Are we Stuck in an Era of Jurisdictional Hyper-Regulation?*

Dan Jerker B. Svantesson

---

* This contribution draws, and expands, upon research findings discussed in: Svantesson, D., *Solving the Internet Jurisdiction Puzzle*, Oxford 2017; Polcak, R. and Svantesson, D., *Information Sovereignty – Data Privacy, Sovereign Powers and the Rule of Law*, Cheltenham 2017; Svantesson, D., *Celebrating 20 years of WWW – a reflection on the concept of jurisdiction*, Masaryk University Journal of Law and Technology 2012, pp. 177-190; Svantesson, D., *Rättens internationalisering genom digitalisering*, in Cecilia Magnusson Sjöberg (ed.), Rättsinformatik: Juridiken i det digitala informationssamhället, Studentlitteratur 2015, pp. 29-54 (reworked for 2nd Ed. 2016, pp. 31-56); Svantesson, D., *The holy trinity of legal fictions undermining the application of law to the global Internet*, International Journal of Law and Information Technology 2015, pp. 219-234; Svantesson, D., *Nostradamus Lite - Selected Speculations as to the Future of Internet Jurisdiction*, Masaryk University Journal of Law and Technology 2016, pp. 47-72; Svantesson, D., *Give (cyber) peace a chance: The risks of cyber warfare just got more dangerous, and we hardly even noticed*, 11 September 2017, "/www.policyforum.net/give-cyber-peace-a-chance/".

1 Introduction

Elsewhere, I have sought to bring attention to the fact that we are now in what may be described as an era of hyper-regulation online; that is, even our most mundane online activities expose us to (1) the risk of being brought before the courts in an overwhelming number of jurisdictions, and (2) the laws of an equally overwhelming number of jurisdictions.

In this contribution, I will describe why this is so. I will also attempt to provide suggestions for some steps we may take to minimise the negative consequences of this, or even to move away from hyper-regulation.

But first, I will provide a brief description of how we arrived at this stage, and I will try to define exactly what I mean by hyper-regulation (something that should have been done already quite some time ago).

2 The Path to Hyper-Regulation

While the regulatory world one enters when 'going' online has always been complex and associated with uncertainties, we have not always been in an era of hyper-regulation. Instead, a study of approaches to Internet jurisdiction over time hint at a pendular movement between over-regulation and under-regulation.

If we allow ourselves a degree of simplification, and using 1991[1] as a starting point, I have suggested that we, to-date, can point to four rather distinct stages or phases. The first such phase (1991-1999) was characterised by under-regulation and can perhaps be seen as the 'Wild West' era. During this era, there were significant calls for states to refrain from making jurisdictional claims over the Internet and Internet-related activities, and the U.S. government was leading the way with 'self- regulation' for the so- called 'information superhighway'. John Perry Barlow's famous, often repeated—and indeed ground-breaking—'Declaration of the Independence of Cyberspace'[2] was setting the tone, and the most striking characteristic of the academic discourse, at the time, is its openness to debating even the fundamentals. There was creativity and a willingness, indeed eagerness, to find innovative solutions.

This 'hands-off' attitude was, at least partially, reflected in attitudes towards jurisdictional claims online. Looking back at the decisions from this time—especially amongst some important U.S. courts— one almost gets the feeling of there being a 'race' to be the first to find the solution to the Internet jurisdiction conundrum.[3] Unfortunately, comparatively speaking, there is precious little of

1 In 1991, CERN researcher Tim Berners-Lee developed the World Wide Web (WWW).

2 Barlow, J.P., *A Declaration of the Independence of Cyberspace*, 8 February 1996, "www.eff.org/cyberspace-independence".

3 For more details on some of the seminal cases, refer e.g. to the excellent study on the topic by the Fordham Center on Law and Information Policy (Reidenberg, J.R. et al, *Internet Jurisdiction: A Survey of Legal Scholarship Published in English and United States Case Law*, Fordham Law Legal Studies Research Paper No 2309526 30 June 2013, "papers.ssrn.com/sol3/papers.cfm?abstract_id=2309526", p. 55.

this entrepreneurial spirit left in the court decisions (and indeed the academic literature) of today.

The second phase (2000-2009) saw courts and legislators display a much more aggressive attitude as to when they could claim jurisdiction over Internet conduct. Put simply, their attitude was that their jurisdictional powers extended to any Internet conduct that impacted, or had the potential to impact, on their territory or citizens. The High Court of Australia's December 2002 Internet defamation decision in the *Gutnick* case is characteristic as well as illustrative of the thinking of the time:

> However broad may be the reach of any particular means of communication, those who make information accessible by a particular method do so knowing of the reach that their information may have. In particular, those who post information on the World Wide Web do so knowing that the information they make available is available to all and sundry without any geographic restriction.[4]

Under this reasoning, those brave enough to do so enter the online environment at their own risk as far as Internet jurisdiction is concerned. One of the more obvious flaws with this reasoning is that it is based on the assumption that an online presence necessitates an (objective) intention to reach the world at large. The *Gutnick* case is also illustrative of a judicial hesitation to treat the Internet as something novel. In a now classic statement, one of the judges on the High Court – Callinan J – expressed the view that '[t]he Internet, which is no more than a means of communication by a set of interconnected computers, was described, not very convincingly, as a communications system entirely different from pre-existing technology.'[5]

The third phase (2010-2014) saw courts and legislators around the world seemingly having started to accept, to a degree, the impossibility of viewing an online presence as an indication of an intention to do business with the world at large. But perhaps they went a bit too far, and I have described this third phase as characterised by a degree of under-regulation.

We find an example of this in the targeting approach as applied by the Advocate General and the Court in *Pammer*/*Hotel Alpenhof*.[6] Both direct their focus on the subjective intentions of the relevant party, and both the Advocate General and the European Court of Justice (as it then was) seem to have taken the view that the phrase 'directs such activities' implies a conscious decision executed without mistakes. For example, the Advocate General states: 'It is therefore essential for there to be active conduct on the part of the undertaking,

4 *Dow Jones & Company Inc. v. Gutnick* (2002) 210 C.L.R. 575, at 605.

5 *Dow Jones & Company Inc. v. Gutnick* [2002] H.C.A. 56 [180].

6 Advocate General Trstenjak, *Opinion of Advocate General Trstenjak delivered on 18 May, Case C-585/08* Peter Pammer v. Reederei Karl Schlüter GmbH & Co. KG *and Case C-144/09* Hotel Alpenhof GesmbH v. Oliver Heller 2010.

the *objective and outcome* of which is to win customers from other Member States.'[7] Such an approach is limiting indeed.

It is also noteworthy that, during this period, we began to see an increase in technology-specific, as opposed to technology-neutral, lawmaking. The most famous example can be found in the Court of Justice of the European Union's (CJEU) decision in the joined cases of *eDate Advertising GmbH v. X* and *Olivier Martinez, Robert Martinez v. MGN Ltd.*,[8] where the Court dealt with online publications differently to offline publications. However, other examples unquestionably can also be found.

As I see it, we are now in the fourth phase (2015 - present). This is the phase of hyper-regulation, and I have, on many occasions, used the same example to illustrate what this involves;[9] that is, what laws do you need to consider when posting something on social media?

In most instances, it seems beyond intelligent dispute that you will have to take account of the law of the state you are in at the time you make the posting. However, that is, of course, not the end of the matter. You may also need to consider the law of the state in which you are habitually residing (and/or domicile) and the law of your state of citizenship. Then you will probably also need to consider U.S. law, as most major social media platforms are based in the U.S. I am already talking of a few, potentially very different, legal systems supplying laws with which you are meant to comply.

If your posting relates to another person, you may also need to consider the laws of that person's location, residence, domicile and citizenship. You may also need to consider the laws of any additional state in which that person has a reputation to protect.

But then, under the law of many (not to say most) states, focus may be placed on where content is downloaded or read. This means that you will also need to take account of the laws of all the states in which your Facebook 'friends' or LinkedIn 'connections' are found—and less predictably, the laws of all the states in which they may be located when reading your posting. It goes without saying that the number of additional legal systems to be considered grows with the number, and geographical diversity, of your friends or connections, and in the light of the mobility of people, may never be fully ascertained at the time of posting.

Then things get rather messy. Given that your postings may be re-posted, you also need to take account of the laws of all the states in which re- posted versions of your posting may be downloaded or read. Here the original poster obviously loses all possibility of predicting the scope of laws to which she or he may be exposed.

---

7 Advocate General Trstenjak 2010, *Opinion of Advocate General Trstenjak delivered on 18 May*, [63] (emphasis added).

8 Cases C- 509/09 eDate Advertising GmbH v. X and C- 161/10 Olivier Martinez and Robert Martinez v. MGN Limited.

9 *See* e.g. Rättens, D., *Internationalisering genom digitalisering*, in Cecilia Magnusson Sjöberg (ed.), Rättsinformatik: Juridiken i det digitala informationssamhället, Student-litteratur 2015, pp. 29-54 (reworked for 2nd Ed. 2016, pp. 31-56).

As if this was not complicated enough, we must also bear in mind that content placed on social media platforms is often 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 state in which it is stored. Finally, content posted may, depending on both your settings and on how your social media platform treats those settings, be available to third parties and you may then need also to let the laws of the locations of those third parties guide your conduct.

3 What is Hyper-Regulation?

While I have, for some time now, argued that we are in a stage of hyper-regulation, I have not at any point sought to clearly define what I mean by hyper-regulation. While the example above gives an illustration of what is involved, I will seek to remedy this carelessness here. After all, defining what is hyper-regulation is most likely as important as mapping out how it currently is displayed in the online environment.

3.1 What do I Mean by 'Regulation'?

There is a wealth of literature about what 'regulation' is both in the field of information technology law and more generally. However, in our field, no regulation discussion has had a greater impact than Lessig's (now classic) observation as to the four regulatory forces (law, code, market and norms). Given that the majority of readers of this publication would be familiar with Lessig's important work, I will not explore this in detail. It is sufficient to note that Lessig's reasoning has guided and indeed dominated much thinking on Internet governance.

To this may be added in passing that Bygrave convincingly illustrates that Lessig's classic description of the four regulatory forces clearly fails to account for the distinctive role of contracts.[10] This is particularly significant since contracts often have a more direct impact on our lives than does legislation. This topic will, however, not be pursued further here.

At any rate, I do not dispute the significance and relevance of Lessig's four regulatory forces combined with Bygrave's observation. However, at least for now, I will focus only on legal regulation when I discuss hyper-regulation. In other words, while I acknowledge that our online conduct is regulated by various forces, it is only the legal regulation I currently see as contributing towards hyper-regulation as I define it. In the light of this, purists may prefer to read my reference to hyper-regulation as shorthand for *legal* hyper-regulation.

10 *See* further, Bygrave, L.A., *Internet Governance by Contract*, Oxford 2015, pp. 4–5.

3.2 The Concept of a 'Contextual Legal System'

The concept of a contextual legal system is an important component in defining hyper-regulation. If we revisit the social media example I used above to illustrate what I mean by hyper-regulation, it is clear that Internet users are exposed to a complex matrix of legal systems. Thus, to speak of their legal system in a meaningful manner, I have suggested that we need to introduce the concept of a 'contextual legal system', by which I refer to the system of legal rules from all sources that purport to apply to the conduct of the person in question in the setting in which he or she is acting.[11]

When we choose to drive over the speed limit, our contextual legal system is typically that of the country in which we are driving; if we, in country A, post a letter to someone in country B defaming someone in country C, the contextual legal system may be made up of the relevant aspects of the laws of at least countries A, B and C.

Where this reasoning is accepted, it is clear that the contextual legal system Internet users face is made up of parts of the laws of many different countries. It should therefore surprise no one that our contextual legal system in a situation such as the social media example will typically contain legal rules overlapping and clashing with other legal rules. Indeed, in such a contextual legal system, we are likely to see instances of legal rules directly contradicting each other, leaving the Internet user with the perilous exercise of selecting which law to comply with and which to ignore.

3.3 A Potential Definition

Drawing upon the above, we may define hyper-regulation, or perhaps more accurately legal hyper-regulation or even jurisdictional hyper-regulation, as involving a situation where: (1) the complexity of a party's contextual legal system amounts to an unsurmountable obstacle to legal compliance, and (2) the risk of legal enforcement of—at least parts of—the laws that make up the contextual legal system is more than a theoretical possibility.

I hasten to acknowledge that with this definition, we are likely to remain in an era of hyper-regulation for quite some time.

3.4 The 'Double Passive-Active Matrix'

Given the definition of hyper-regulation above, the suggestion that we can have varying degrees of hyper-regulation seems beyond intelligent dispute. And I dare say that there may be a variety of manners in which we may seek to measure the degree of hyper-regulation in any given situation. Here, I will limit myself to outlining one possible method for doing so and for measuring the extent to which

11 Svantesson, D., *The Holy Trinity of Legal Fictions Undermining the Application of Law to the Global Internet,* Intl JL & Info Tech 2015, pp. 219–234.

a particular legislative initiative contributes towards hyper-regulation, through what we may refer to as a 'double passive-active matrix'.

The first thing we consider in a 'double passive-active matrix' is the ease with which a country's laws become part of a person's contextual legal system. Obviously, the situation is less serious where a person will only be caught by a particular country's laws where she actively engages with that country on an ongoing basis, compared to situations where a person is caught by a particular country's laws where she merely has a passive online presence, or an online presence that only occasionally engages with the country in question.

The second aspect taken into account in the 'double passive-active matrix' is what the law that forms part of a person's contextual legal system actually demands from that person whether the person is aware of it or not. Where the law merely demands that the person passively steers clear of activities that predictably will contravene laws, the situation stemming from a potential lacking knowledge of the applicability of that law is less serious than it is where the law in question requires active steps, especially where those steps are not necessarily predictable.

The discussion so far can usefully be illustrated in a matrix:

	Law merely requiring passively avoiding illegal acts	Law requiring active steps for legal compliance
Law activated merely by passive online presence	Medium level of hyper-regulation	High level of hyper-regulation
Law activated only by active contact with the country in question	Low level of hyper-regulation	Medium level of hyper-regulation

Alternatively, we may say that, while it is possible to draw a sharp line between laws requiring active steps for legal compliance, on the one hand, and laws merely requiring passively avoiding illegal acts, on the other hand, no such sharp line may be drawn between laws activated only be active contact with the country in question compared to laws activated merely by passive online presence. Rather than being binary, the level of activity required as far as the person's contact with a certain country is concerned may be viewed as better expressed as a scale, for example:

	Law merely requiring passively avoiding illegal acts	Law requiring active steps for legal compliance
Law activated merely by passive online presence	Very high level of hyper-regulation	Extreme level of hyper-regulation
Low degree of contact sufficient to activate law	High level of hyper-regulation	Very high level of hyper-regulation
Medium degree of contact required to activate law	Medium level of hyper-regulation	High level of hyper-regulation
High degree of contact required to activate law	Low level of hyper-regulation	Medium level of hyper-regulation
Law activated only be active, substantial and on-going contact with the country in question	Very low level of hyper-regulation	Low level of hyper-regulation

To illustrate how the 'double passive-active matrix' may be utilised to assess the impact a particular piece of legislation may have on the degree of hyper-regulation, we may, for example, consider the most hotly discussed legislative initiative (at the time of writing): the European Union's General Data Protection Regulation (GDPR).

Article 3 of the GDPR determines the GDPR's 'territorial scope', or more correctly, it outlines what types of contact with the EU's territory will activate the application of the GDPR, and it does so in a manner that is partly territoriality-dependent and partly territoriality-independent. At any rate, it reads as follows:

> 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
>
> 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
>
> (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
>
> (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.
>
> 3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

I have analysed this provision in detail in a forthcoming *Commentary* edited by Christopher Kuner, Lee A. Bygrave, and Christopher Docksey and published by

Oxford University Press.[12] Here, it suffices to note that, while it would be unfair to describe the GDPR as a law activated merely by a passive online presence, there can be no doubt that – as drafted (we are still to see how Article 3 is applied) – Article 3 places the GDPR in the category of laws activated already at a low degree of contact.

Having identified where we would find the GDPR on the scale of degree of contact required to active the law, we can turn to examining the type of obligations to which the GDPR gives rise; that is, is the GDPR to be classed as a law requiring active steps for legal compliance, or rather as a law merely requiring persons to passively avoid illegal acts? This question need not detain us for long. The answer is that the GDPR – as do many other data privacy instruments – contains both provisions requiring active steps for legal compliance, and provisions merely requiring passive avoidance of illegal acts. And in such a situation, we must obviously primarily focus on the fact that at least some provisions do require active steps for legal compliance.

In the light of this, the conclusion is that – due to the combination of being a law activated already at a low degree of contact and being a law that includes provisions requiring active steps for legal compliance – the GDPR is contributing to a very high level of hyper-regulation.

4 The Current Online Landscape of Hyper-Regulation

The above has already provided an example of hyper-regulation, a definition of hyper-regulation and a tool for analysing the extent to which particular legislative initiatives contribute to a climate of hyper-regulation. However, I want to at least dedicate a couple more paragraphs to the current landscape of how hyper-regulation manifests itself.

4.1 Excessively Broad Jurisdictional Claim

The most obvious source of hyper-regulation is of course excessively broad, indeed crude,[13] jurisdictional claims such as that of the GDPR. This, I would argue, is clearly a longstanding attitude problem that can be seen, to varying degrees, throughout all the four phases I outlined above. Consider, for example, the statement by the Advocate-General's office of Minnesota in the mid-90s that '[p]ersons outside of Minnesota who transmit information via the Internet

12 Kuner, C., Bygrave, L.A. and Docksey C. (eds), *Commentary on the EU General Data Protection Regulation*, 2018, "global.oup.com/academic/product/commentary-on-the-eu-general-data-protection-regulation-9780198826491?cc=au&lang=en&".

13 Svantesson, D., *A 'layered approach' to the extraterritoriality of data privacy laws*, International Data Privacy Law 2013, pp. 278-286.

knowing that information will be disseminated in Minnesota are subject to jurisdiction in Minnesota courts for violations of state criminal and civil laws'.[14] We quite simply must get smarter in how we delineate our jurisdictional claims. Only then do we stand a chance to overcome hyper-regulation.

4.2 Scope of (Remedial) Jurisdiction

In addition to the standard jurisdictional issues normally brought into focus, it is clear that a major arena for hyper-regulation is in relation to what we may refer to as scope of jurisdiction, or scope of (remedial) jurisdiction. Scope of jurisdiction relates to the appropriate geographical scope of orders rendered by a court that has personal jurisdiction and subject-matter jurisdiction. This question has gained far less attention to date than have other jurisdictional issues. Yet, while this third dimension often is overlooked, clear examples can be found of its articulation. One such example is found in the following quote from the CJEU's *eDate* decision, commenting on the EU's Brussels Regulation's approach to jurisdiction in torts cases:

> Article 5(3) of the Regulation must be interpreted as meaning that, in the event of an alleged infringement of personality rights by means of content placed online on an internet website, the person who considers that his rights have been infringed has the option of bringing an action for liability, in respect of all the damage caused, either before the courts of the Member State in which the publisher of that content is established or before the courts of the Member State in which the centre of his interests is based. That person may also, instead of an action for liability in respect of all the damage caused, bring his action before the courts of each Member State in the territory of which content placed online is or has been accessible. Those courts have jurisdiction only in respect of the damage caused in the territory of the Member State of the court seised.[15]

This statement outlines rules of personal jurisdiction in stating e.g. that an action can be taken 'before the courts of the Member State in which the publisher of that content is established or before the courts of the Member State in which the centre of his interests is based'. But it also delineates the scope of jurisdiction. For example, it makes clear that, if you sue at the defendant's place of establishment or where you have your centre of interests, the relevant scope of jurisdiction is global, while if you sue in a different country, the relevant scope of jurisdiction is just that member state.

There can be no doubt that the question of the scope of jurisdiction is becoming increasingly important, not least as we see more and more litigation aimed at Internet intermediaries such as search engines, social media operators

14 Memorandum of Minnesota Attorney General as found in: Jew, B., *Cyber Jurisdiction – Emerging Issues & Conflict of Law when Overseas Courts Challenge your Web*, Computers & Law, Dec. 1998, p. 23.

15 Cases C- 509/ 09 *eDate Advertising GmbH v. X* and C- 161/ 10 *Olivier Martinez and Robert Martinez v. MGN Limited*, para 69.

and video hosting platforms. The reason is obvious: such intermediaries allow us to 'kill a mosquito with a nuclear bomb' – we can achieve global removal of content based on that content being contrary to the law of one single state.

There are more and more examples of courts ordering Internet intermediaries to block/remove/delist content globally in response to the content arguably violating local law. These are clearly matters of scope of jurisdiction, and given that there are strong reasons to think that these types of questions will only grow in prominence, it is time we recognise the distinct issues involved in this third dimension of jurisdiction.[16] And we obviously need to consider scope of jurisdiction in any attempt at addressing hyper-regulation.

4.3 Unclear International Law (Anchored in Territoriality)

Reading the standard texts on international law, you would be forgiven for coming to believe that we are blessed with a flawless, clear and completely logical system of international law rules governing jurisdiction. The truth, I would venture to say, is quite the opposite. As far as jurisdiction is concerned, and in particularly as to how we apply jurisdictional rules online, international law is a messy rabbit warren populated by inconsistency and lacking logic. To see that this is so, we need only consider the question of how assertions such as the following statement made by the Permanent Court of Arbitration in the *Island of Palmas* case—'Territorial sovereignty […] involves the exclusive right to display the activities of a State'[17]—possibly is reconcilable with the effects doctrine and the passive personality principle. It seems to me that international law – and even more so commentaries on international law – is replete with absolutist statements that are better suited for the political arena than they are for law—statements that then can be (ab)used in the pursuit of particular positions in legal discussions.

A key issue is the extent to which the territoriality principle dominates our thinking on jurisdiction. Put simply, territoriality seems largely to be viewed as the true jurisprudential basis for jurisdictional claims— a state has the exclusive right to regulate all that occurs in its territory for the simple reason that it occurs in its territory.

However, territoriality, as a foundation for jurisdictional claims, aims to fill two functions—and it fails at both. It is meant to articulate delineations as to how far jurisdiction legitimately may reach, but time and time again we see examples where territoriality fails to prevent jurisdictional overreach. As the other side of the proverbial coin, territoriality is also meant to work as a warning light that indicates when a jurisdictional claim reaches too far, thus preventing illegitimate interference with other countries' jurisdictions. The scepticism about territoriality expressed here is, of course, not unique. Since the mid-1990s, at least, we have been quite broadly agreeing that territoriality does not work very

16 *See* further: Svantesson, D., *Jurisdiction in 3D – 'scope of (remedial) jurisdiction' as a third dimension of jurisdiction*, Journal of Private International Law 2016, pp. 60-76.

17 Island of Palmas (*Neth. v. U.S.*), 2 R.I.A.A 829, 838 (Perm. Ct. Arb. 1928).

well for the Internet context. The typical challenges are that online it is very difficult to point to the location of an activity and to where data is stored.

We have also probably moved past that now as we start realising there is another problem associated with territoriality's location focus: it is very easy to manipulate locations online. To this we can add that territoriality, with the way the Internet works, might divert the focus to several locations when we are trying to find one spot on which we want to focus for some applicable law or as to jurisdiction.

Until we make progress in the sense of (1) moving away from territoriality being seen as the jurisprudential foundation of jurisdiction towards a better regime, and (2) getting greater logical consistency in how international law approaches jurisdiction, we are unlikely to make much progress in a fight against hyper-regulation.

4.4 Lacking Willingness to Coordinate and Cooperate

Since 2004, negotiations have been taking place within the United Nations aimed at developing an agreement regarding how international law applies to cyberwarfare. The work was carried out within the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE). GGE consists of representatives from 25 countries, including from the five permanent UN Security Council Member States.

However, on 23 June 2017, the work of the GGE came to a disappointing end. Reportedly, several matters were in contention, including the right to respond to internationally wrongful acts, the right to self-defence under Article 51 of the UN Charter, the potential applicability of international humanitarian law to the information and communications technology context and a perceived lack of focus on cooperation as a solution to potential disputes.

Neither the GGE negotiations nor their collapse have managed to attract much reaction in the media. However, the collapse is bad news and should have us very worried indeed. The collapse of the GGE negotiations does not change the fact that urgent action is required on this topic. Consequently, it is possible that the UN will manage to reconfigure its work resulting in a new working group structure carrying on the work. Should this not happen, however, other international bodies need to step forward and provide a structure for further dialogue.

At any rate, the events surrounding the GGE negotiations and their ultimate collapse are illustrative of the difficulty in getting international consensus enabling the coordination and cooperation needed to overcome hyper-regulation.

4.5 Increasing Value Clashes

Given the very nature of Internet communications, it has always been the case that such communications may result in clashes of values. Perhaps the most well-known such clash can be seen in the transatlantic dispute in the *Yahoo!* case.[18] Put in the fewest of words, there French concerns regarding the auctioning of Nazi materials clashed with U.S. conceptions of freedom of speech.

When a French court ruled that Yahoo must take steps to prevent French Internet users from accessing the sections of the auction site containing Nazi memorabilia,[19] Yahoo turned to a U.S. court seeking a summary judgment to the effect that U.S. courts would not enforce the French decision. While acknowledging France's right to make law for France, Justice Fogel decided in Yahoo's favour, granting the summary judgment, declaring that the 'First Amendment precludes enforcement within the United States of a French order intended to regulate the content of its speech over the Internet'.[20] It is submitted that it might not be unreasonable for a French court to exercise jurisdiction over an act violating French law in France, and it might not be unreasonable for a U.S. court to refuse to recognise and enforce a foreign judgment infringing a U.S. company's freedom of speech as protected by the U.S. Constitution, in relation to an act done by that company exclusively in the U.S. – herein lies one of the greatest normative challenges, a challenge that is most recently showcased in the aftermath of the *Google Canada* case.[21]

Seeking to predict the future, I suspect that we will see more rather than less of such clashes in the years to come. After all, we are seeing more and more countries becoming serious Internet users –Internet usage is no longer an exclusive Western developed world domain. And at the same time, we are seeing little by way of harmonisation of substantive law in the relevant fields in which we see jurisdictional issues arise.

But even leaving aside the value clashes that we may see as a result of more countries becoming Internet users, in the CJEU's *Safe Harbour* decision of October 2015, we were rather recently reminded of just how big the legal attitude gaps are also between relatively similar countries.[22]

These value clashes can be addressed in a number of ways, most of which are seriously damaging. For example, we could start searching for the lowest common denominator, but such a race to the strictest laws would seriously harm the Internet's usefulness. Alternatively, we could fragment the Internet into smaller components such as national Internets accessible only within defined

---

18 *Ligue contre le racisme et l'antisémitisme et Union des étudiants juifs de France c. Yahoo! Inc. et Société Yahoo! France* and *Yahoo! Inc v. La Ligue Contre Le Racisme et l'Antisemitisme* 433 F.3d 1199 (9th Cir. 2006).

19 *International League Against Racism & Anti-Semitism (LICRA) and the Union of French Jewish Students (UEJF) v. Yahoo! Inc.* High Court of Paris, 20th of November 2000.

20 *Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme*, 169 F.Supp. 2d 1181 (N.D. Cal. 2001), at 22.

21 *Google LLC v. Equustek Solutions Inc.*, 2017 WL 5000834 (N.D. Cal. Nov. 2, 2017).

22 C-362/14 (Schrems).

geographical regions (such as States) each of which would be governed only by the applicable law of that region. However, that would, of course, mean the end of the Internet as we know it. A better solution would naturally be to harmonise all substantive laws. The only problem with such an approach is that it is entirely unrealistic. A slightly more realistic, yet still herculean, task is to create uniform rules, whether through an international agreement or other means, allocating jurisdiction so as to avoid value clashes.

5 How do we get out of the Quagmire of Hyper-Regulation?

So, given the discussion above, the obvious question is how we get out of this quagmire and regain firm ground allowing us to move past the current paradigm of hyper-regulation. In my view, we can move towards solutions by building upon the important insights expressed by Palfrey and Gasser in their seminal 2012 book *Interop: The Promise and Perils of Highly Interconnected Systems*.[23] There, Palfrey and Gasser discuss what they call 'legal interoperability' in terms of 'the process of making legal norms work together across jurisdictions'.[24] In their view, there are three reasons why we need a higher degree of legal and policy interoperability:

> At the most basic level, legal interoperability can reduce the costs associated with doing business across borders. [. . .] More broadly, recent studies suggest that legal interoperability— particularly in the fields of trade and business law— drives innovation and economic growth by making countries more competitive. Finally, increased levels of legal interoperability among multiple jurisdictions can lead to better laws that foster the development of fundamental values and rights, such as information privacy and freedom of expression.[25]

This fits perfectly with the idea of 'jurisdictional interoperability' I first presented in an article in 2015.[26] Rather than vainly hoping for an all-encompassing international agreement overcoming the problems of Internet jurisdiction, we must accept instead that the road ahead will be travelled by many thousands of small steps. Just as the Internet is a successful 'network of networks', the mid- term solution to the issue of hyper-regulation will be found in what we can see as a 'system of legal systems'— a system in which our domestic legal systems operate (relatively) smoothly together with a minimum of inconsistencies and clashes.

---

23 Palfrey, J. and Gasser, U., *Interop: The Promise and Perils of Highly Interconnected Systems*, 2012.

24 Ibid 178.

25 Ibid 178-179.

26 Svantesson, D., *The holy trinity of legal fictions undermining the application of law to the global Internet*, International Journal of Law and Information Technology 2015, pp. 219-234. At the time, I was unfortunately not aware of Palfrey and Gasser's excellent work on the topic.

Importantly, this means that rather than sitting back waiting for a miraculous international agreement addressing all the jurisdictional concerns online, everyone can get involved— law reformers, courts, legislators, lawyers, legal academics, civil society and law students— in identifying uniting features and in chipping away at the inconsistencies, contradictions and clashes that hinder interoperability between the various legal systems that govern our conduct online. Getting such work underway is a matter of urgency, and it may well be the case that aspects of cosmopolitanism may prove to be a useful source of inspiration, or even guidance. That is, however, a topic I will not pursue further here.

To provide a definition of jurisdictional interoperability, we may say that it is achieved where we have: (1) only a minimal level of serious jurisdictional clashes, and (2) an acceptable level of less serious jurisdictional clashes. For these purposes, 'jurisdictional clashes' include both clashes of duties and clashes between rights and duties. In my view, it is this goal we currently should work towards in the context of Internet jurisdiction. In doing so, we will, unsurprisingly, have a better prospect of success in some areas than in others. As a result, we may well end up with what may be referred to as 'sectorial jurisdictional interoperability' in some areas of law. Nevertheless, as I see it, 'jurisdictional interoperability' is the antidote to hyper-regulation.

6 Final Remarks

In the above, I have sought to draw attention to, and explore in some detail, what I see as one of the most important challenges facing the information technology law community. In fact, the risks and complications I have alluded to in this contribution represent one of the greatest challenges we face in the pursuit of a positive online environment benefitting humanity at large.

Having said all this, the undeniably most important factor in addressing hyper-regulation is the continued effort to increase the understanding of these issues by the next generation of lawyers. In this context, due credit should be given to the work done at Stockholm University in incorporating legal informatics and IT law into the standard law degree, as well as to the work done on the now abandoned Master of Laws programme on IT law. It is that type of initiatives that will ensure that the next generation of lawyers are better equipped to tackle the issues associated with Internet jurisdiction than we have been.