper RSCAS 2015/45 (21 pages) (Reviewed by the EUI law professors)

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 (Peer reviewed)

Sovereignty in international law – how the Internet (maybe) changed everything, but not for long, Masaryk University Journal of Law and Technology 8(1) (2014) pp. 137-155 (Peer reviewed)

Between a rock and a hard place – an international law perspective of the difficult position of globally active Internet intermediaries, Computer Law & Security Review 30 (2014) pp. 348-356 (Peer reviewed)

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) (2014); pp. 53-102

How does the accuracy of geo-location technologies affect the law?, Masaryk University Journal of Law and Technology, Vol. 2 No. 1 (2008); pp. 11-21 (Peer reviewed)

Geo-identification and the Internet – A New Challenge for Australia's Internet Regulation, Murdoch E-Law Journal Vol 14, No 2, 2007; pp. 155 – 177 (Peer reviewed)

Protecting privacy on the "borderless" Internet – Some thoughts on extraterritoriality and transborder data flow, Bond Law Review 19(1) (June 2007); pp. 168 – 187 (Peer reviewed)

The Legal Implications of Geo-identification, Yearbook of New Zealand Jurisprudence special edition (2006) Vol. 9; pp. 279 – 287 (Peer reviewed)

Borders on, or border around – the future of the Internet, Albany Law Journal of Science & Technology, Vol. 16 No. 2 (2006); pp. 343 – 381

Geo-location technologies and other means of placing borders on the 'borderless' Internet, John Marshall Journal of Computer & Information Law, Vol XXIII, No 1, Fall 2004; pp. 101 – 139

About the Centre for Space, Cyberspace & Data Law

The Centre for Space, Cyberspace & Data Law is established at the Faculty of Law, Bond University (Australia). The Centre brings together researchers and experts in all aspects of space, cyberspace, and data-flows law to engage in research aimed at creating a better understanding of, and a better direction for, the relationship between space, Cyberspace, and data.

Suggested citation: Dan Jerker B. Svantesson, *Global content orders: A legal analysis of eSafety Commissioner v X Corp.*, Centre for Space, Cyberspace & Data Law 2024:1 (7 May 2024)