

**Submission by Professor Dan Jerker B. Svantesson to the UNESCO
global study on Internet-issues**

***Question 25 – How do cross-jurisdictional issues operate with
regard to freedom of expression and privacy?***

19 October 2014

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

Professor Svantesson is the recipient of an Australian Research Council Future Fellowship (project number FT120100583). The views expressed herein are those of the author and are not necessarily those of the Australian Research Council.

Summary of major points

In my view:

- both freedom of expression and privacy are essential conditions for democracy, development and human dignity. While we often need to balance the two, it is never a choice of one or the other; we need both freedom of expression and privacy;
- in some instances, both domestically and internationally, privacy is an essential condition for freedom of expression;
- also through the most mundane Internet activities, people are exposed to a complex matrix of overlapping, and sometimes contradictory, legal rules;
- there is a trend of increasing extraterritorial claims affecting Internet activities. Such claims may significantly impact freedom of expression, and the right of privacy;
- the legitimacy of extraterritorial claims is undermined by the difficulty of *accessing* and *understanding* foreign law. In fact, the well established principle that 'ignorance of the law is no defence' may legitimately be called into question where the laws to which people are exposed are not accessible in an understandable form. UNESCO may play an important role (perhaps with appropriate partnerships) in making foreign laws more accessible and understandable;
- in the absence of harmonised jurisdictional rules, it falls to the individuals to decide which conflicting laws to abide by and which laws to ignore. Such a decision, where it cannot be avoided, should most appropriately be guided by ethical considerations. UNESCO may be eminently well suited for the task of identifying how various ethical considerations ought to be balanced so as to adequately cater for the competing interest;
- UNESCO could usefully undertake work towards what we can call *jurisdictional interoperability*; identifying and ironing out legal differences (in both procedural and substantive law) that create barriers for cross-border interaction and, ultimately, an international agreement;
- there is a trend of courts requiring global blocking where they find content unlawful under their laws. This trend is particularly worrying in relation to actions taken against Internet intermediaries such as search engines and social media platforms;

- where an Internet intermediary is ordered to block or remove certain Internet content, the default position must be that ordinarily the blocking/removal should be geographically limited rather than having a global reach. UNESCO could undertake work to encourage respect for this suggested default position;
- in assessing whether two (or more) laws are in conflict, we need to take account of both the duties and the rights for which those laws provide;
- due to a number of drivers, we are currently witnessing a paradigmatic change in how states seek to regulate Internet activities; having seen the difficulties of extraterritorial enforcement, states are moving towards *domestic enforcement of extraterritorial claims* – they are taking *market destroying measures* to force foreign Internet actors to comply with states' laws; and
- while this development may be natural, it has great potential to cause tensions in international relations unless it is carefully monitored and managed. UNESCO is the most appropriate organisation to undertake this task.

1. Introduction

I welcome the initiative taken by UNESCO to initiate a discussion about the most suitable future direction in this area. The discussion is timely, and the provided documents are useful in identifying and highlighting key questions that must be considered.

These submissions are intended to be made public.

2. General remarks

Perhaps the most unique characteristic of Internet communication is its ability to enable individuals to become global publishers with comparatively simple and inexpensive means. The Internet is thus the great enabler of cross-border communication of information as varied as the thoughts created in the human mind – the Internet is morally neutral in the sense that ‘good’ and ‘bad’ content is, technically speaking, distributed in the same manner without discrimination. In light of this, there is little surprise in the fact that some content online violates some countries’ laws, for example, by infringing upon persons’ fundamental human right to privacy.

Too often, this sparks debates between those advocating privacy (often Europeans) and those pushing for unfettered free speech (typically from the US). However, the picture is more complex than that. Privacy may play an important role in enabling freedom of expression – sparked by fears of being e.g. fired, prosecuted or harassed, people may feel comfortable in making certain statements only where their identity is not revealed. It is this obvious fact that causes governments in some countries to impose rules (or technical standards) requiring Internet users to always be identifiable.

Importantly, the complex and multi-faceted relationship between freedom of expression and privacy exists also on an international level. Here, even more than in the domestic context, the discussion to date has been mainly focused on the clashes that often occur between the freedom of expression in one country and the protection of privacy in another country. Yet, also on an international level we can see privacy aiding the freedom of expression. For example, dissidents in one country (country A) may rely on Internet platforms or services from another country (country B) to express their views in country A. Where a court in country A then demands information from the Internet platform or service in country B, country B’s privacy laws may effectively protect the dissidents in country A. This scenario is by no means far-fetched, and the situation described is likely to become more and more common.

Thus, the first key conclusion must be that a loss of privacy may very well also be a loss for freedom of expression;¹ as noted on the UNESCO website, freedom of expression is “an essential condition for democracy, development and human dignity”. But so is privacy, and privacy may also be an essential condition for freedom of expression. In the end, it suffices to conclude that we need both privacy and freedom of expression.

The question of how cross-jurisdictional issues operate with regard to freedom of expression and privacy is broad indeed. I will here focus only on three particularly topical issues.

3. A trend of increasing extraterritorial claims

There is a trend of increasing extraterritorial claims affecting Internet activities. Examples may be drawn from a variety of areas, but the field of data privacy provides a rich source of particularly interesting examples. For example, while now amended and modified several times, the extraterritorial scope of the proposed EU Data Protection Regulation was such that Europeans would enjoy EU level data privacy rights even when they physically travelled to other countries – a German tourist in New York would be able to rely on EU data privacy law in its dealing with US organisations in the US. Despite its obvious absurdity, this provision met surprisingly little resistance. In fact, it gained very limited attention at all.

While this type of extreme example fortunately is rare, there is a wealth of examples of countries giving their data privacy laws extraterritorial application. When combined, these laws create a complex, and partly inconsistent, regulatory matrix which even the best equipped Internet actors struggle to navigate. It is then no surprise that the average Internet user is quite simply unable to get a clear idea of the legal landscape in which they operate.

To get an idea of the magnitude of the problem, we need only consider the mundane situation of a person making a posting on Facebook – a social media platform with around 1.3 billion registered users. So let us assume that you post something on your Facebook site. In most instances, it seems beyond intelligent dispute that you will have to take account of the guidance provided by the law of the country you are in at the time you make the posting. But that is, of course, not the end of the matter. You may also need to consider the guidance provided by the law of the country in which you are habitually residing and the law of your country of citizenship, in case you make the posting outside those countries. We are here already talking of three, potentially very different, legal systems supplying guidance. If your posting relates to another person, you may also need to consider the laws of that person’s location,

¹ This is also noted in UNESCO’s *Global Survey on Internet Privacy and Freedom of Expression* (2012), at 95.

residence, domicile and citizenship. But then, under the law of many, not to say most, countries, focus may be placed on where content is read. This means that you will also need to take account of the laws of all the countries in which your Facebook 'friends' are found and, less predictably, the laws of all the countries in which your Facebook friends may be located when reading your posting, as well as the laws of all the countries in which re-posted versions of your posting may be read. It goes without saying that the number of additional legal systems to be considered grows with the number, and geographical diversity, of your Facebook friends and, in light of the mobility of people, may never be fully ascertained at the time of posting. As if this was not complicated enough, we must also bear in mind that content placed on Facebook will be stored in 'the cloud', and while we as users may not necessarily be able to find out where our content is stored, we may be legally obligated to consider the laws of the country in which the content is stored. Finally, content posted on Facebook may, depending on both your Facebook settings and on how Facebook treats those settings, be available to third-parties, and you may then need to also let the laws of the locations of those third-parties guide your conduct. This legal situation of extraordinary complexity is what 1.32 billion Facebook users expose themselves to on a daily basis. And of course, a similar reasoning could be applied to users of other social media platforms such as LinkedIn with its 300 million users and Google+ with its 1.15 billion registered users.

This takes us to three issues that ought to fall squarely within UNESCO's mandate:

- (1) How are people supposed to access the law of all the foreign legal systems to which they are exposed?
- (2) How are people supposed to *understand* the law of all the foreign legal systems to which they are exposed?
- (3) How are people supposed to deal with contradictions between the laws of all the foreign legal systems to which they are exposed?

All three of these issues substantially undermine the legitimacy of extraterritorial claims – a country that does not make its laws available in an accessible and understandable manner must realise that there is little prospect that people will be able to abide by those laws. In fact, the well established principle that 'ignorance of the law is no defence' may legitimately be called into question where the laws to which people are exposed are not accessible in an understandable form. Much work is needed when it comes to making laws accessible and understandable, and UNESCO (perhaps with appropriate partnerships) may be able to play an important role on these two issues.

As to the third issue – contradictions between the laws of the foreign legal systems to which individuals are exposed – the reality is that, in the absence of harmonised jurisdictional rules, it falls to the individuals to decide which of the conflicting laws to abide by and which laws to ignore. Such a decision, where it cannot be avoided,

should most appropriately be guided by ethical considerations. Identifying how various ethical considerations ought to be balanced so as to adequately cater for the competing interest may be a task eminently well suited for UNESCO given UNESCO's role to "define the ethical values intended to inspire the future information society so that it may be democratic both for all those living today and for future generations".² To avoid any confusion, I hasten to add that such work is no substitute for work towards what we can call *jurisdictional interoperability*, identifying and ironing out legal differences (in both procedural and substantive law) that create barriers for cross-border interaction and, ultimately, an international agreement. Rather, in the climate we are in, work should proceed in all these fields, and UNESCO can play an important part in all aspects of this work.

4. A trend of courts requiring global blocking

There is a trend of courts requiring global blocking where they find content unlawful under their laws. This trend is particularly worrying in relation to actions taken against Internet intermediaries such as search engines and social media platforms. Orders requiring global blocking may represent an interference with the availability of content in other countries, content that may be perfectly lawful there. Further, global blocking in such a situation may be seen as a violation of the creator's freedom of expression: the right to communicate that content in the countries where doing so is lawful.

It is important that we do not overlook these rights just because there may be a duty not to communicate that content in some countries. On numerous occasions, I have discussed this in some detail, and it may be useful to repeat part of that discussion here.

One often sees the adherence to the harshest rules as a proposed solution to the difficulty of variances in legal standards where more than one standard applies to specific conduct. Such suggestions rely on the notion that no conflict exists where a person subject to regulation by two states can comply with the laws of both.

I object to this *duties-focused approach*. Essentially what such claims are suggesting is that we should only focus on the duties imposed by law. If the duties do not conflict, the laws do not conflict. This is too simplistic a perspective. It completely neglects the importance of the rights that laws provide. Importantly, the correlative relationship between rights and duties to which we may be accustomed from a domestic law setting does not necessarily survive when transplanted into a cross-

² Teresa Fuentes-Camacho (Ed.), *The International Dimensions of Cyberspace Law* (UNESCO publishing 2000), at 3.

border environment; that is, rights provided under one country's legal system may not necessarily create corresponding duties under other legal systems.

I argue that in assessing whether two (or more) laws are in conflict we need to take account of both the duties and the rights those laws provide for. In other words, even where the duties do not clash, the rights of one country may clash with the duties of another country.

The difference can be illustrated by way of an example. Imagine that the laws of state A specifically provide for a right of religious freedom, while the laws of state B specifically impose a duty of adherence to Norse pagan faith. Where a person, for one reason or another, finds herself bound to comply with both the laws of state A and those of state B, there is no conflict in the view of the reasoning put forward by Justice Souter and others – such a person can comply with the law of both states by adhering to Norse pagan faith.

In contrast, from the perspective I advocate here, there is a conflict since the right provided by the law of state A cannot be freely exercised while at the same time complying with the duty imposed by the law of state B (except, of course, by those who voluntarily chose to exercise their right to worship Odin, Thor, Freja etc).

In light of all this, I argue that calls for compliance with the strictest rules, as a solution to the problem of conflicting laws, are misguided.

In this context, it is also relevant to consider the practical implications of the fact that most major Internet intermediaries are based in the United States. One thing seems beyond intelligent dispute: the courts that can control Internet intermediaries can, to a great extent, control the accessibility of Internet content. This fact alone taints the issue discussed with interesting geo-political considerations and agendas that may fall within UNESCO's mandate to consider.

In my view, where an Internet intermediary is ordered to block or remove certain Internet content, the default position must be that ordinarily the blocking/removal should be geographically limited rather than having a global reach. Elsewhere, I have proposed the following four broad principles:

Principle 1: *The extent to which a court order in one country should force the blocking/removal of content beyond that country must depend on the type of legal action that produced the relevant court order.*

Principle 2: *Generally, orders requiring global blocking/removal should only be awarded against the party who provided the content, not parties that merely act as intermediaries in relation to that content. And such orders should only be awarded by the courts at the defendant's place of domicile.*

Principle 3: *Exceptions to Principle 2 should be made in relation to particularly serious content such as child pornography materials.*

Principle 4: *In relation to rights limited to the territory of a specific country, whether based on registration or not, courts should not order blocking/removal beyond that country.*

These principles do obviously only cover a selection of issues, and are merely meant as a starting point for further discussion.

5. A trend of ‘market destroying measures’

I suspect we are currently witnessing a paradigmatic change in how states seek to regulate Internet activities. Having seen the difficulties of extraterritorial enforcement, states are moving towards what I elsewhere have referred to as *domestic enforcement of extraterritorial claims* – they are taking what we can call *market destroying measures* to force foreign Internet actors to comply with their laws. For example, in 2013, a Brazilian court threatened to block Facebook in Brazil unless Facebook complied with the Court’s judgment. I think this approach has certain merits (e.g. it does not interfere with content globally) and have suggested that it may be used as the foundation for a doctrine of *market sovereignty*.

If we wish to point to drivers of the trend towards a use of market destroying measures, the following may be strong candidates:

- (1) States are well aware of the difficulties of extraterritorial enforcement;
- (2) There is a cyclical trend oscillating between over-regulation and under-regulation, and we are now heading back into a period of over-regulation;
- (3) There is an increase in nationalism;
- (4) There is a decrease in trust between states following the so-called Snowden revelations; and
- (5) With globalisation in a sense downplaying the significance of geography, we may be seeing a shift in the thinking that underpins jurisdictional claims going from a territorial, map-based, thinking to a thinking based on possession and control.

In light of this, I suspect this development is perfectly natural, if not unavoidable. However, unless it is carefully monitored and managed, it has great potential to cause tensions in international relations. Consequently, I suggest this as an additional area for further work by UNESCO.

These submissions draw upon several publications including the following:

Books

Dan Svantesson, *Extraterritoriality in Data Privacy Law*, Ex Tuto Publishing (November 2013)

Dan Svantesson, *Private International Law and the Internet 2nd Ed.*, Kluwer Law International (January 2012)

Journal articles

Dan Svantesson, A Jurisprudential Justification for Extraterritoriality in (Private) International Law (August 4, 2014). *Forthcoming Santa Clara Journal of International Law* (Volume 13 (2015), Issue 1). Available at SSRN: <http://ssrn.com/abstract=2475760>

Dan 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) <http://script-ed.org/?p=1539>

Dan Svantesson, 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

Dan Svantesson, 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

Dan Svantesson, Celebrating 20 years of WWW – a reflection on the concept of jurisdiction, *Masaryk University Journal of Law and Technology*, Vol. 6 No. 1 (2012); pp. 177-190.

Blog posts

Dan Svantesson, *Bite v. Bark Jurisdiction – More Nuances to Internet Jurisdiction* (5 August 2014) <http://blawblaw.se/2014/08/bite-v-bark-jurisdiction-%e2%80%93-more-nuances-to-internet-jurisdiction/>

Dan Svantesson, *Do we need an international law doctrine of selective legal compliance to protect Internet intermediaries?* (3 June 2014) <http://blawblaw.se/2014/06/do-we-need-an-international-law-doctrine-of-selective-legal-compliance-to-protect-internet-intermediaries/>

Dan Svantesson, *A doctrine of 'market sovereignty' to solve international law issues on the Internet?* (5 April, 2014) <http://blog.oup.com/2014/04/market-sovereignty-international-law-internet/>

Dan Svantesson, *Ignorance or arrogance – A US court claims the right to regulate the Internet world-wide* (3 April, 2014) <http://blawblaw.se/2014/04/ignorance-or-arrogance-%e2%80%93-a-us-court-claims-the-right-to-regulate-the-internet-world-wide/>

Dan Svantesson, *The territorial scope of the proposed EU Data Protection Regulation* (24 March 2013) <http://blawblaw.se/2013/03/the-territorial-scope-of-the-proposed-eu-data-protection-regulation/>