CELEBRATING 20 YEARS OF WWW – A REFLECTION ON THE CONCEPT OF JURISDICTION

by

DAN JERKER B. SVANTESSON*

The concept of jurisdiction has a relatively long history. However, being a core concept affecting every single Internet user, its most appropriate application in the Internet era has been the subject of much debate.

In the 90’s there were significant calls for states to make no jurisdictional claims in relation to Internet-related activities. A competing view was that too many forms of Internet conduct would fall outside the jurisdictional scope of all states, leaving a regulatory vacuum.

As the Internet, and the discussion of Internet regulation, has matured, it now – 20 years after the birth of the World Wide Web – seems clear that rather than there being no regulation, or under-regulation, the Internet is overregulated in that conduct on the global Internet may come under the jurisdiction of virtually all states in the world. At the same time, there is a recent trend of courts showing reluctance to claim jurisdiction as broadly as they arguably can do under applicable law.

This paper discusses, and analyses, a selection of approaches to the concept of jurisdiction. In doing so, account is taken of both public international law and private international law.

KEYWORDS
Jurisdiction, Private International Law, Conflict of Laws, Internet Regulation

* Associate Professor, Faculty of Law Bond University, Gold Coast Queensland 4229 Australia, Ph: +61 7 5595 1418, (www.svantesson.org). Researcher, Swedish Law & Informatics Research Institute, Stockholm University (Sweden). Dan_Svantesson@bond.edu.au
1. INTRODUCTION

In 1991, CERN researcher Tim Berners-Lee developed the World Wide Web (WWW). That means that, at the time of writing, the WWW – the key characteristic of the modern Internet – turned 20 this year. This is undoubtedly a cause for celebration. It is also an interesting point in time to pause to consider what developments have occurred during these 20 years. This paper does so with a focus on how the concept of jurisdiction, as applied to the Internet, has developed over the lifespan of the WWW.

The concept of jurisdiction has a relatively long history, obviously predating both the WWW and the Internet as such. However, not least due to the impact extraterritorial jurisdictional claims may have on international relations, it has proven to be a fruitful source of controversy and debate. Or more accurately, there has always been controversy associated with the question of when a court may claim jurisdiction over a particular matter or person. Being a core concept affecting every single Internet user, its most appropriate application in the Internet era has, as can be expected, been the subject of much debate.

In the 90’s there were significant calls for states to refrain from making jurisdictional claims over the Internet and Internet-related activities. A competing view soon developed that, too many forms of Internet conduct fell outside the jurisdictional scope of all states, leaving a regulatory vacuum; a vacuum that needed to be filled.

As the Internet, and the discussion of Internet regulation, has matured, it now – 20 years after the birth of the World Wide Web – seems clear that rather than there being no regulation, or under-regulation, the Internet is overregulated in that conduct on the global Internet may come under the jurisdiction of virtually all states in the world. At the same time, there is a recent trend of courts showing reluctance to claim jurisdiction as broadly as they arguably can, and perhaps ought to, do under applicable law.

This paper discusses, and analyses, a selection of approaches to the concept of jurisdiction. In doing so, account is taken of both public international law and private international law.

The paper illustrates that, while the subject-matter does not lend itself to sharp delineations, four different phases can be identified; each with its own characteristics and tendencies. Using the mental picture of a pendu-
lum, these four phases are analysed and some thoughts about future applications of the concept of jurisdiction to Internet conduct are provided.

2. THE FIRST PHASE – TERRA NULLIUS

The early years, about 1991 to 1999, were characterised by hopes and dreams of the WWW-driven Internet as a new frontier, open to everyone and regulated by no one. It was an era of freedom during which the abbreviation WWW might just as well stood for the “Wild Wild Web”. A defining moment took place in 1996 when John Perry Barlow famously unveiled his groundbreaking Declaration of the Independence of Cyberspace:

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather...¹

The somewhat enigmatic quality of this Declaration may make it look amusingly eccentric, or even utterly absurd, today. However, it must be remembered that it was presented to the world at a time when people consciously decided to “go” online and spend time “in” Cyberspace for a set period of time. Our world today is very different to this. Today, we do not go online. Instead our lives, characterised by a continuous Facebook presence, tablets and Internet-connected kitchen appliances, are immersed in the so-called Cyberspace – we are experiencing a conflation of the online and offline world. Thus, it is simply no longer clear where Cyberspace starts and the “real world” ends.

In any case, the relevant time period saw the emergence of one of the most interesting academic “exchanges of ideas” ever in the field of Internet, or Cyberspace, law. I am here referring to the series of articles written by Johnson and Post on the one hand (taking a cyber libertarian point of view), and Jack Goldsmith’s writings on the other hand. In 1996, Johnson and Post wrote an article titled Law And Borders - The Rise of Law in Cyberspace² in which they argued that the Internet should be viewed as a separate ‘space’, beyond the control of individual nations’ regulation. Moreover, the article suggested that, to the extent that this separate space is to be regulated, such

---

³ Johnson and Post, Law And Borders, p. 1378.
regulations would emerge in the form of self-regulation. Johnson and Post’s reasoning is neatly summarised in the following statement:

Treating Cyberspace as a separate ‘space’ to which distinct laws apply should come naturally, because entry into this world of stored online communications occurs through a screen and (usually) a ‘password’ boundary. There is a ‘placeness’ to Cyberspace because the messages accessed there are persistent and accessible to many people. You know when you are ‘there’. No one accidentally strays across the border into Cyberspace. To be sure, Cyberspace is not a homogenous place; groups and activities found at various online locations possess their own unique characteristics and distinctions, and each area will likely develop its own set of distinct rules. But the line that separates online transactions from our dealings in the real world is just as distinct as the physical boundaries between our territorial governments--perhaps more so.

Crossing into Cyberspace is a meaningful act that would make application of a distinct ‘law of Cyberspace’ fair to those who pass over the electronic boundary. (footnotes omitted)

Essentially replying to this article, Goldsmith published Against Cyberanarchy in 1998. In that article he emphasised that:

Cyberspace transactions are no different from ‘real-space’ transnational transactions. They involve people in real space in one jurisdiction communicating with people in real space in other jurisdictions in a way that often does good but sometimes causes harm. There is no general normative argument that supports the immunization of cyberspace activities from territorial regulation. And there is every reason to believe that nations can exercise territorial authority to achieve significant regulatory control over cyberspace transactions.

A few additional shots, such as Post’s Against against cyberanarchy, were fired in this exchange, however none as significant as the opening salvoes mentioned.

In the space available, it would be quite impossible to account in full for this highly interesting debate. However, it can perhaps be said that this ex-

---

4 Johnson and Post, Law And Borders, p. 1367.
5 Johnson and Post, Law And Borders, p. 1379.
change of ideas was the dying phase of a serious movement in favour of courts not claiming jurisdiction over Internet activities.

Staying with the notion of the Internet as a separate “space”, it is worth pointing out that, every now and then, one sees articles expressing the “novel” idea that the Internet is a separate space akin to other international spaces such as the High Seas, Antarctica and Outer Space (i.e. as an independent international space beyond individual nations’ regulation). But in fact, such an idea has not been novel since at least 1998 when Darrel Menthe discussed that option in detail.

These three physical spaces are nothing like cyberspace which is a non-physical space. The physical/non-physical distinction, however, is only one of so many distinctions which could be made between these spaces. After all, one could hardly posit three more dissimilar physicalities – the ocean, a continent, and the sky. What makes them analogous is not any physical similarity, but their international, sovereign quality. These three, like cyberspace, are international spaces.7

Having illustrated how there are currently three international spaces, and that ‘cyberspace’ should be the fourth, Menthe describes how the ‘nationality principle’ has been applied to regulate behaviour in these spaces. In doing so he notes that all three international spaces rely on the nationality principle (e.g. the ‘law of the flag’ from maritime law),8 and makes the point that “[s]imilarly, a webpage would be ascribed the nationality of its creator, and thus not be subject to the law of wherever it happened to be downloaded.”9 In the context of how to determine the nationality of actions taking place in ‘cyberspace’, Menthe also notes that “[a] person who follows a link is simply a downloader, and is subject to the territorial jurisdiction of the keyboard at which he or she sits, as well as the laws governing persons of his or her nationality in cyberspace.”10

As is hinted at in the above, academic discourse on the concept of jurisdiction as applied to the Internet was, during the first phase (1991 – 1999), mainly focused on two matters: (1) to regulate or not to regulate?, and (2) how to regulate? This careful hesitation, and realisation that the Internet is ‘different’, can also be observed in how some courts approached jurisdic-  

---

8 Menthe, Jurisdiction in Cyberspace, p. 83.
9 Menthe, Jurisdiction in Cyberspace, p. 74.
10 Menthe, Jurisdiction in Cyberspace, p. 94.
tional claims over Internet conduct during this phase. For example, in *Macquarie Bank Limited & Anor v Berg* the Supreme Court of New South Wales\(^{11}\) refused to grant an injunction restraining the defendant from publishing allegedly defamatory material on a particular website.\(^{12}\) During the proceedings, the plaintiffs limited the order sought to publications within New South Wales. Despite this, Simpson J refused the order, stating that:

An injunction to restrain defamation in NSW’s designed to ensure compliance with the laws of NSW, and to protect the rights of plaintiffs, as those rights are defined by the law 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. It is not to be assumed that the law of defamation in other countries is coextensive with that of NSW, and indeed, one knows that it is not. It may very well be that according to the law of the Bahamas, Tazhakistan [sic], or Mongolia, the defendant has an unfettered right to publish the material. To make an order interfering with such a right would exceed the proper limits of the use of the injunctive power of this court.\(^{13}\)

This conclusion was heavily influenced by the perception that “[o]nce published on the Internet material can be received anywhere, and it does not lie within the competence of the publisher to restrict the reach of the publication.”\(^{14}\)

But perhaps the courts’ awareness, during this period, of their own limits in dealing with new technologies is best summarised by Preska J in *American Libraries Association v. Pataki*:

Judges and legislators faced with adapting existing legal standards to the novel environment of cyberspace struggle with terms and concepts that the average […] five-year-old tosses about with breezy familiarity.\(^{15}\)

If we allow ourselves to conclude that this, the first, phase during which the pendulum started moving from its point of departure, firmly engrossed

\(^{11}\)[1999] NSWSC 526.

\(^{12}\)As it turned out, however, the defendant in this action was arguably not the publisher of the allegedly defamatory website. During the proceedings a US resident, Fernando Adrian Sirio, stated in an affidavit that he was the responsible publisher, and that he had constructed the relevant website in conjunction with his studies at University of California, San Diego. It was, however, admitted that Mr Sirio had received some of the material from Mr Berg.


in what can be called un(der)-regulation, lasted from 1991 to 1999, it is interesting to also consider what happened by way of technological advancements during that same timeframe. If we do so, we find that, in the time it took for the legal world to debate whether or not to regulate the WWW-driven Internet, and if so, how such regulation should look, technology advanced significantly. For example, by 1999, there was over 6.5 million websites on the WWW.\(^\text{16}\)

3. THE SECOND PHASE – OVERREGULATION

Major changes in law and legal attitudes do not occur overnight, and there is ample evidence to show that the second phase of overregulation gradually commenced during what I here have time-stamped as the first phase. For example, already in the mid-1990s, the Advocate-General’s office of Minnesota issued a statement that ‘[p]ersons outside of Minnesota who transmit information via the Internet knowing that information will be disseminated in Minnesota are subject to jurisdiction in Minnesota courts for violations of state criminal and civil laws’\(^\text{17}\). Nevertheless, by the start of the new millennium, courts and legislators had developed a rather 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 global nature of the Internet, combined with a limited utilisation of geographical identifiers, meant that courts thus could claim jurisdiction over virtually all Internet conduct. Looking at it from the position of someone who makes content available online, they could come under the jurisdiction of any court in the world and should, thus, abide by all the laws of all the countries in the world. The impracticality of this need not be elaborated upon.

There is no lack of cases that illustrate the complications that this situation gives rise to. I will use two of the most prominent cases as examples.

In December 2002, the High Court of Australia decided that Victorian businessman, Joseph Gutnick, was allowed to sue US publishing company, Dow Jones & Company Inc, in a Victorian court over an allegedly defamat-

---


ory article available on Dow Jones’ website.\(^{18}\) Further it was decided that Victorian law would be applied. Importantly, the majority of the Court stated that:

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.\(^{19}\)

The transatlantic dispute between US Internet company, Yahoo!, and two French associations, La Ligue Contre Le Racisme et L’Antisemitisme and L’Union Des Etudiants Juifs De Franc, related to Yahoo!’s operation of a website which, amongst other things, contained an auction service where Nazi memorabilia/junk was frequently on offer.\(^{20}\) The website could be described as the Yahoo! family’s ‘flagship’, and in contrast to the country-specific Yahoo! sites (e.g., www.yahoo.fr), this site was said to be aimed at the world at large.\(^{21}\) When La Ligue Contre Le Racisme et L’Antisemitisme et al. attempted to have Yahoo! remove the Nazi material from the auction service, in accordance with French penal Code,\(^{22}\) Yahoo! refused.

The French Court characterized Yahoo!’s activities as a tort (faute) and issued a civil law injunction based on the French Code of Civil Procedure. The Court ruled that Yahoo! must take steps to prevent French Internet users from accessing the sections of the auction site containing Nazi memorabilia.\(^{23}\)

These cases, like many others, share an important characteristic – they highlight a gap between what can be regarded as legitimate grounds for claiming jurisdiction and what can be regarded as legitimate grounds for expecting another country to recognise and enforce the judgment. In other words, in both these cases it could be argued to be legitimate for the courts in question to claim jurisdiction over the dispute. At the same time, it can

\(^{18}\) Dow Jones v. Gutnick [2002] 210 CLR 575. This case is discussed in much greater detail throughout the book.

\(^{19}\) Dow Jones v. Gutnick CLR 575, 605.

\(^{20}\) However, the auction service was not at all specifically designed for the purpose of auction Nazi material.

\(^{21}\) A notion backed by the fact that country-specific advertisement was provided on the site.

\(^{22}\) French Penal Code 1791 Article R645-1.

also be argued that both cases involve scenarios in which it is perfectly reasonable to refuse to recognise and enforce the judgments.

In the Yahoo case, that is exactly what happened. Yahoo! sought and obtained a summary judgment to the effect that US courts would not enforce the French decision. While acknowledging France’s right to make law for France, J. 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’.

The Gutnick case was settled and there was consequently no need for Mr Gutnick to seek to have a judgment enforced in the US. Had he had reason to do so, one can expect that he would have run into difficulties as US courts have a tradition of refusing to recognise and enforce foreign judgments that are viewed as out of line with the US’ strict approach to freedom of speech (see also discussion of this below).

While one can say that the second phase started around the change to the new millennium, it is difficult to say when it came to an end. Indeed, it may be correct to say that we are still in the second phase. However, for the sake of this paper, I suggest that the year 2009 can usefully be seen as the end of the second phase. If this is accepted, it is interesting to note that, despite the harsh legal attitudes of the second phase, the number of websites increased dramatically from approximately 6.5 million to almost 250 million.

4. THE THIRD PHASE – A DEGREE OF UNDER-REGULATION

I think we are now in the third phase – a phase characterised by a degree of under-regulation – and due to two significant developments in 2010 I would put that year as the starting point for the third phase. Courts and legislators around the world seem to have accepted the impossibility of viewing an online presence as an indication of an intention to do business with the world at large. This is of course acceptable. However, it seems there is a tendency to be so overly eager to avoid too broad jurisdictional claims so

---


as to end up with a degree of under-regulation. A recent ECJ case is illustrative.

In 2010, the ECJ addressed the two cases of *Pammer v Reederei Karl Schlüter GmbH & KG*\(^{26}\) and *Hotel Alpenhof GesmbH v Oliver Heller*\(^{27}\) jointly. The key question common to the two cases was whether the fact that a website can be consulted on the Internet in the Member State of the consumer’s domicile is sufficient to justify a finding that commercial or professional activities are being directed to that Member State within the meaning of Article 15(1)(c) of Regulation No 44/2001. The Court concluded that:

- The mere fact that a website can be accessed in the consumer’s jurisdiction does not mean that the business has directed its activities to that state;\(^{28}\) and
- Whether a trader has directed its activity to the Member State of the consumer’s domicile, should be ascertained by reference to “whether, before the conclusion of any contract with the consumer, it is apparent from those websites and the trader’s overall activity that the trader was envisaging doing business with consumers domiciled in one or more Member States, including the Member State of that consumer’s domicile, in the sense that it was minded to conclude a contract with them.”\(^{29}\)

The first of these conclusions, while sensible as such, is irrelevant for the cases at hand. Both the *Pammer* case and the *Hotel Alpenhof* case involved contractual situations, as can be expected when the disputes relate to the proper interpretation of an Article addressing contracts concluded by consumers. Thus, we are here not dealing with the more or less randomness of contact and risk typical of claims relating e.g. to marketing practises or other non-contractual situations.

In other words, it must be remembered that the only situation in which the matter of whether a business has directed its activities to the consumer’s state arises, is where that business has entered into a contract with the consumer. To me, it seems contrary to intuition to conclude that a business that has contracted with a consumer did not, at least *prima facie*, direct its activities to the consumer’s state. Thus, the existence of a contract between the

---

\(^{26}\) [2008] Case C-585/08.

\(^{27}\) [2009] Case C-144/09.

\(^{28}\) \(2010\) joined Cases C- 585/08 and C- 144/09 para 95.

\(^{29}\) \(2010\) Joined cases para 95.
business and the consumer should give rise to a strong, but rebuttable, presumption that the business directed its activities to the consumer’s state. That is; in every case where a business has contracted with a consumer in another Member State, it should be presumed that the business has directed its activities to that Member State. After all, the business has made the choice to reap the benefits of contracting with a consumer from that Member State.

Linking this to the main topic of this paper, I suggest that, the approach taken by the ECJ in *Pammer/Hotel Alpenhof* heralds a new era characterised by a fear of making too broad jurisdictional claims resulting in a degree of under-regulation.

Another important component of the emerging under-regulation is exemplified in the US’ recent adoption on 10 August 2010 of a federal statute seeking to address what the US perceives as ‘libel tourism’.30 The key feature of the statute is to make mandatory the nonrecognition of foreign defamation judgments that are seen as inconsistent with the First Amendment’s protection of free speech. With actual enforcement being such a central component in the proper functioning of the private international law machinery, the approach taken by the US is doubtlessly a step in the direction of under-regulation. The obvious risk is that this initiative prompts the response that other countries implement similar non-recognition legislation as to areas of law they do not trust how US courts adjudicate matters. In other words, the US initiative may spark a downward spiral effect.

5. THE FOURTH PHASE – EQUILIBRIUM?
So where to next? If it is conceded that we currently are in a third phase characterised by a degree of under-regulation, we may ask what will replace this phase when it comes to an end. Because one thing is for certain, phases such as those discussed here come and go like the seasons, or like fashions.

One possible future development is that the pendulum again swings too far and we end up with a degree of overregulation. However, the aim should of course be to reach the state of a well balanced regulation that amount neither to overregulation, nor to under-regulation.

---

For the past 7 years, I have been arguing that such equilibrium can be found through the combination of a dis-targeting focus and the widespread utilisation of so-called geo-location technologies. I will here only repeat the key characteristics of such an approach, briefly.

There are sufficiently accurate so-called geo-location technologies available that can be used to ascertain the geographical location of Internet users. That this is so is easily proven by reference to the number of occasions the geographical location of the Internet user affects the content that is provided.

Interestingly, in addition to server-side geo-location technologies, such as technical means for connecting an IP address with a physical location, due to the increasing use of portable devices such as smart phones and tablets, we must now also take account of client-side geo-location provided e.g. through GPS devices and signal triangulation.

There can be no doubt that geo-location technologies are, and have been for some time, sufficiently accurate to be taken into account by the law. It is regrettable that lawyers, legal academics, courts and legislators so often have chosen to turn a ‘blind eye’ to this technical development.

Dis-targeting is a simple concept – we should focus on whether any reasonable steps have been taken to avoid contact with the particular jurisdiction in question. That is, where no such steps have been taken, it may be valid to *prima facie* assume that the content provider was aiming at that jurisdiction (at least as one amongst several jurisdictions being aimed at).

Taken together, the use of geo-location technologies and the focus on dis-targeting, would provide a high level of predictability and party autonomy. Further, flexibility would be available were required through the attention being placed on the taking of “reasonable steps”.

6. CONCLUDING REMARKS
As is the case with any writings on historical events, the parts above that focus on what has been can only ever provide a subjective account of what has happened since the introduction of the WWW. It is subjective in that certain events are emphasised instead of others, and it is subjective in that I have had to interpret those events to describe their overall significance. Further, concerns can also be raised against the parts of the above that seek to predict the future as doing so is difficult and, thus, my guesses may quite simply turn out to be wrong.
However, even given these obvious limitations, I think it is worthwhile to, at this point in time, reflect on how much, and how little, has happened over the past 20 years in the field of private international law as applied to the Internet.

The discussion above lends itself to several conclusions. The sceptic may argue that it shows that, while we have travelled far, we have in fact gotten nowhere, which typically is the case when one moves in circles. There is no doubt validity in such a conclusion. However, if we adopt the views expressed in John Perry Barlow’s *Declaration of the Independence of Cyberspace* as our starting point, it must be said that considerable development has taken place.

Two additional observations can be made in the context of what progress has been made. First, despite a widespread recognition of the complexities specifically associated with the Internet, there are very few examples of Internet-specific private international law rules. However, perhaps this is changing. For example, on 28 October 2010, the Standing Committee of China’s National People’s Congress adopted the *Law of the People’s Republic of China on the Application of Law for Foreign-Related Civil Relations*. That law came into effect on 1 April 2011. Article 46 deals specifically with Internet defamation:

Where such personal rights as the right of name, portrait, reputation and privacy are infringed upon via network or by other means, the laws at the habitual residence of the infringed shall apply.\(^{31}\)

Another recent example of a technology-specific approach can be found in the recent joined cases of *eDate Advertising GmbH v X*\(^ {32}\) and *Olivier Martinez, Robert Martinez v MGN Ltd*,\(^ {33}\) where the ECJ dealt with online publications differently to offline publications. Perhaps this is signalling the end of an almost religious adherence to the so-called ‘technology neutral’ approach.

Second, given the tremendous amount of international interactions that take place on a daily basis online, there are few court cases dealing with jurisdictional claims over Internet conduct. The obvious explanation for this is found in the significant costs and complexities that are associated with

\(^{31}\) *Law of the People’s Republic of China on the Application of Law for Foreign-Related Civil Relations* 2011, Article 46.

\(^{32}\) [2011] Referring court Bundesgerichtshof Germany Case C-509/09.

\(^{33}\) [2011] Referring court Tribunal de grande instance de Paris France Case C-161/10.
cross-border litigation. Thus, the absence of heard cases cannot be seen as an indication of a lack of disputes, and should of course not be seen as an indication that the issue of jurisdiction in Cyberspace is lacking in importance.

However, the most important conclusion may be that the attitude adopted by the law, at least as regards to the regulation of jurisdictional claims, has a very limited impact on technological developments. How else would one explain that, the number of websites increased approximately 38 times (from approximately 6.5 million to almost 250 million) during the second phase characterised by harsh legal attitudes?

Having said that, this conclusion should not prevent us from trying to construct the ‘best’ jurisdictional rules possible.