Borders on, or border around

The future of the internet

Svantesson, Dan Jerker B

Published in:
Albany Law Journal of Science and Technology

Published: 01/01/2006

Document Version:
Publisher's PDF, also known as Version of record

June 2006

Borders on, or border around – the future of the Internet

Dan Jerker B. Svantesson
Bond University, dan_svantesson@bond.edu.au

BORDERS *ON*, OR BORDER *AROUND*— THE FUTURE OF THE INTERNET

Dr. Dan Jerker B. Svantesson *

TABLE OF CONTENTS

* Assistant Professor, Faculty of Law, Bond University, Gold Coast Queensland 4229 Australia, Ph: +61 7 5595 1418, E-mail: Dan_Svantesson@bond.edu.au, (www.svantesson.org) - Research Associate, Cyberspace Law and Policy Centre - Contributing Editor, World Legal Information Institute (www.worldlii.org) - National Convener, International Law Interest Group (Australasian Law Teachers Association) - National Rapportuer (Australia) Data Protection Research and Policy Group, (The British Institute of International and Comparative Law).

This article illustrates how borders currently are being placed within the Internet through a combination of jurisdictional claims and technical developments. It makes clear that these borders are transforming the Internet from an open, and virtually global, communications network, into something that more resembles our physical world divided by borders of different kinds.

It submits that, in light of the threat of such an undesirable development, we must re-examine the possibility of treating the Internet as a separate space. Such a space must be approached in a context-specific manner. In other words, we must deal with each legal issue separately. Furthermore, if states ever are to be inclined to give up their claims to regulating the Internet, alternative forms of regulation must be put in place; relying on self-regulation is not an option today. In addition, an appropriate judiciary must be put in place, and effective enforcement must be ensured.

Focusing on Internet defamation, the article highlights how a well-recognized regulatory framework is already in place through the *International Covenant on Civil and Political Rights*, and that an adjudicative body exists in the *United Nation's Human Rights Committee*. Drawing upon these existing mechanisms, a Convention Model to regulate cross-border Internet defamation arising out of mass-communication is presented.

I. INTRODUCTION

Certain Internet applications, such as the World Wide Web (WWW), are widely recognized as being borderless.[1] This "borderlessness" causes complications in relation to the application of law to Internet behavior.

It is submitted that there are at least two ways in which the jurisdictional difficulties associated with the Internet's unique set of characteristics can be addressed. Either borders need to be placed *on* the Internet, or borders need to be placed *around* the Internet.

The first alternative can be achieved in either of two ways: private international law can be adjusted to properly address Internet conflicts and place sensible protective borders on the Internet, or technical borders may be placed on the Internet, e.g.,

---

[1] David R. Johnson & David Post, *Law and Borders –The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367 (1996); Dan Jerker B. Svantesson, *Geolocation Technologies and Other Means of Placing Borders On the 'Borderless' Internet*, 23 J. MARSHALL J. COMPUTER & INFO. L. 101, 101 (2004).

through so-called geo-location technologies.[2] Currently, borders seem to be placed on the Internet through a combination of these two approaches.

The second alternative—placing borders around the Internet—partly echoes the message of pioneer cyber-libertarians, such as that expressed by John Perry Barlow in his famous *Declaration of the Independence of Cyberspace*.[3] Such ideas were popular amongst early commentators, but have essentially been abandoned as unrealistic.

However, this article argues that, in light of the extraordinarily serious consequences of placing borders on the Internet, it is necessary to re-examine the possibility of placing borders around it. For that to be a feasible path to take, however, we must depart from the utopian dreams of "self regulation" relied upon by early commentators.[4] This article argues that, at least in relation to some areas of law, placing borders around the Internet is a realistic alternative provided that a structure of separate regulation with separate dispute resolution functions is put in place. This proposition is discussed in the context of one of the most controversial areas of law—Internet defamation.[5]

II. The Difficulties Associated with Internet Defamation

The regulation of defamation is essentially an exercise in balancing two fundamental human rights: the freedom of expression on the one hand, and the right of reputation on the other.[6] As such, it is not surprising that states generally are very protective of their right to decide defamation disputes. Serious problems arise when material is lawful from where it is made available, but

---

[2] Svantesson, *supra* note 1, at 101-03, 137; Dan Jerker B. Svantesson, *Private International Law and the Internet* (Unpublished PhD thesis, University of New South Wales (2004)) (on file with author).

[3] *See* John Perry Barlow, *A Declaration of the Independence of Cyberspace*, Feb. 8, 1996, http://homes.eff.org/~barlow/Declaration-Final.html (purporting that the law of the physical world does not apply to the dimensions of cyberspace).

[4] Johnson & Post, *supra* note 1, at 1367, 1387; Barlow, *supra* note 3.

[5] *See infra* Part II; Johnson & Post, *supra* note 1, at 1367, 1381 (noting that treatment of the global Internet as a separate place creates confusing standards with regards to liability because allegedly defamatory statements would only be considered as published "on the Net" and not distributed on paper).

[6] David Lindsay, Ctr. for Media Comm. & Info. Tech. Law, Research Paper No. 10, Liability for the Publication of Defamatory Material via the Internet 4 (2000), *available at* http://www.law.unimelb.edu.au/cmcl/publications/Defamation.pdf.

unlawful in some other state, and that latter state is asked to exercise jurisdiction over the person responsible for the material being made available. Several Internet applications, including WWW, BBS and e-mail, are ideally suited for distributing material to foreign places in an easy and cost-effective manner.

There has been a range of high-profile disputes relating to jurisdictional issues in Internet defamation cases. In the United States, jurisdiction has been exercised on a range of grounds in earlier Internet defamation cases.[7] It would now, however, seem that the "effects test" has prevailed online also. The leading case on this topic is arguably *Young v. New Haven Advocate*.[8] There, two newspapers based outside Virginia published articles, in part discussing the conduct of Virginian residents in Virginia.[9] The articles were available both offline and online.[10] Despite this, the United States Court of Appeals for the Fourth Circuit concluded that:

> The newspapers did not post materials on the Internet *with the manifest intent of targeting* Virginia readers. Accordingly, the newspapers could not have "reasonably anticipate[d] being haled into court [in Virginia] to answer for the truth of the statements made in their article[s]." . . . In sum, the newspapers do not have sufficient Internet contacts with Virginia to permit the district court to exercise specific jurisdiction over them.[11]

Throughout its published decision, the Court made frequent reference to *ALS Scan, Inc. v. Digital Service Consultants, Inc.*,[12] a copyright case decided a couple of months earlier.[13] In *ALS*

---

[7] *See, e.g.,* Krantz v. Air Line Pilots Ass'n, 427 S.E.2d 326, 328-29 (Va. 1993); Bochan v. La Fountaine, 68 F. Supp. 2d 692, 698-99 (E.D. Va. 1999) (holding that jurisdiction was based on the location of the internet server).

[8] *See generally* Young v. New Haven Advocate, 315 F.3d 256 (4th Cir. 2002) (reversing the lower court's decision denying defendant's motion to dismiss for lack of jurisdiction because the newspapers failed to show sufficient contacts with Virginia by merely posting on the Internet).

[9] *Id.* at 259. Maximum-security prisons in Connecticut were overcrowded, and as a consequence, Connecticut had contracted with Virginia to house a number of Connecticut prisoners. The articles in question discussed the state of a penal institution in Virginia, as well as the conduct of its warden. *Id.*

[10] *Id.* at 260.

[11] *Id.* at 264 (quoting Calder v. Jones, 465 U.S. 783, 790 (1984) (emphasis added)). The targeting approach has also been strongly advocated in recent literature. *See, e.g.,* Gregory J. Wrenn, *Cyberspace is Real, National Borders are Fiction: The Protection of Expressive Rights Online Through Recognition of National Borders in Cyberspace*, 38 STAN. J. INT'L L. 97, 98 (2002).

[12] 293 F.3d 707 (4th Cir. 2002).

[13] *Young,* 315 F.3d at 261-63.

Scan,[14] the Court formulated the following test, based on the so-called "*Zippo* test"[15] developed in 1997:

> [W]e conclude that a State may, consistent with due process, exercise judicial power over a person outside of the State when that person (1) directs electronic activity into the State, (2) with the manifested intent of engaging in business or other interactions within the State, and (3) that activity creates, in a person within the State, a potential cause of action cognizable in the State's courts. Under this standard, a person who simply places information on the Internet does not subject himself to jurisdiction in each State into which the electronic signal is transmitted and received. Such passive Internet activity does not generally include directing electronic activity into the State with the manifested intent of engaging business or other interactions in the State thus creating in a person within the State a potential cause of action cognizable in courts located in the State.[16]

By considering part one and part two of the test together, the Court in *Young* modified the *ALS Scan* test to work "more smoothly"[17] for cases where the Internet activity is the posting of news articles on a website: "We thus ask whether the newspapers manifested an intent to direct their website content—which included certain articles discussing conditions in a Virginia prison—to a Virginia audience."[18]

On September 16, 2005, the Ontario Court of Appeal (Canada) decided that former United Nations official Cheickh Bangoura would not be allowed to sue the *Washington Post* in Ontario over two articles that accused Mr. Bangoura of sexual harassment, and financial wrongdoings while he was working in the Ivory Coast.[19] When the disputed articles were published in 1997, there were only seven subscribers to the Washington Post in Ontario.[20] However, the articles could also be accessed on the newspaper's website.[21]

---

[14] 293 F.3d 707.

[15] Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1124 (W.D. Pa. 1997) (developing a "sliding scale" of personal jurisdiction analysis, stating that "the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet").

[16] *ALS Scan*, 293 F.3d at 714.

[17] *Young,* 315 F.3d at 263.

[18] *Id.*

[19] Bangoura v. Washington Post, No. C41379, 142 A.C.W.S. (3d) 247 (O.C.A. Sept. 16, 2005), *available at* 2005 A.C.W.S.J. LEXIS 6141, *1, *3-4, *23-24.

[20] *Id.* at *1-2.

[21] *Id.* at *5-6.

Mr. Bangoura, who moved to Ontario approximately three years after the articles first were published, initiated the action against the Washington Post in an Ontario court in 2003, six years after the articles were published.[22] Motivated by the view that the Washington Post "should have reasonably foreseen that the story would follow the plaintiff wherever he resided,"[23] the Ontario Superior Court of Justice ruled in favor of Mr. Bangoura in January 2004.[24] However, the Superior Court of Justice's decision in this matter changed the direction in which Canadian law is heading within this controversial area of law. The court noted "that there is simply no real and substantial connection between this action and Ontario."[25]

The Internet defamation dispute between Victorian (Australia) businessman, Joseph Gutnick, and U.S. publishing company, Dow Jones & Company Inc., has gained a large amount of attention.[26] Dow Jones published an article allegedly defamatory of Mr. Gutnick.[27] The article was available both in a magazine and online, and was mainly read in the U.S.[28] However, a small number of copies of the magazine were distributed in Victoria, and the website containing the article had a small number of subscribers in Victoria.[29] An exact number of readers could not be established for either the web or the magazine version of the article, but it was suggested that important Victorian business people had in fact read the article. Mr. Gutnick sued Dow Jones in the Supreme Court of Victoria seeking damages for defamation. Dow Jones responded by claiming that the court lacked jurisdiction over the dispute; however, in case the court should find it has jurisdiction, it should decline to exercise its jurisdiction. Finally, if the court was to decide the dispute, U.S. law should be applied.[30]

The *Gutnick* case is interesting for several reasons, and is believed to be the first of its kind. As far as jurisdiction is concerned, it is to be noted that the majority of the High Court of

---

[22] *Id.* at *1-2, *4.
[23] Bangoura v. Washington Post, [2004] 235 D.L.R (4th) 564, 571.
[24] *Id.* at 576.
[25] *Bangoura*, 2005 A.C.W.S.J. LEXIS 6141, at *622.
[26] *See generally* Dow Jones & Co. v. Gutnick, (2002) 210 C.L.R. 575.
[27] *Id.* at 594.
[28] *Id.* at 622.
[29] *Id.* at 607.
[30] *Id.* at 595-96, 607. This is a common approach for a defendant wishing to avoid having a dispute heard in the forum in question. Note, however, that the option of asking the court to decline jurisdiction is mainly available in common law courts.

Australia found that Victoria may exercise jurisdiction over Dow Jones as the tort sued for was committed in Victoria[31] and damages were suffered in Victoria. The basis for the court's conclusion can arguably be said to be found in the following passage:

> 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.[32]

Another Australian Internet defamation case of interest involved a dispute between, on the one hand, the Macquarie Bank Limited and one employee, and on the other hand, a former employee of the bank.[33] In that case, the plaintiffs were seeking an injunction against publications occurring via a website alleged to be linked to the defendant.[34] The Court however, did not grant the injunction:

> An injunction to restrain defamation in NSW is designed to ensure compliance with the laws of NSW, and to protect the rights of plaintiffs, as those rights are defined by the law 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. For this reason alone, I would refuse the order sought.[35]

Finally, in *Investasia v. Kodansha*, a businessman and his business (neither of them based in Hong Kong, but both doing business in Hong Kong and elsewhere) initiated a defamation action in

---

[31] *See* Vict. Stat. R. Regs. & B., § 7.01(1)(i), 1996 (Austl.).

[32] Dow Jones & Co. v. Gutnick, (2002) 210 C.L.R. 575.

[33] Macquarie Bank Ltd. v. Berg, (1999) N.S.W.S. Ct. 526 at ¶ 1, 3, *available at* http://www.austlii.edu.au (enter search query for [1999] NSWSC 526, and select case from list).

[34] *Id.* at ¶ 1, 4, 5.

[35] *Id.* at ¶ 14-15.

a Hong Kong court against two defendants based in Japan.[36] According to the statement of claim, the plaintiffs were libelled by two articles, written in Japanese, by one defendant and published by the other.[37] The articles appeared in a magazine as well as on a website.[38] While approximately 500,000 copies of the magazine were published, only 157 copies were distributed in Hong Kong.[39] Further, it was not known how many people read the online version.[40] In relation to the comparatively small number of copies that had been distributed in Hong Kong, Justice Findlay remarked that:

> Of course, one can do sums with the figures and say that the number published in Hong Kong compared with the total number is very small, but I do not think this is the right approach. What I am concerned about is whether or not the number is significant for the purposes of deciding whether a complaint about the publication could be said to be one of substance. I think it is.
>
> This consideration must take into account the nature of the publication. If it is low-key and boring, one might think that a greater size of publication is necessary to consider the tort committed as substantial for present purposes. Where, however, as here, the alleged defamatory material is what one may describe as sensational and juicy, a much smaller size of publication would be sufficient. The nature of the material published in the case before me is such that, in the nature of things, one would expect what is said about the plaintiffs to spread from mouth to ear quickly amongst those who might do business with them. In these circumstances, I would regard a significantly smaller number than 157 as sufficient.[41]

In deciding the matter, Justice Findlay made an interesting observation also in relation to whether the plaintiff had a sufficient connection to, and reputation in, Hong Kong. While Lord

---

[36] Investasia Ltd. v. Kodansha Co. [1999] H.K.C.F.I. 499 (H.C.), *available at* http://legalref.judiciary.gov.hk/lrs/common/ju/judgment.jsp (search case number HCA012519/1997 and select case link).

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] *Id.* It is interesting to note that this way of thinking (i.e. "one can do sums with the figures and say that the number published in Hong Kong compared with the total number is very small, but I do not think this is the right approach") appears to be contrary to the English tradition. *Id. See, e.g.,* Tara Garfinkel, *Jurisdiction Over Communication Torts: Can You be Pulled into Another Country's Court System for Making a Defamatory Statement Over the Internet? A Comparison of English and U.S. Law*, 9 TRANSNAT'L LAW. 489, 523 (1996) (stating that "[t]he court will consider a defendant publication's relative circulation in England as compared to elsewhere").

Justice Hirst used the conjunctive, "and," between "connection" and "reputation" in the famous English case *Berezovsky v. Forbes Inc.*, Justice Findlay argued "that the fundamental consideration is the extent to which the plaintiffs have a reputation in Hong Kong to protect. The degree to which the plaintiffs have connections here is evidence that they have, or have not, a reputation here that merits protection."[42] Furthermore, having noted the well-established common law principle that "[p]ublication[43] of the libels in Hong Kong would be torts committed in Hong Kong,"[44] Justice Findlay made the odd remark that "damage in Hong Kong in a libel case can flow only from a publication in Hong Kong. So, whether they say so or not, the plaintiffs are confined in their action to a tort committed in Hong Kong causing damage in Hong Kong."[45]

The above highlights the difficult issues involved in cross-border Internet defamation cases, and makes clear that different courts take different approaches to these matters. It also brings attention to the fact that defamation law is a rather intensively litigated area of law, as far as Internet jurisdictional issues are concerned.

The above examination also reveals that individual states do make jurisdictional claims over foreign publishers, and do seek to apply their laws to them. A consequence of this is that virtual borders are being placed on the Internet—website operators are forced to take measures to avoid contact with those jurisdictions they do not wish to be legally exposed to.[46] In other words, if a United States publisher wishes to avoid the risk of being sued in Australia under Australia's defamation laws, it must take steps to

---

[42] *Compare* Berezovsky v. Forbes Inc., (1999) E.M.L.R. 278, 300 (stating that "the extent to which the plaintiff has connections with and a reputation to protect in this country" as the standard in England), *with Investasia*, [1999] H.K.C.F.I. 499 (considering primarily "the extent to which the plaintiff[ ] [has] a reputation . . .to protect").

[43] Note that under the common law, "publication" occurs where the defamatory meaning enters the mind of a third person. *See, e.g.*, Webb v. Bloch (1928) 41 C.L.R. 331, 363 (Austl.) ("To publish a libel is to convey by some means to the mind of another the defamatory sense embodied in the vehicle.").

[44] *Investasia*, [1999] H.K.C.F.I. 499; *see also* Yung v. Brion, [2002] H.K.C.F.I. 652, ¶ 13 (C.F.I.), *available at* http://legalref.judiciary.gov.hk/lrs/common/ju/judgment.jsp (search case number HCA000079/2002 and select case link) (making reference to Bata v. Bata, [1948] WN 366 (C.A.)).

[45] *Investasia*, [1999] H.K.C.F.I. 499.

[46] *See id.* (supporting the proposition that if defendants did not want to be legally exposed to Hong Kong, then they should have taken measures to avoid contact with Hong Kong).

prevent its websites from being accessed in Australia. Alternatively, such a publisher could attempt to ensure that all of its content is legal everywhere. This latter approach has two serious problems associated with it: first, it is unrealistic for a website operator to know all the laws of all the states of the world. Second, to avoid having to know all the laws of all the states of the world, website operators would need to adjust their content to the most restrictive laws they are exposed to. This would clearly lead to a race to the bottom and valuable online content would be lost.

At the same time, the placing of borders *on* the Internet seems to be a more realistic goal than placing borders *around* the Internet. This is due to several factors, but in particular it is due to the fact that states would be unwilling to give up their jurisdictional claims over the Internet, and Internet activity.

III. Finding the Answers in Private International Law

The most obvious manner in which borders are being placed on the Internet is through the application of private international law rules; states make jurisdictional claims reaching outside their territory and thereby stake their claims over Internet activities.[47] Arguably, the most prominent article discussing the role played by private international law in Internet regulation is Goldsmith's *Against Cyberanarchy*.[48] Taking his point of departure in the writings of the people he refers to as "regulation skeptics," Goldsmith draws essentially two conclusions: "From the perspective of jurisdiction and choice of law, regulation of cyberspace transactions is no less feasible than regulation of other transnational transactions";[49] and extraterritorial claims of jurisdiction, and application of law, are legally legitimate when local harm has been caused.[50]

Logically, Goldsmith is correct in dismissing the notion that all Internet activities are, or should be, immune from territorial regulations: "Cyberspace participants are no more self-contained than telephone users, members of the Catholic Church, corporations, and other private groups with activities that transcend jurisdic-

---

[47] Samuel F. Miller, Note, *Prescriptive Jurisdiction over Internet Activity: The Need to Define and Establish the Boundaries of Cyberliberty*, 10 Ind. J. Global Legal Stud. 227, 229, 254 (2003).

[48] Jack L. Goldsmith, *Against Cyberanarchy*, 65 Univ. Chi. L. Rev. 1199 (1998).

[49] *Id.* at 1199, 1213.

[50] *E.g.*, *id.* at 1240 (explaining that a jurisdiction can regulate extraterritorial acts under the concept of territorial sovereignty).

tional borders."[51] From the perspective of jurisdiction and choice of law, the conclusion that regulation of cyberspace transactions is feasible should not stem from any comparison between Internet communications and offline communications. Instead, it is respectfully submitted, that the real motivation for the feasibility of private international law rules being applied to the Internet is that *we* create the rules of private international law, so *we* can make them work in any context. The rules of private international law have developed, been modified and changed continuously since rules of private international law were first created – there is no reason to think that we will not be able to apply private international law rules to Internet activities.

A. Internet Architecture and "Borders"

There has been considerable technical development towards placing geographical borders on the Internet.[52] These technological advancements are partly motivated by perceived business advantages. For example, if a website operator can see where an access-seeker is located, "suitable" advertisement can be specifically targeted at that individual.[53] Other perceived advantages include ensuring regulatory compliance, reduced fraud risk and the keeping of licensed content within boundaries.[54] At the same time, it cannot be ignored that these technological advancements also are partly motivated by website operators' desire to avoid contact with "web-surfers" from undesirable states.[55]

The fact that the Internet is being regulated through both the law and technical developments is widely acknowledged.[56] One of

---

[51] *Id.* at 1242.

[52] *See* Svantesson, *supra* note 1, at 137-38 (explaining the development of the Internet from a borderless dimension to a place that takes into account legal and geographical borders).

[53] *Id.* at 102.

[54] *See id.* at 102-03 (emphasizing the advantage of being able to alter web site material to comply with the regulations of an access-seeker's geographical location).

[55] *See id.* at 114-17 (discussing the advantages to web site operators when accurate geographic location technology is employed).

[56] However, so far, little attention has been given to this issue in relation to the placing of borders on the Internet. *See, e.g.,* Matthew Fagin, Comment, *Regulating Speech Across Borders: Technology vs. Values*, 9 MICH. TELECOMM. & TECH. L. REV. 395, 398-99 (2003) (noting the new, emerging trend of imposing geographic borders on cyberspace, as evolved through case law and new technology).

the better-known articles dealing with the relation between law and technology is Joel Reidenberg's *Lex Informatica*[57]:

> This Article will show that for network environments and the Information Society, . . . law and government regulation are not the only source of rulemaking. Technological capabilities and system design choices impose rules on participants. The creation and implementation of information policy are embedded in network design and standards as well as in system configurations.[58]

Although it is undeniably true that the technological structure of the Internet does impose rules on Internet activities, this is hardly a new phenomenon.[59] In a sense, this is not different from the way the physical structures of the road network imposes rules on activities on our roads. Just as the introduction of PICS[60] will affect Internet users' behavior,[61] the expansion of a certain road from, for example, four to six lanes, will affect the behavior of the users of that road. Similarly, just as regulators of the Internet need to take account of technological solutions, regulators of the road network need to consider technological solutions (e.g., speed cameras, widening of roads, traffic lights etc.).[62] The important difference is that the road network is essentially under government control and the Internet's architecture and development is largely in the hands of private companies. Lawrence Lessig has explored this vital difference.[63] In referring to architecture as

---

[57] Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEXAS L. REV. 553 (1998).

[58] *Id.* at 554-55.

[59] Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 507-09 (1999).

[60] *See* Reidenberg, *supra* note 57, at 558-59 ("PICS [Platform for Internet Content Selection] is a set of technical specifications that define a standard format for rating labels describing materials available on the Internet and a standard mechanism for distributing those labels.").

[61] *See id.* at 558-60 (explaining that the structure of PICS could permit filtering by individual choice but still provide automatic enforcement).

[62] *See* Graham Greenleaf, *An Endnote on Regulating Cyberspace: Architecture vs. Law?*, 21 U. N.S.W. L. J., 593, 604, stating:

> In real space laws criminalising bank robbery are very helpful, but thick walls, bulletproof glass, armed guards and combination locks on safes are the most effective constraints. We don't need a law on larceny of real property. When considering the combination of constraints which make up regulation in real space, it is easy to ignore the roles of the natural environment, the artefacts of the built environment, and human biology, because we so often take them as the 'givens' of the situation being regulated.

[63] *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999) (giving a detailed discussion of the architecture and development of the internet).

"code", Lessig states that "[o]nce it is plain that code can replace law, the pedigree of the codewriters becomes central. Code in essence becomes an alternative sovereign—since it is in essence an alternative structure of regulation. But who authors this sovereign authority? And with what legitimacy?"[64]

B. Geo-Location Technologies[65]

In bringing popular attention to, and increased understanding of, the fact that the Internet is being regulated both through law and technical developments, Lawrence Lessig made several interesting statements:

> I said that we could understand regulation in real space as a function of four sorts of constraints—law, norms, markets, and what I called real space code. We can understand regulation in cyberspace in the same way. Regulation in cyberspace is a function of similar constraints. It too is a function of the constraints of law, of norms, of the market, and of what I will call, "code."[66]

While Lessig outlines four mechanisms for regulation, only the relation between legal code and computer code is relevant here. The fact that lawmakers take account of technological developments is of central importance when examining the potential uses of so-called geo-location technologies.

The use of technology to pinpoint the geographical location of those active on the Internet is a fairly new phenomenon and has not yet gained any large amount of attention in literature. In "older" Internet commentaries[67] and case law[68] pinpointing the geographical location of a user was frequently said to be impossible. Indeed, the impossibility of linking those active on the Internet to a geographical location has been said to be a distinc-

---

[64] Lawrence Lessig, The Law of the Horse: What Cyberlaw Might Teach 25 (1997) (unpublished working draft, on file with Albany Law Journal of Science and Technology) [hereinafter *Lessig's Law of the Horse Working Draft*] (as referred to in: Greenleaf, *supra* note 62, at 601 n.29).

[65] I have previously dealt with these technologies in detail. *See* Svantesson, *supra* note 1, at 101-39. This part of the article draws upon that publication.

[66] *Lessig's Law of the Horse Working Draft*, *supra* note 64, at 17; *see also* Lawrence Lessig, *supra* note 59, at 506-508 for the revised published version.

[67] *See* Johnson & Post, *supra* note 1, at 1374 (exploring the increasing involvement of the legal system within the expanding boundaries of Cyberspace); *see also* more recent works, such as: HENRIK SPANG-HANSSEN, NORWEGIAN RESEARCH CENTER FOR COMPUTERS AND LAW, CYBERSPACE JURISDICTION IN THE U.S. – THE INTERNATIONAL DIMENSION OF DUE PROCESS 3 (2001) (investigating the structure of the world wide web and its expansion since its birth).

[68] *See, e.g.*, Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 170-71 (S.D.N.Y. 1997).

tive feature of the Internet.[69] If ever true, the development of the Internet has now rendered these statements obsolete, at least in part. As Dan Jerker B. Svantesson wrote:

> [I]t is still true that Internet communication largely lacks reliable geographical identifiers . . . geo-location technologies are becoming increasingly accurate, and while [they are] unlikely to ever be one hundred percent accurate, may, [as will be discussed below] in the near future or perhaps already today, be accurate enough for legal purposes.[70]

As outlined elsewhere, geo-location technologies operate on several levels.[71] We will here focus on geo-location technologies that are based on the translation of Internet Protocol (IP) addresses into geographical locations, by the use of information stored by the provider of the geo-location service. URLs work as follows:

> As the access-seeker enters the appropriate Uniform Resource Locator ("URL") into his/her browser, or clicks on the appropriate hyperlink, an access-request is sent to the server operating the requested Web site. As the server receives the access-request, it, in turn, sends a location request (e.g. forwards the access-seeker's Internet Protocol ("IP") address) to the provider of the geo-location service. The provider of the geo-location service has gathered information about the IP addresses in use, and built up a database of geo-location information. Based on the information in this database, the provider of the geo-location service gives the Web site server an educated guess as to the access-seeker's location. Armed with this information, the Web server can provide the access-seeker with the information deemed suitable [or if desirable, deny access to the requested content].[72]

Reconnecting back to the interaction between law and architecture (here exemplified by geo-location technologies), it is interesting to note how the French Court's 2000 decision in the *Yahoo!* case concluded, based on the expert evidence provided, that the defendant, Yahoo! Inc., successfully could prevent access-seekers, located in France from accessing the disputed Nazi memorabilia/

---

[69] *See id.* at 164, 166 (commenting on the Internet's lack of a centralized, geographic location).

[70] Svantesson, *supra* note 1, at 101-102.

[71] *See id.* (distinguishing between sophisticated geo-location technologies and unsophisticated geo-location technologies).

[72] *Id.* at 110.

junk available on its website.[73] In that case, the existence of feasible technical solutions was determinative.

C. *The Problems with Borders Being Placed on the Internet*

The placing of borders on the Internet has the obvious consequence of people using the Internet having to cross these borders. It is in relation to this observation that the difference between borders imposed by private international law, and borders imposed by technology, becomes clear.

If a person located outside the US, for example, seeks to access the website of *Showtime Online* (by entering the URL "www.sho.com"), they will be met with the following message: "Sorry. We at Showtime Online express our apologies; however, these pages are intended for access only from within the United States."[74] In this case, the average Internet user is simply unable to access the relevant website—a relatively firm geographically focused border is placed around the website in question. If, or perhaps more likely when, this practice becomes widespread, then the "borderless" Internet will cease to exist.

While the borders imposed by private international law may make people reluctant to engage in cross-border interactions, they do not directly prevent such activities. In contrast, the borders imposed by technology may actually prevent the crossing of those borders. At the same time, however, it must be remembered that the borders raised by technology may be motivated by the need for borders created by claims under private international law. Thus, in a sense, private international law does not only directly erect borders through extraterritorial jurisdictional claims, it also indirectly erects borders through its influence on people's use of technology.

While the technologies that make these kinds of borders possible can be circumvented,[75] we are doubtlessly witnessing the

---

[73] Int'l League Against Racism & Anti-Semitism (LICRA) v. Yahoo! Inc., Superior Court of Paris, Nov. 20, 2000 (Fr.) *translated by* GigaLaw.com, http://www.gigalaw.com/library/france-yahoo-2000-11-20-lapres.html.

[74] *See* The L Word, Guinevere Turner.com, http://www.sociopranos.com/GTS/thelword.html (last visited Mar. 19, 2006) (blogging about Showtime Online's message to non-US residents); *see also* Reason: Hit & Run, A Steaming Pile of Entertainment (Dec. 22, 2003), http://www.reason.com/hitandrun/2003/12/a_steaming_pile.shtml (blogging about Showtime Online's message to non-US residents).

[75] *See* Svantesson, *supra* note 1, at 101-02 (explaining that even though technology that identifies geographical Internet borders is getting more accurate, it will probably never be one hundred percent reliable).

Internet undergoing a remarkable change—from the world's first and only "borderless" communications medium to something that much more resembles our physical world divided by borders of different kinds. Thus, it may no longer, if it ever was, be valid to claim that states cannot make jurisdictional claims in relation to what occurs on the Internet. However, it is still important to question whether such claims are desirable, and having recognized the problems that arise from such jurisdictional claims, it is still important to search for better alternatives.

IV. Borders Around the Internet

Any attempt to turn the Internet into a totally separate legal space would be highly complex. In fact, such a development may be unlikely, at least in the foreseeable future. At the same time, it must be acknowledged that in at least one area, the Internet is conceptually treated as a separate space with separate, or, more accurately, co-existing regulation, and to an extent separate dispute resolution functions—domain names. The Internet Corporation for Assigned Names and Numbers (ICANN) is a quasi-governmental organization in control of the IP address space allocation, protocol parameter assignment, domain name system management, and root server system management functions.[76] The World Intellectual Property Organisation (WIPO) is an international organization dedicated to helping to ensure that the rights of creators and owners of intellectual property are protected worldwide and that inventors and authors are recognized and rewarded for their ingenuity,[77] and it provides a dispute resolution forum for domain name disputes.[78] While playing different parts, when combined, these two bodies provide for regulation of, and adjudication of disputes relating to, domain names.[79] However, it is to be remembered that decisions made under the

---

[76] ICANN, FAQs, What is ICANN, http://www.icann.org./faq/#WhatisICANN (last visited Mar. 19, 2006).

[77] WIPO, About WIPO, http://www.wipo.int/about-wipo/en/index.html?wipo_content_frame=/about-wipo/en/gib.htm (last visited Mar. 19, 2006).

[78] ICANN, Approved Providers for Uniform Domain-Name Dispute-Resolution Policy, http://www.icann.org/dndr/udrp/approved-providers.htm (last visited Mar. 19, 2006).
While WIPO is the largest dispute resolution provider, in relation to domain name disputes, it must be remembered that there also are other providers of the same sort of service. At the time of writing, WIPO was one of four approved providers for ICANN's Uniform Domain-Name Dispute-Resolution Policy. *Id.*

[79] ICANN, Uniform Domain Name Dispute Resolution Policy, http://www.icann.org/dndr/udrp/policy.htm (last visited Mar. 19, 2006).

ICANN/WIPO arrangement very well may be challenged in the courts or under other dispute resolution arrangements. What makes the ICANN/WIPO model unique is that Internet-related disputes are, to an extent, separated from offline disputes.[80] ICANN/WIPO represents a model where the Internet is viewed as a separate "space"- borders, although not very firm ones, are placed *around* the Internet. This can be contrasted to virtually all other areas (e.g. defamation), where Internet activities are regulated in the same manner as "real world" activities—borders are placed *on* the Internet. Of course, it is much easier to distinguish domain name disputes from other IP disputes than it would be to distinguish, for example, between online and offline defamation. Yet, perhaps similar organization should be established in order to keep disputes arising out of other Internet activities separate from offline disputes? Perhaps there is a need for Internet specific regulations? Could further existing international courts, or specifically designed international courts for these purposes, determine disputes arising from Internet activities? Or, perhaps other forms of dispute resolution are better equipped to deal with Internet disputes?

A. The Internet—Another (International) "Space"?

Over the relatively short period of time since the introduction of the Internet, several models for self-regulation or "alternative regulation" have been presented. Although the more extreme models have largely become a thing of the past,[81] the debate goes on.[82]

---

[80] WIPO Arbitration and Mediation Center, Frequently Asked Questions: Internet Domain Names, http://arbiter.wipo.int/center/faq/domains.html (last visited Mar. 19, 2006) (explaining the type of disputes handled by WIPO: internet domain names disputes).

[81] *See generally* Barlow, *supra* note 3 (voicing his opposition to regulation in Cyberspace by "Governments of the Industrial World").

[82] Perhaps particularly noteworthy is the discussion between Chicago law professor Jack Goldsmith on the one hand, and the prominent "cyber-libertarians" David Johnson and David Post on the other. The latest contribution being David Post's *Against* "Against Cyberanarchy" (a response to Goldsmith's *Against Cyberanarchy*). *See* Goldsmith, *supra* note 48, at 1199, 1200; David G. Post, *Against* "Against Cyberanarchy," 17 BERKELEY TECH. L.J. 1365, 1366 (2002). There are also, of course, other contemporary or recent proponents of regulation resistance. *See* Shamoil Shipchandler, Note, *The Wild Wild Web: Non-Regulation as the Answer to the Regulatory Question*, 33 CORNELL INT'L L.J. 435, 461-63 (2000) (supporting self-regulation by Internet users and ISPs over government regulation of the Internet); Edward J. Valauskas, *Lex Networkia: Understanding the Internet Community*, FIRST MONDAY (1996), *available at* http://www.firstmonday.dk/issues/issue4/valauskas/; Robert Corn-Revere,

ICANN/WIPO arrangement very well may be challenged in the courts or under other dispute resolution arrangements. What makes the ICANN/WIPO model unique is that Internet-related disputes are, to an extent, separated from offline disputes.[80] ICANN/WIPO represents a model where the Internet is viewed as a separate "space"- borders, although not very firm ones, are placed *around* the Internet. This can be contrasted to virtually all other areas (e.g. defamation), where Internet activities are regulated in the same manner as "real world" activities—borders are placed *on* the Internet. Of course, it is much easier to distinguish domain name disputes from other IP disputes than it would be to distinguish, for example, between online and offline defamation. Yet, perhaps similar organization should be established in order to keep disputes arising out of other Internet activities separate from offline disputes? Perhaps there is a need for Internet specific regulations? Could further existing international courts, or specifically designed international courts for these purposes, determine disputes arising from Internet activities? Or, perhaps other forms of dispute resolution are better equipped to deal with Internet disputes?

A. The Internet—Another (International) "Space"?

Over the relatively short period of time since the introduction of the Internet, several models for self-regulation or "alternative regulation" have been presented. Although the more extreme models have largely become a thing of the past,[81] the debate goes on.[82]

---

[80] WIPO Arbitration and Mediation Center, Frequently Asked Questions: Internet Domain Names, http://arbiter.wipo.int/center/faq/domains.html (last visited Mar. 19, 2006) (explaining the type of disputes handled by WIPO: internet domain names disputes).

[81] *See generally* Barlow, *supra* note 3 (voicing his opposition to regulation in Cyberspace by "Governments of the Industrial World").

[82] Perhaps particularly noteworthy is the discussion between Chicago law professor Jack Goldsmith on the one hand, and the prominent "cyber-libertarians" David Johnson and David Post on the other. The latest contribution being David Post's *Against* "Against Cyberanarchy" (a response to Goldsmith's *Against Cyberanarchy*). *See* Goldsmith, *supra* note 48, at 1199, 1200; David G. Post, *Against* "Against Cyberanarchy," 17 BERKELEY TECH. L.J. 1365, 1366 (2002). There are also, of course, other contemporary or recent proponents of regulation resistance. *See* Shamoil Shipchandler, Note, *The Wild Wild Web: Non-Regulation as the Answer to the Regulatory Question*, 33 CORNELL INT'L L.J. 435, 461-63 (2000) (supporting self-regulation by Internet users and ISPs over government regulation of the Internet); Edward J. Valauskas, *Lex Networkia: Understanding the Internet Community*, FIRST MONDAY (1996), *available at* http://www.firstmonday.dk/issues/issue4/valauskas/; Robert Corn-Revere,

One of the more widely acknowledged proposals for viewing the Internet as a separate space is found in Johnson and Post's *Law And Borders -The Rise of Law in Cyberspace*.[83] The authors argue that the Internet should be viewed as a separate "space,"[84] beyond the regulatory control of individual nations. Moreover, the article suggests that, to the extent that this separate space is to be regulated, such regulations would emerge in the form of self-regulation.[85]

Although this approach does not seem realistic it is, in part, thought-provoking. Due to trust issues, it can safely be assumed that parties to contractual relations would not benefit from the Internet being viewed as a lawless dimension, but as an example it is interesting to consider the alternative in relation to Internet defamation. Leaving Internet defamation unregulated, or if preferred, self-regulated, would carry both desirable and undesirable consequences. The most obvious benefit would be that no "artificial" and more or less flawed rules would have to be created in relation to jurisdictional claims over Internet defamation. There simply would not be such a phenomenon as Internet defamation—statements on the Internet could not be defamatory. Thereby a previously unseen total freedom of expression would be created, in relation to defamatory material. If this is accepted, self-regulation would presumably be achieved as a result of "serious" content providers' desire to remain credible online as well as offline. Further, the users of the Internet would have to be aware of the fact that information provided on the Internet generally should be viewed with a great deal of skepticism and greater care would have to be taken in determining which sources to rely on. The absence of threatening legal consequences would not necessarily lead to a wave of untrue allegations, at least not from serious content providers. Already, people's trust in the accuracy of information is undeniably based, in part, on an evaluation of the source.[86]

Caught in the Seamless Web: Does the Internet's Global Reach Justify Less Freedom of Speech? 13, Briefing Paper of the Cato Institute, July 24, 2002, *available at* http://www.cato.org/pubs/briefs/bp71.pdf; Henry H. Perritt, Jr., *The Internet is Changing the Public International Law System*, 88 KY. L.J. 885, 917 (1999-2000).

[83] Johnson & Post, *supra* note 1, at 1367.

[84] *Id.* at 1367, 1378.

[85] *Id.* at 1367.

[86] *See* Tamar Frankel, *Trusting and Non-Trusting on the Internet,* 81 B.U. L. REV. 457, 469, 477 (2001) (pointing out that "reputable institutions, intermediaries, verifiers and providers of trust services contribute to public trusting on the Internet").

The negative consequences of self-regulation are rather obvious. The fact that a person's reputation can be greatly damaged by information spread via the Internet is beyond intelligent dispute, and if there is no form of regulation, the individual has no chance to prevent damage or get compensation for damage made to his/her reputation. Furthermore, the general feeling of distrust towards the Internet would be amplified. The self-regulation advocates' arguments that people, or "netizens"—the citizens of the "net"—would move away from the disliked parts of the Internet, does not have much effect in relation to defamation.[87] A person is no less defamed by avoiding reading or viewing the defamatory material; just because a person avoids viewing certain websites, it does not mean that he or she runs any less risk of being defamed on those websites.

Taking a somewhat more practical approach, it would be extremely difficult, if not impossible, to come to an international agreement making the Internet a "defamation law-free zone" or a lawless dimension in general. Governments all over the world have passed legislation aimed at regulating the Internet,[88] already existing laws have been applied to activities on the Internet,[89] and international agreements have evolved to regulate Internet behavior.[90] It would be unthinkable to see the govern-

---

[87] David Post & David Johnson, *The New Civic Virtue of the Net: Lessons from Models of Complex Systems for the Governance of Cyberspace* (1997) [hereinafter *Post & Johnson Working Paper*] (unpublished working paper, on file with Stanford Technical Law Review), *available at* http://stlr.stanford.edu/STLR/Working_Papers/97_Post_1/index.htm.

[88] *See, e.g.*, Justin Hughes, *The Internet and the Persistence of Law*, 44 B.C. L. REV. 359, 360 (2003) ("In California, the *state* legislature saw 258 Internet-related bills introduced in its 1999-2000 session, up from four bills in 1994.").

[89] *See* It's in the Cards, Inc. v. Fuschetto, 535 N.W.2d 11, 14 -15 (Wis. Ct. App. 1995) ("Applying the present libel laws to cyberspace or computer networks entails rewriting statutes that were written to manage physical, printed objects, not computer networks or services. Consequently, it is for the legislature to address the increasingly common phenomenon of libel and defamation on the information superhighway.").

[90] *See* The Council of Europe's Convention on Cybercrime, Nov. 23, 2001 (Budapest), E.T.S. No. 185, *available at* http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm (attempting to create a unified international criminal regulatory policy against cybercrime generally, including such cybercrimes as child pornography, copyright infringement, Internet fraud) [hereinafter Convention on Cybercrime]. *See also* Peter Csonka, *The Council of Europe Convention on Cyber-Crime: A Response to the Challenge of the New Age, in* CYBER-CRIME: THE CHALLENGE IN ASIA 303 (Roderic Broadhurst & Peter Grabosky eds., 2005) (explaining that the Council of Europe's Cyber Crime Convention has been signed by 37 states, including the U.S. and Sweden, ratified by eight, and entered into force on July 2004).

ments of the world all agreeing not to apply their laws to the Internet in favor of making the Internet a lawless dimension or leaving it to "self regulation." There must be another well-working means of regulation to replace national laws if states were ever to be inclined to cease making jurisdictional claims over Internet activity. Anything else would arguably be irresponsible. It is argued that the Internet more accurately should be seen as a common thing, rather than "a thing of no one"; thus, states have a common obligation to regulate it, while at the same time observing the interests of other states and the overall common interest of a healthy development of Internet technologies. If this is accepted, large parts of Johnson and Post's ideas carry mainly theoretical value.[91]

Viewing the Internet as a separate "space" also creates severe practical complications. Any model attempting to make the Internet a separate space, with or without separate regulation, would be faced with questions such as: What takes place in the "real" world, and what takes place in the Internet space? Which rules should govern a contract that is formed via the Internet but performed in the real world? Does an act of defamation take place in the real world or in Internet space, if a person receives and prints a defamatory e-mail and only ever reads the printed copy? With these types of questions in mind, I cannot subscribe to Johnson and Post's following statement:

> Treating Cyberspace as a separate "space" to which distinct laws apply should come naturally. There is a "placeness" to Cyberspace because the messages accessed there are persistent and accessible to many people. Furthermore, because entry into this world of stored online communications occurs through a screen and (usually) a password boundary, 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.

---

[91] It is noteworthy that Johnson & Post's article, *Law And Borders—The Rise of Law in Cyberspace* was published in 1996. Since then, numerous things have changed, indicating their article was arguably more realistic at the time of publication. Johnson & Post, *supra* note 1, at 1367.

> 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.[92]

In addition, the statements made by Hughes, Johnson, and Post seem to be much less true today than when they were first made. As Hughes postulated "[t]he Internet is being woven into the rest of reality—technologically, socially, and economically. As our appliances become 'smart,' our houses become 'wired,' our telephony is done with packet-switching, and our cable, telephone, and Internet services bundle and unbundle, will we know when we 'crossed' the cyberspace border?"[93] In other words, will we, in the view of Johnson and Post, be crossing the border and entering "Cyberspace" when getting a beer out of our network-connected fridge?[94]

If the Internet is to be made into a separate legal space, is it necessary to have well thought-out and harmonized rules to determine which disputes are Internet disputes and which disputes are off-line?

B. Adding Public International Law

Darrel Menthe also approaches the Internet as a separate space.[95] In his view, this separate space should be treated as another international space, similar to the high seas, Antarctica, and outer space (i.e., as an independent international space beyond individual nations' regulation):[96]

---

[92] *Id.* at 1379 (footnotes omitted).

[93] Hughes, *supra* note 88, at 371.

[94] After all, since a network-connected fridge can both track food-items and order more items online, it could be argued that the act of taking a beer out of the fridge crosses the border into cyberspace. *See* Leander Kahney, *The Coolest Internet Appliance,* WIRED NEWS, Feb. 12, 1999, *available at* http://www.wired.com/news/technology/0,1282,17872,00.html (describing an Internet-connected refrigerator marketed by Electrolux that has the capability to re-order food items as needed).

[95] Darrel C. Menthe, *Jurisdiction in Cyberspace: A Theory of International Spaces*, 4 MICH. TELECOMM. & TECH. L. REV. 69, 71 (1998). Menthe has explicitly limited his observations to so-called prescriptive jurisdiction or jurisdiction to prescribe laws. From a public international law perspective, determining a state's jurisdiction to prescribe law obviously does just that; it determines to what extent a state can prescribe laws. *Id.* As noted above, from a court's perspective, prescriptive jurisdiction is a factor taken into account in determining the applicable law. *See id.* at 73. In practice, however, states' choice of law rules seldom offend the limits of public international law under the rules for prescriptive jurisdiction. *Id.* at 77.

[96] *Id.* at 83.

> These three physical spaces are nothing at all 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, sovereignless quality. These three, like cyberspace, are international spaces.[97]

Before continuing to explore Menthe's theories, it is necessary to briefly venture out on an exploratory excursion of some jurisdictional theories of public international law. It is frequently said that there are six different grounds for jurisdiction under public international law (sometimes, however, the two grounds based on territoriality are viewed as one, of course, resulting in only five theories):[98] the subjective territoriality principle,[99] the objective territoriality principle,[100] the nationality principle,[101] the passive personality principle,[102] the protective principle,[103] and the universality principle.[104] The relationship between these sometimes overlapping principles are occasionally ranked in order of priority. However, such rankings are prone to be subjectively influenced. The only general observation that realistically could be made is that the territoriality principles and the nationality principles appear to be the most widely accepted.[105]

---

[97] *Id.* at 85.

[98] *See, e.g.* TIM HILLIER, SOURCEBOOK ON PUBLIC INTERNATIONAL LAW 253 (1998) (listing the general principles of jurisdiction).

[99] The subjective territoriality principle of jurisdiction is based on the idea that the offending activity takes place within the territory of the forum. *See* IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 303-06 (5th ed. 1998).

[100] Objective territoriality is jurisdiction based on the idea that the offending activity, while taking place outside the territory of the forum, has its primary effect within the territory of the forum. *See id.*

[101] The nationality principle refers to jurisdiction based on the nationality of the offending party being that of the forum. *Id.* at 306.

[102] *Id.* at 306-07. "According to [the passive personality] principle aliens may be punished for acts abroad harmful to nationals of the forum." *Id.* at 306.

[103] Also referred to as the security principle, the protective principle implicates "jurisdiction [assumed] over aliens for acts done abroad which affect the security of the state." *Id.* at 307.

[104] Under this principle, a state may claim jurisdiction over non-nationals acting inside or outside the state's territory. The principle is, however, only applicable in relation to certain particularly offensive crimes, such as piracy. *Id.* at 307-08.

[105] *See* BROWNLIE, *supra* note 99, at 306, 309-10 (explaining how territorial and nationality principles are closely related, and how their broad principles have been adopted within various European provisions).

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 behavior in these spaces.[106] In doing so, he notes that all three international spaces rely on the nationality principle (for example, the "law of the flag" from maritime law),[107] and he points out that "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."[108] A side issue here is that Menthe acknowledges that placing the focus on the creator of the website is not always the only option: "[W]ebpages are now also created by individuals and companies for others. This makes us ask who 'owns' the page for jurisdictional purposes—the creator or the person on whose behalf it is maintained?"[109] In answering this question he states that "[i]nternational law is not displeased with either answer. If a nation wishes, it can ascribe nationality to all webpages maintained 'on behalf of' its citizens, as well as any webpages actually created (i.e. uploaded) by its citizens."[110] 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."[111]

It is this mixture of the obvious, reasonable, and undisputed on the one hand, and the seemingly reasonable, but outrageously unreasonable on the other, that makes Menthe's article so deceptive. While it is obvious, reasonable, and undisputed that a state cannot regulate what the citizens of another state download, acting in their home state, it is hopefully unthinkable, often unreasonable, and frequently unjust to give exclusivity to the nationality principle. It is submitted that Menthe underestimates the importance of the fact that the so-called cyberspace is non-physical. The non-physical nature of Internet events result in much more direct consequences in the jurisdictions of the world than events occurring in the other three international spaces do. To illustrate the implications of the Internet's non-physical

---

[106] Menthe, *supra* note 95, at 83.
[107] *Id.* at 83-84.
[108] *Id.* at 74.
[109] *Id.* at 93.
[110] *Id.* at 93-94.
[111] *Id.* at 94.

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 behavior in these spaces.[106] In doing so, he notes that all three international spaces rely on the nationality principle (for example, the "law of the flag" from maritime law),[107] and he points out that "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."[108] A side issue here is that Menthe acknowledges that placing the focus on the creator of the website is not always the only option: "[W]ebpages are now also created by individuals and companies for others. This makes us ask who 'owns' the page for jurisdictional purposes—the creator or the person on whose behalf it is maintained?"[109] In answering this question he states that "[i]nternational law is not displeased with either answer. If a nation wishes, it can ascribe nationality to all webpages maintained 'on behalf of' its citizens, as well as any webpages actually created (i.e. uploaded) by its citizens."[110] 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."[111]

It is this mixture of the obvious, reasonable, and undisputed on the one hand, and the seemingly reasonable, but outrageously unreasonable on the other, that makes Menthe's article so deceptive. While it is obvious, reasonable, and undisputed that a state cannot regulate what the citizens of another state download, acting in their home state, it is hopefully unthinkable, often unreasonable, and frequently unjust to give exclusivity to the nationality principle. It is submitted that Menthe underestimates the importance of the fact that the so-called cyberspace is non-physical. The non-physical nature of Internet events result in much more direct consequences in the jurisdictions of the world than events occurring in the other three international spaces do. To illustrate the implications of the Internet's non-physical

---

[106] Menthe, *supra* note 95, at 83.
[107] *Id.* at 83-84.
[108] *Id.* at 74.
[109] *Id.* at 93.
[110] *Id.* at 93-94.
[111] *Id.* at 94.

nature, we can simply consider the difference between placing a defamatory message on the Internet compared to placing the same message on the high sea, Antarctica, or in outer space. When placed on the Internet, the message can be read, and cause damage, in virtually every country on the planet due to the accessibility of material in cyberspace. In contrast, a message placed in an international space is extremely unlikely to ever even be noted by anybody. On a less serious note, it could be noted that, "in space no one can hear you scream,"[112] so there would be no defamation at all under the rules of many, not to say most, countries since the defamatory material entering the mind of a third person is often a requirement for an actionable defamation.[113]

As argued by Goldsmith:

> 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.[114]

Even if "cyberspace" was to be viewed as a separate international space, its non-physical nature motivates the application of both the subjective and the objective territoriality principles in some cases. In addition, in a situation where the security of a state is threatened, by a computer virus for example, it is possible that states would claim jurisdiction based on the protective principle. With this in mind, there is no good reason to rely exclusively on the nationality principle, as far as Internet activities are concerned.

In fact, the better view is to see the non-physical nature of cyberspace as being of such a fundamental importance in the context of jurisdictional issues, that any comparison with physical international spaces is made impossible. Before moving away from the comparison between cyberspace and the three international spaces, at least two more fundamental differences should be

---

[112] A line made famous by the 1979 cult-movie *Alien*.

[113] It is very common that defamation laws require the defamatory message to have entered the mind of a third person for there to be an actionable defamation. *See* RESTATEMENT (SECOND) OF TORTS § 558 (2000) (stating the elements of defamation).

[114] Goldsmith, *supra* note 48, at 1250.

noted. As pointed out by Perritt, the Internet's "low economic barriers of entry . . . distinguish it sharply from outer space regulation [as well as the regulation of Antarctica] and moderately from law of the sea."[115] Further, he notes that "these regulatory regimes focus on state actors rather than private actors, and thus make them unsuitable conceptual models for Internet regulation of many thousands of private actors."[116]

Against this background it would seem that, as far as Internet regulation is concerned, only very limited lessons can be drawn from the development of the three international spaces. One such lesson is that the development of international regulation often, but not always, is fairly slow and effort-intensive.

V. Separate Internet Space, Regulation, and Judiciary

From the above, it should at the very least be obvious that if the Internet is to be treated as a separate legal space, then that space needs to be regulated, not left with the hope of some form of self-regulation emerging. The "community feeling," emphasized by early commentators[117] cannot be relied upon to provide effective regulation of today's Internet. In this context it is submitted that if one proposes self-regulation, it is also necessary to examine from which sources that regulation will emerge, and what the underlying driving forces for the development of these particular forms of regulation are. As Lawrence Lessig illustrated, the absence of governmental control might not at all be in the public's best interest:

> There is nothing to guarantee that the regime of values constituted by code [i.e. Internet architecture] will be a liberal regime; and little reason to expect that an invisible hand of code writers will push it in that direction. Indeed, to the extent that code writers respond to the wishes of commerce, a power to control may well be the tilt that this code begins to take.[118]

In other words, the absence of governmental intervention is no guarantee for liberal self-regulation, but may rather be an invitation to corporate control. However, as noted by Franz C. Mayer,

---

[115] Perritt, *supra* note 82, at 923-24.

[116] *Id.* at 924.

[117] *See, e.g.* Valauskas, *supra* note 82 (suggesting that evolved internet communities have created their own method of regulation that should be considered by legislatures).

[118] Lessig, *supra* note 59, at 548.

Lessig's observation is merely the beginning of a much needed discussion:

> Lessig does not bring his argument to a satisfactory conclusion and does not inquire about the appropriate arena for this kind of regulatory problem: from an international law perspective, the most intriguing aspect of Lessig's book [*Code is Law*] is that he barely mentions international law at all, instead he remains focused on intra-American dichotomies such as West Coast (computer) code versus East Coast (legal) code. If it is correct that liberty in cyberspace will not come from the absence of the state, but from the state of a certain kind, as Lessig claims (p. 5), the question arises whether that authority should be that of one particular state or whether it should not be exercised by the community of states on the international level.[119]

A. Separate Regulation

If rules can be used to properly draw lines between online and offline activities, national laws could be replaced by a uniform code for the Internet legal space. Different theories as to how future Internet regulation will evolve have been presented. Matthew Fagin has made one of the more interesting observations:

> In the future, Internet regulation will require international arrangements that transcend state borders and originate beyond independent state governmental processes; collective efforts that arise either through private enterprise by non-state entities, such as technical-standards bodies, or governmental collaboration. In these areas, the Internet encourages the internalization of international law.[120]

Fagin's point about how "the Internet encourages the internalization of international law" is of particular relevance for this article in that one of the main points being made here is that the complications stemming from the Internet's particular set of characteristics are best addressed through an international instrument.[121]

Another take on the development of a regulative structure is presented in Viktor Mayer-Schönberger and Teree Foster's article *A Regulatory Web: Free Speech and the Global Information Infra-*

---

[119] Franz C. Mayer, *The Internet and Public International Law - Worlds Apart?*, 12 EUR. J. INT'L L. 617, 620 (2001) (the page reference refers to Lessig's book, *Code is Law* (1999)).

[120] Matthew Fagin, Comment, *Regulating Speech Across Borders: Technology vs. Values*, 9 MICH. TELECOMM. & TECH. L. REV. 395, 448 (2003).

[121] *Id.*

structure.[122] In the context of free speech they suggest that "a method should be devised for defining *certain categories of speech that will be subject to regulation*, while at the same time staunchly *protecting all speech not within these categories*."[123] In aiming at a method providing a broad multi-national and multi-cultural consensus they point to the international concept of *jus cogens*.[124] In the Vienna Convention, *jus cogens* is given the following definition: "[A] norm accepted and recognized by the international community of States as a whole as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character."[125]

While, as is reflected in the Cybercrime Treaty,[126] Mayer-Schönberger and Foster's observation that "*jus cogens* represents a corpus of international law rules that are binding upon every nation and every people"[127] is undeniably true, and it provides a good starting point for the first half of their desired aim, it does not provide any solid base as far as the second half of their aim is concerned. It is, as illustrated in practice, possible to gain consensus in defining certain forms of communication that are universally deemed undesirable (e.g., child-pornography). However, that does not mean that all states would be willing to give up their regulation of all other forms of communication (e.g., subversive material). In a world where, in one country, a picture of a woman (otherwise fully dressed) showing her hair is illegal, and pornographic movies are legally shown in picture theatres (be as it may with age restrictions) in another country, it is difficult to imagine the development Mayer-Schönberger and Foster aim at becoming a reality. With this in mind, it could be said that, while it has proven possible to agree upon some things that are illegal, unlawful and undesirable, it is much harder, not to say impossible, to agree upon what otherwise is in fact legal, lawful and desirable.

---

[122] Viktor Mayer-Schönberger & Teree E. Foster, *A Regulatory Web: Free Speech and the Global Information Infrastructure*, 3 MICH. TELECOMM. & TECH. L. REV. 45 (1997).

[123] *Id.* at 57 (emphasis added).

[124] *Id.* at 57-58.

[125] Vienna Convention on the Law of Treaties, May 23, 1969, art. 53, 8 I.L.M. 679, 698-99.

[126] Convention on Cybercrime, *supra* note 90.

[127] Mayer-Schönberger & Foster, *supra* note 122, at 59.

B. Separate Judiciary

Even with a regulatory scheme in place, it is, of course, also necessary to have some organ supervising compliance with any separate rules and adjudicating disputes arising from those rules. Such a body must further have some effective means for ensuring that its decisions are enforced.

International courts are not a new idea, but so far they exist only in very limited and specialised contexts.[128] A specific court responsible for all Internet activities is unlikely to ever become a reality. At the same time, however, one cannot ignore the development of Online Dispute Resolution (ODR). ODR, is best described as a branch of Alternative Dispute Resolution (ADR).[129] Internet technology is not only the cause of disputes, but can also be a means for dispute resolution. There is a range of ADR schemes, such as in-house complaints offices, mediation and arbitration, available online.[130] A full discussion of these schemes, their advantages and disadvantages and so on, is clearly beyond the scope of this article.[131] However, in the context of a separate judiciary for Internet conflicts, the experiences from ODR should not be overlooked.

More importantly, ODR might be the most effective remedy for one of the problems created by Internet communication's particular set of characteristics. Even the most cleverly drafted private international law rules simply cannot solve the problem of the imbalance between the ease and cost-effectiveness of cross-border contacts on the one hand, and the difficulty and expense of solving cross-border disputes on the other. Unless we want to make it more difficult and expensive to enter into cross-border contacts, which would defeat very important benefits of the Internet, we have to create easier access to dispute resolution. The costs involved in court proceedings fit uneasily with the small values involved in many online contracts, and many, not to say most, court systems are notoriously slow. In fact, it could be said that the legal system does not provide for any reasonable dispute reso-

---

[128] For example, the International Court of Justice, International Tribunal for the Law of the Sea and the Bosnia War Crimes Tribunal.

[129] Lee Bygrave, *Online Dispute Resolution – What it Means for Consumers,* 4 INTERNET LAW BULLETIN Vol. 81, 8 (2002).

[130] *See, e.g.,* http://www.ombuds.org/center/onlineadr.html (last visited Mar. 19, 2006) (providing links to a range of different ODR websites).

[131] There has been a range of material published on this topic. *See, e.g.,* Bygrave, *supra* note 129, at 1; ETHAN KATSH & JANET RIFKIN, ONLINE DISPUTE RESOLUTION: RESOLVING CONFLICTS IN CYBERSPACE (2001).

lution option in relation to many small value contracts. This in turn could lead to the suggestion that alternatives must be developed in order to provide an appropriate level of access to justice.

VI. A Model for Placing Borders Around Internet Defamation

To be useful, any exploration of the possibilities of treating specific aspects of Internet activities separately, with separate regulation and judicial system, should focus on one specific legal area at a time. As each legal area gives rise to its own set of concerns, it would be impractical to address all areas in one study. This part of the article outlines one possible approach to placing borders around Internet defamation.

As noted above, a defamation dispute is essentially an exercise in balancing freedom of expression and the right of reputation. It has been noted that "[t]he most obvious area of law where the Internet is unlikely to produce substantial harmonization of legal norms in the medium term is freedom of expression."[132] While this claim makes sense as far as absolute worldwide harmonization is concerned, it becomes incorrect when the term "worldwide" is not taken literally. In a sense, there has already been substantial harmonization in the area of freedom of expression. The *International Covenant on Civil and Political Rights* (ICCPR),[133] which could be said to be a codification of parts of the 1948 Universal Declaration of Human Rights, represents a minimum standard of freedom of expression, as well as the protection of reputation, in signatory states. In accordance with Article 19:

> 1. Everyone shall have the right to hold opinions without interference.
>
> 2. *Everyone shall have the right to freedom of expression*; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

---

[132] Hughes, *supra* note 88, at 364.

[133] International Covenant on Civil and Political Rights, Mar. 23, 1976, *available at* http://www.ohchr.org/english/law/pdf/ccpr.pdf [hereinafter ICCPR]. As of the 13th of December 2005, no less than 154 states (including Sweden, Australia, the PRC and the US) have become parties to the ICCPR. Office of the United Nations High Commissioner for Human Rights, *Ratifications and Reservations: International Covenant on Civil and Political Rights*, *available at* http://www.ohchr.org/english/countries/ratification/4.htm (last visited Mar. 19, 2006).

> 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
> (a) For *respect of the rights or reputations of others;*
> (b) For the protection of national security or of public order (ordre public), or of public health or morals.[134]

This Article illustrates that freedom of expression is a fundamental human right, but it also allows for restrictions of this right. Since the ICCPR also establishes a minimum standard of rights directly opposite to freedom of expression,[135] it is submitted that the ICCPR and its associated documents[136] establish the outer limits of the allowable spectrum of the balancing between freedom of expression and competing rights. Each signatory state is allowed to strike its own balance between freedom of expression and competing rights, as long as that balance falls within the spectrum provided for under the ICCPR. Using the defamation laws of Australia and the United States as examples, it can be noted that Australia has placed a greater emphasis on the right of reputation, while the United States has placed a greater emphasis on freedom of expression; however, both states' balances arguably fall within the ICCPR's allowable spectrum. Consequently, from this perspective, harmonization of the substantive law has occurred to a certain extent. Further, it is interesting to note that, while not binding on the states, the First Optional Protocol[137] of the ICCPR provides for a form of adjudication by a supranational body—the United Nation's Human Rights Committee (UNHRC). Although so far not all of the states that have signed the ICCPR have signed the First Optional Protocol,[138] this is an example of

---

[134] ICCPR, *supra* note 133, at 6 (emphasis added).

[135] *See, e.g., id.* at 5-6 (noting the existence of limitations in Article 19, and explicitly stating in Article 17 that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation").

[136] Such documents include the general comments and individual decisions under the Optional Protocol to the ICCPR.

[137] Optional Protocol to the International Covenant on Civil and Political Rights, March 23, 1976, *available at* http://www.ohchr.org/english/law/pdf/ccpr-one.pdf.

[138] As of the 13th of December 2005, 105 states have become parties to the First Optional Protocol (including Sweden and Australia). Office of the United Nations High Commissioner for Human Rights, *Ratifications and Reservations: Optional Protocol to the International Covenant on Civil and Political Rights,* http://www.ohchr.org/english/countries/ratification/5.htm (last visited Mar. 19, 2006).

harmonization of substantive law under the supervision of a supranational body.

The UNHRC has already received communication asking it to determine a dispute relating to Internet defamation. Having lost in the High Court of Australia, the team of lawyers sought a fresh avenue to challenge Australia's jurisdictional claim in the defamation dispute between Joseph Gutnick and Dow Jones. The author of the allegedly defamatory article, Bill Alpert, has petitioned to the UNHRC in an attempt to have the Australian standpoint declared to be in violation of the ICCPR.[139] This was possible due to the fact that Australia, in contrast to Mr. Alpert's home country, the United States of America, has signed the First Optional Protocol (OP-1)[140] of the ICCPR. It may here be mentioned that the OP-1 thus does not allow Dow Jones (a business entity) to lodge an application, and an application can only be lodged against the conduct of state parties, in this case Australia (in contrast to the plaintiff of the disputed action, Mr. Gutnick). The UNHRC has not yet dealt with the matter.

VII. A Model Convention to Regulate Cross-Border Internet Defamation Arising out of Mass-Communication

To provide a starting point for how borders may be placed around Internet defamation, a suggested Model Convention to regulate cross-border Internet defamation arising out of mass-communication is outlined below.

This Model takes the existing framework provided through the ICCPR and the UNHRC as its point of departure.[141] Cross-border disputes relating to situations where material is lawful from where it is made available, but unlawful in some other state, and that latter state is asked to exercise jurisdiction over the person responsible for the material being made available, are to be decided by a special sub-panel of the UNHRC. In contrast, disputes relating to situations where the relevant material is unlaw-

---

[139] Fergus Shiel, *Journalist Appealing to UN Over Gutnick Case*, The Age, Apr. 17, 2003, http://www.theage.com.au/articles/2003/04/16/1050172650855.html.

[140] The Optional Protocol to the International Covenant on Civil and Political Rights (CCPR-OP1), Dec. 16, 1966.

[141] *See* Human Rights Library, *International Covenant on Civil and Political Rights*, *available at* http://www1.umn.edu/humanrts/instree/b3ccpr.htm (last visited Mar. 19, 2006) (using a similar layout of Sections, Articles, and subdivisions).

ful, both where it was uploaded and where it was downloaded, remain matters for the national courts.

Disputes brought before the special Internet Defamation Panel of the UNHRC are to be determined by reference to the minimum standard for freedom of speech and right of reputation set by the ICCPR. This way, the Model ensures a high level of freedom of speech, as well as a reasonable level of protection for the right of reputation, in relation to the types of Internet communication it covers.

Section I: Aim, Scope, and Accession

Article 1

This Convention is to regulate cross-border Internet defamation arising out of mass-communication.

Elsewhere,[142] I have discussed the potential benefits of rules being technology neutral. However, if we are to draft an instrument that separates online behavior from offline behavior, then such an approach is, of course, not possible. On the other hand, we can not allow rules to be too technology-specific either. This proposal is therefore aimed at all forms of communication used for mass-communication via the Internet.

Article 2

1. Criminal defamation is not to be governed by this Convention.

2. Paragraph one does not prevent the application of this Convention to civil liability arising as a consequence of criminal defamation.

As the issue of defamation is a politically sensitive area of law, particularly as far as criminal defamation is concerned, it was deemed suitable to refrain from regulating the criminal aspects of defamation law. However, as is made clear in Article 2(2), this is not to prevent the application of the Model to civil claims associated with criminal actions, as long as the requirements set out in the Model are fulfilled.

Article 3

This Convention is open for signature by states that have previously signed, and where required ratified, both of the following international instruments:

The International Covenant on Civil and Political Rights; and

The Optional Protocol to the International Covenant on Civil and Political Rights.

---

[142] Svantesson, *supra* note 2, at 96-98.

As the possibility of placing reliance on the practice of the UN Human Rights Committee, or a sub-panel of the UN Human Rights Committee, is a central function of the Model, it can only be opened to states that already provide for such a procedure. Therefore, the Model is open only to states that have already signed and ratified the *International Covenant on Civil and Political Rights* and the *Optional Protocol to the International Covenant on Civil and Political Rights*.

Although Article 3 sets up rather strict requirements for accession, a large number of states nevertheless qualify. There are, however, some rather important exceptions, such as the People's Republic of China, the UK, and the US, because these states have chosen not to sign the *Optional Protocol to the International Covenant on Civil and Political Rights*.[143]

Section II: Interpretation

Article 4

For the purpose of this Convention the following terms bear the meaning outlined in this Article:

"foreign defendant" means a defendant that "acted" outside the jurisdiction of the court;

"Internet defamation" means alleged defamation occurring as a consequence of material being communicated by the use of the Internet;

"mass-communication" means communication that is not aimed at one specific individual;

"the Panel" means the UNHRC Panel on Internet Defamation (to be created).

The first problem facing an attempt to regulate Internet activities separately is, as hinted at above, the difficulty of separating what constitutes Internet activity and what does not constitute Internet activity. Such a distinction can be drawn in many different ways. It is submitted that, in this context, the best way is to focus on whether the communication took place, wholly or in part, via the Internet. Thus, the focal point is placed on the mode of communication rather than the medium used by a third person in having the allegedly defamatory material enter his or her mind. The consequence of this is, for example, a situation where the defamatory material is posted on a website, downloaded and printed, and then the defamation is classed as Internet defama-

---

[143] CCPR-OP1, *supra* note 140.

tion even though the person reading the defamatory material did not read it on the screen, but from a printed document.

Such a reference point may be undesirably inclusive, so further refinement is called for. There seems to be no real reason why one-to-one communication should be dealt with under this instrument simply due to the fact that it occurs online. Thus, communication using applications such as e-mail and Voice over IP (VoIP) would not fall under this Model Convention unless it is used to communicate to more than one person at the time.

Article 4 also makes clear the meaning of the terms "foreign defendant" and "the panel." However, it should be noted that the exact construction of the panel requires further discussion.

Article 5

1. Subject to Paragraphs 4 and 5, "the place where the defendant acted" means the place where the defendant is habitually resident.

2. A natural person shall be considered to be resident –

if that person is resident in only one state, in that state;

if that person is resident in more than one state,

in the state in which that person has his or her principal residence; or

if that person does not have a principal residence in any one state, in each state in which that person is resident.

3. For the purposes of this Article, an entity or person other than a natural person shall be considered to be habitually resident in the state where it has its principal place of business.

4. If there is no, or merely a coincidental, relevant nexus between the defendant's injuring act and the place identified under Paragraphs 1-3, "the place where the defendant acted" shall be deemed to be the place that has the most substantial connection with the defendant's act.

5. Where a party attempts to break existing connecting factors with one state or attempts to create connecting factors with another state, in order to circumvent actual natural connections with "the place where the defendant acted," as defined in Paragraphs 1-4, such attempts shall be null and void.

Article 5 defines the key concept of "the place where the defendant acted." The motivation for focusing on "habitual residence," instead of, for example, domicile or nationality, is found in its international recognition. As noted by Nygh, although never defined, "[t]he term 'habitual residence' is an old standby of the

Hague Convention with a history of over 100 years."[144] In contrast to *domicile*, it further has the advantage of not being associated with differing national meanings.

The definition of the residence of "an entity or person other than a natural person" as being the "state where it has its principal place of business" is supported, for example, by the Australian Law Reform Commission,[145] but obviously only represents one possible option. However, it would seem likely that the principle place of business ordinarily is of more relevance than, for example, the place of incorporation.

While applying to the question of jurisdiction, Article 5(4) has its origins in the flexibility of the applicable choice of law rules of, for example, the UK and Hong Kong SAR,[146] and the US.[147] It is necessary to leave room for these sorts of exceptions in certain cases. If, for example, a publishing company is located in Norway, but the allegedly defamatory article is researched, written, uploaded from South Africa onto a server located in South Africa, and the article is concerned with events and people in South Africa, there may be reasons to focus on the actual "place where the defendant acted" rather than on the place of habitual residence. Obviously, both the advantage and the disadvantage of this Article is the extent of its flexibility.

Today's technology with its portability and high level of anonymity provides a perfect environment for so-called fraudulent evasions or *fraude à la loi*.[148] For example, connecting factors can

---

[144] Peter Nygh, *The Preliminary Draft Hague Convention on Jurisdiction and Foreign Jurisdiction and Foreign Judgments in Civil and Commercial Matters, in* INTERNATIONAL CONFLICT OF LAWS FOR THE THIRD MILLENNIUM: ESSAYS IN HONOR OF FRIEDRICH K. JUENGER 271 (Patrick J. Borchers & Joachim Zekoll eds., 2001).

[145] *Choice of Law*, ALRC 58, § 6.57 (1992), *available at* http://www.austlii.edu.au/au/other/alrc/publications/reports/58/58.pdf.

[146] *See* Chaplin v. Boys, 1971 L.R. 356, 357 (A.C. 1969) ("Given the general rule the necessary flexibility can be obtained through segregation of the relevant issue and consideration whether, in relation to that issue, the relevant rule ought as a matter of policy to be applied.").

[147] *See* RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 150 (1969) (explaining that rights and liabilities from defamatory matter are determined by the local law of the state with the most significant relationship to the occurrence and the parties under the principles stated in § 6). For an illustration of how the factors listed in § 6 are applied in a cross-border defamation case, *see* Hammer DeRoburt v. Gannet Co., 83 F.R.D. 574, 578-79 (1979) (listing and discussing each of the § 6 factors in turn).

[148] *Fraude à la loi* is the "fraudulent evasion of a statute or provision." WIPO, *Ad Hoc* Informal Meeting on the Protection of Audiovisual Performances (Nov. 6-7, 2003) (Geneva).

be created and/or broken by moving a website from one server to another, changing the physical location of a server, or simply by downloading something onto your laptop after crossing the geographical border to another country. The need to prevent such practice has gained remarkably little attention in discussions of Internet regulation. Article 5(5) represents a safety mechanism to prevent perversion of the Model's application through fraudulent evasion, for example, through a publisher seeking to make a particular location appear to be the appropriate focal point instead of the location that should be the focal point in the absence of the *fraude à la loi*.

Section III : Jurisdiction

Article 6

1. A court of a Convention Sate may only claim jurisdiction over a foreign defendant, in a matter falling within the scope of this Convention, where it is satisfied that:

a) the plaintiff can establish a prima facie case against the defendant under the law of the forum; and

b) the plaintiff can establish a prima facie case against the defendant under the law of the place where the defendant acted.

2. Where the plaintiff has satisfied the court that it can establish a prima facie case against the defendant under the law of the forum, it is presumed that it also has such an action under the law of the place where the defendant acted.

Article 6 is one of the two key provisions of the Convention Model. It draws upon the so-called double actionability test expressed in the old English case *Phillips v. Eyre*:

As a general rule, in order to found a suit in England for a wrong alleged to have been committed abroad, two conditions must be fulfilled. First, the wrong must be of such a character that it would have been actionable if committed in England . . . Secondly, the act must not have been justifiable by the law of the place where it was done.[149]

This rule has been criticized and recently abolished as the choice of law rule in Australia and some other common law jurisdictions.[150] Yet that does not prevent it from being a useful point

---

[149] Phillips v. Eyre, 6 L.R.-Q.B. 1, 28-29 (1870); *see also* DICEY AND MORRIS ON THE CONFLICT OF LAWS 1560 -65 (Lawrence Collins et al. eds., 13th ed. 2000).

[150] The double actionability test is still relevant in relation to actions in defamation in the UK, although it was abandoned in relation to other matters. *See* Private International Law (Miscellaneous Provisions) Act, 1995, c. 16 §§ 10-13 (Eng.).

of departure for the Model proposed here. The idea is that national court will continue to deal with those disputes where the defendant has acted contrary to the law of both the place it acted and the place where the action is brought. Such disputes are not particularly controversial and may be dealt with under national law.

Article 6 does, however, also contain the weakest part of the proposed Model—a national court will be asked to evaluate the validity of the claim already at the stage of determining whether it can claim jurisdiction. While this is not an entirely unique situation, it is nevertheless a problem. The problem is partly limited by the presumption that, where the plaintiff has satisfied the court that he, or she, can establish a prima facie case against the defendant under the law of the forum, he or she also has such an action under the law of the place where the defendant acted. This also highlights that the burden of proof is divided between the parties. For the court to claim jurisdiction, the plaintiff has to show that it has a prima facie case against the defendant under the law of the forum. To avoid the court claiming jurisdiction, where the plaintiff has succeeded in proving that he, or she, has got a prima facie case against the defendant under the law of the forum, the defendant has to show that the plaintiff does not have a prima facie case against him, or her, under the law of the place where the defendant acted.

Ordinarily, the court will be in a good position to evaluate whether the plaintiff has succeeded in proving that he, or she, can establish a prima facie case against the defendant under the law of the forum. However, expert evidence is likely to be required to establish whether or not the defendant has shown that the plaintiff does not have a prima facie case under the law of the place where the defendant acted.

Article 7

The Panel has jurisdiction to hear all disputes involving cross-border Internet defamation arising out of mass-communication.

Article 7 makes clear that, even where a plaintiff could have brought an action before a national court, it may bring the matter, falling within the scope of the proposed Model, before the Panel.

Section IV: Operation of the Panel

Article 8

1. The Panel is to decide the dispute by reference to whether a national court, of a state having signed the ICCPR and the OP-1, would be in violation of its undertaking if it had jurisdiction over

the parties and did not find in favor of the plaintiff in the circumstances of the case.

2. Where the Panel concludes that a national court, of a state having signed the ICCPR and the OP-1, would be in violation of its undertaking if it had jurisdiction over the parties and did not find in favor of the plaintiff in the circumstances of the case, it is to decide in favor of the plaintiff and decide on an appropriate remedy and division of costs.

3. Where the Panel concludes that a national court, of a state having signed the ICCPR and the OP-1, would not be in violation of its undertaking if it had jurisdiction over the parties and did not find in favor of the plaintiff in the circumstances of the case, it is to decide in favor of the defendant and decide on an appropriate division of costs.

Article 8 is the second key provision of the Convention Model. It is aimed at establishing a minimum standard of protection both in relation to the right of reputation and in relation to freedom of speech. In doing so, it draws upon the balance between these fundamental human rights struck in the ICCPR.

Under Article 8, the Panel will only ever find in the plaintiff's favor where not doing so would mean that the minimum standard of protection for the right of reputation would be violated. In other words, as far as mass-communicated material on the Internet is concerned, the balance struck between the right of reputation and freedom of speech would be as favorable to the freedom of speech as is allowable under the ICCPR.

Section V: Entry into force

Article 9

This Convention shall enter into force when signed, and where required ratified, by at least two states, both of which meet the criteria set out in Article 3.

Article 9 simply outlines when the proposed Convention Model is to come into force. There appears to be no reason why the Convention would not enter into force if at least two states want it to do so.

Section VI: Other provisions

Article 10

The Panel shall report its judgments. In particular, the judgments shall be made available, free of charge, on the World Wide Web.

In order to establish an appropriate balance between freedom of speech and the right of reputation, it is important that the Panel's

decisions are made public. As is demonstrated, for example, through the World Legal Information Institute successful models for online, free of charge, publication of legal materials can be found.

7. Concluding Remarks

This article has illustrated how borders currently are being placed on the Internet through a combination of jurisdictional claims and technical developments. It has also made clear that these borders are likely to transform the Internet from an open and virtually global communications network, into something that more resembles our physical world divided by borders of different kinds.

It has been submitted that in light of the threat of such an undesirable development, we must re-examine the possibility of treating the Internet as a separate space. Such a space must be approached in a context-specific manner. In other words, we must deal with each legal issue separately. Furthermore, if states ever are to be inclined to give up their claims to regulating the Internet, alternative forms of regulation must be put in place; relying on self-regulation is not an option today. In addition, an appropriate judiciary must be put in place and effective enforcement must be ensured.

As far as defamation is concerned, a well-recognized regulatory framework is already in place through the ICCPR, and an adjudicative body exists in the UNHRC. Drawing upon these existing mechanisms, a Convention Model to regulate cross-border Internet defamation arising out of mass-communication was presented.