JOGI FÓRUM PUBLIKÁCIÓ

www.jogiforum.hu

Krisztina Turza

Electronic Commerce Law (LWN125) Research Paper

Semester 1, 2013

2013. május 12.

Introduction

This paper concludes the following research question:

"Courts in many countries have been grappling with the question of which state may properly exercise jurisdiction over the parties to cyberspace transactions. Through their decisions, the jurisdictional principles applying to the Internet are beginning to emerge."

The global nature of the Internet, which transcends national and state boundaries, raises complex jurisdictional issues.[1] Cyberspace is a venue with very special problems in the field of regulation because it poses a serious challenge to our existing legal system as global computer-based communications that cut across territorial borders create jurisdictional conflicts that undermine the feasibility and legitimacy of applying laws based on geographic boundaries.[2] As the Internet is accessible from almost anywhere in the world, transactions whose real world analogues would have been restricted to only one or two jurisdictions may potentially be subject to multiple jurisdiction. This paper considers jurisdictional issues associated with cyberspace in comparison with traditional jurisdiction rules. It also examines the law of defamation in selected English, Australian, U.S., and Canadian case law emerging from cyberspace.

Characteristics of cyberspace

Cyberspace is an amorphous space that does not occupy a set of physical or geographic location in which individuals, corporations, communities, governments and other entities can exist within and beyond the borders of the nation state in an instantaneous, contemporaneous or ubiquitous manner.[3] In technical terms, the Internet is essentially a 'decentralised, self-maintained

[1] A. Fitzgerald, B. Fitzgerald, C. Cifuentes, P. Cook, *'Going Digital; Legal Issues for e-commerce, software and the Internet'* (2002, Lexis Nexis Butterworths), pg 245.

[2] S. Anil, *'Cyberspace and the law of defamation: developing a workable model'*, Computer and Telecommunications Law Review, 2001, 7(7), 175-183.

[3] B. Fitzgerald, '*Software as Discourse: The Power of Intellectual Property in Digital Architecture*' (2000) 18 Cardozo Arts and Entertainment Law Journal 337, 353 fn 52. Gutnick (2002) 194 ALR 433. L. Lessig, '*The Law of the Horse: What Cyberlaw Might Teach*' (1999) 113 Harvard Law Review 501. D. Johnson and D. Post, '*Law and Borders - The Rise of Law in Cyberspace*'

telecommunications network'[4] or a 'decentralised, global medium of communication' comprising a 'global web of linked networks and computers'[5] and can be described as 'having the characteristics of a newspaper, a television station, a magazine, a telephone system, an electronic library and a publishing house.'[6]

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.[7] What we call 'cyberspace' can be characterized as a multitude of individual, but interconnected, electronic communications networks. The Internet is not a physical object with a tangible existence, but is itself a set of network protocols that has been adopted by a large number of individual networks allowing the transfer of information among them. Cyberspace enables communication between people who do not and perhaps cannot know the physical location of the other party. Locations within cyberspace are the 'addresses' of the machines that route information and messages. The system is indifferent to the physical location of these routing machines because there is no necessary connection between an Internet address and a physical jurisdiction. Any attempts to control the flow of electronic information across geographical borders and legal jurisdictions onto cyberspace are likely to be futile as information, via the form of bits and bytes, can easily 'enter' into any sovereign's territory without any realistic prospect of detection.[8] The volume of electronic communications crossing territorial boundaries is beyond the resources of any government authorities to exercise meaningful control[9] due the nature of electronic transactions of 'near infinite boundary' with territorial jurisdictions.[10] As a result, cyberspace has radically undermined the traditional legal rights and responsibilities that are founded on the basis of territorial space by destroying the link between geographical location and

---

(1996) 48 Stanford Law Review 1367.

[4] *Dow Jones & Company, Inc v Gutnick* [2002] HCA 56, para 80.

[5] *American Civil Liberties Union v Reno* 929 F Supp 824, 831 (ED Pa 1996).

[6] K. Siver, '*Good Samaritans in Cyberspace*' (1997) 23 Rutgers Computer and Technology Law Journal 1, 3. A. Fitzgerald, *'Going Digital: Legal Issues for Electronic Commerce, Multimedia and the Internet'* (Prospect Media Pty Ltd, 1998).

[7] D. R. Johnson, '*Travelling in Cyberspace'*, Legal Times, Apr. 3, 1995, at 26. L. Lessig, '*The Zones of Cyberspace*', 48 Stan. L. Rev. 1403, 1408.

[8] S. Anil, '*Cyberspace and the law of defamation: developing a workable model'*, Computer and Telecommunications Law Review, 2001, 7(7), 175-183.

[9] S. Anil, '*Cyberspace and the law of defamation: developing a workable model'*, Computer and Telecommunications Law Review, 2001, 7(7), 175-183.

[10] See Prof. P. Martin, NewJuris Electronic Conference (September 22, 1993) at p. 13.

the power of a local sovereign to enforce law within its jurisdiction and to determine which law should apply.[11]

The world of cyberspace has no physical existence beyond the computers on which it resides but this fact does not keep it from being real because it is a world of information that have real consequences and a real existence. It is the interplay between the vast number of largely centralized individual networks and the decentralized Internet work through which they can communicate that will prove to be a fundamental importance in determining the efficacy with which state law can be imposed on individual network communities. The key feature of the Internet is that the net is set up to operate logically rather than geographically.[12] The cyberspace is considered an electronic place that conforms to our understanding of the real world, with private spaces such as websites, email servers, and fileservers, connected by the public thoroughfares of the network connections.[13]

There is a need to distinguish between actions taking place in cyberspace without any effect on real world and actions taking place in cyberspace and having effects upon real life. Cyberspace cannot exist out of a state's sovereignty.[14] Geographical borders are of primary importance in determining legal rights and responsibilities. 'All law is prima facie territorial'[15] and the laws of a particular jurisdiction normally only have effect within the boundaries of that jurisdiction.[16] In the geographic world, borders for law make sense because their relationship to the development and enforcement of law is logically based on a number of factors,[17] such as power to exercise sovereignty that is the control over a physical space. The geography of the Internet

---

[11] See D. R. Johnson and D. G. Post, '*The Rise of Law on the Global Network* in Borders in Cyberspace - *Information Policy and the Global Information Infrastructure*' (The MIT Press, 1997).

[12] G. I. Zekos, '*State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction*', International Journal of Law and IT (2007) 15 (1).

[13] See *Voyeur Dorm v. City of Tampa*, 265 F.3d 1232 (11th Cir. 2001) (stating that a live sex show broadcast over the Internet from a house in Tampa did not violate a local zoning ordinance prohibiting adult entertainment, because the entertainment was not physically provided at that location, but sent to remote users).

[14] G. I. Zekos, '*State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction*', International Journal of Law and IT (2007) 15 (1).

[15] See *American Banana Co. v. United Fruit Co.*, 213 U.S. 347, 357 (1909).

[16] C. Reed, *Internet Law*, Second Edition (2004) Cambridge University Press, pg. 217.

[17] D. R. Johnson and D. G. Post, '*The Rise of Law on the Global Network in Borders in Cyberspace*' - *Information Policy and the Global Information Infrastructure* (The MIT Press, 1997).

however is purely virtual as it pays no heed to geographical or political boundaries,[18] therefore when courts attempt to apply traditional territorial based jurisdictional rules to cyberspace; the situation becomes even more complicated, due to the lack of geographical or physical boundaries.[19]

A state has authority to regulate the transmittal of information across its borders and the use of that information by individuals within its territory.[20] The territoriality principle grants a state jurisdiction to prescribe law with respect to conduct that, wholly or in substantial part, takes place within its territory. States rely on the territoriality principle to regulate in-state hardware and software used in Internet communications. Moreover, States rely on the effects principle in applying their domestic laws to out-of-state Internet activity. Electronic activity occurs across multiple jurisdictional boundaries. The effects of online activities are not tied to geographic locations but can be felt by people living in a specific place.[21]

Although no government can monopolise legislation for the entire cyberspace, authorities are likely to claim that they must regulate the new online phenomena on a territorial basis. However, the rise of responsible self-regulatory institutions within cyberspace will weigh heavily against arguments that cyberspace is 'lawless' and thus regulation of online activities based on physical jurisdiction is necessary.[22]

Rules of jurisdiction

[18] C. Reed, '*Internet Law*', Second Edition (2004) Cambridge University Press, pg. 217.

[19] A. Fitzgerald, B. Fitzgerald, C. Cifuentes, P. Cook, '*Going Digital; Legal Issues for e-commerce, software and the Internet*' (2002, Lexis Nexis Butterworths), pg 245.

[20] S. Wilske & T. Schiller, '*International Jurisdiction in Cyberspace: Which States May Regulate the Internet?*', 50 Fed. Comm. L.J. 117, 129-42 (1997).

[21] J. Boyle, '*Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*', 66 U. Cin. L. Rev. 177, 178-83 (1997) ("the technology of the medium, the geographical distribution of its users, and the nature of its content all make the Internet specially resistant to state regulation"). J. R. Reidenberg, '*Governing Networks and Rule-Making in Cyberspace*', 45 Emory L.J. 911, 917-19 (1996) ("*the Internet's infrastructure creates 'visible borders' that replace national borders in regulating online interactions*").

[22] S. Anil, '*Cyberspace and the law of defamation: developing a workable model*', Computer and Telecommunications Law Review, 2001, 7(7), 175-183.

Before we examine some of the views on the differences or even similarities around cyberspace jurisdiction vs. 'real world jurisdiction', we need to review the traditional concept thereof. The rules of jurisdiction can be divided into the following categories: (i) the jurisdiction to prescribe (or 'legislative' jurisdiction); (ii) the jurisdiction to adjudicate (or 'judicial' jurisdiction); and (iii) the jurisdiction to enforce (or 'enforcement' jurisdiction).[23] The jurisdiction to prescribe 'is the right of a state to make its law applicable to the activities, relations, the status of persons, or the interests of persons in things.'[24]

The jurisdiction to adjudicate refers to the power of a state to require a defendant to appear before a court and defend a claim. In most Commonwealth common law countries and the U.S., the courts' ability to adjudicate a dispute arises when the defendant is properly served with a writ.[25] At common law, the writ may be personally served on a person who is present within the jurisdiction[26] or, if the person is outside the jurisdiction, service outside of jurisdiction may be allowed. The service of a foreign writ is illegal in some jurisdictions,[27] and even if the defendant is legally served outside the forum state's jurisdiction, the defendant may choose not to enter a court appearance.

The enforcement jurisdiction of courts is perhaps even more limited than their adjudicative jurisdiction. The courts of one country will not always enforce the judgements of another country.[28] This is manifested in rules which do not give a court jurisdiction in certain cases, as well as rules that permit courts to decline jurisdiction in order to allow a foreign court to exercise its jurisdiction (known as the principle of forum non-conveniens). States enact laws to voluntarily limit the jurisdiction of their courts both unilaterally and multilaterally.[29] In the U.S.,

---

[23] M. Saadat, '*Jurisdiction and the Internet after Gutnick and Yahoo!*', 2005 (1) The Journal of Information, Law and Technology.

[24] D Menthe, "Jurisdiction in Cyberspace: A Theory of International Spaces", 4 *Mich. Telecomm. Tech. Law Rev*69 (1998).

[25] M. Saadat, '*Jurisdiction and the Internet after Gutnick and Yahoo!*', 2005 (1) The Journal of Information, Law and Technology.

[26] *Laurie v Carroll* (1958) 98 CLR 310.

[27] For example, Switzerland does not permit a writ to be served by international post, considering it a breach of its sovereignty.

[28] M. Saadat, '*Jurisdiction and the Internet after Gutnick and Yahoo!*', 2005 (1) The Journal of Information, Law and Technology.

[29] M. Saadat, '*Jurisdiction and the Internet after Gutnick and Yahoo!*', 2005 (1) The Journal of Information, Law and Technology.

service of a state writ may only be done in accordance with the limitations of the U.S Constitution.[30] Further, the member states of the European Union have passed the Brussels Regulation[31] ('Regulation'), which prevents overlapping assertions of jurisdiction by the Member States[32] by providing rules for determining which court shall have jurisdiction. The Regulation stipulates that 'the rules of jurisdiction must be highly predictable and founded on the principle that jurisdiction is generally based on the defendant's domicile and jurisdiction must always be available on this ground save in a few well-defined situations in which the subject –matter of the litigation or the autonomy of the parties warrants a different linking factor. The domicile of a legal person must be defined autonomously so as to make the common rules more transparent and avoid conflicts of interest.[33] To give effect to this aim, it further provides[34] that 'subject to this Regulation, persons domiciled in a Member State shall, whatever their nationality, be sued in the courts of that Member State'. In this sense, the Regulation provides a degree of certainty for Europeans entering into inter-state business transactions. For persons not domiciled in a member state, however, the national rules of jurisdiction continue to apply.[35] Some jurisdictions may decline jurisdiction in accordance with the principle of *forum non-conveniens,*[36] which reflects that often multiple states will have a basis for claiming jurisdiction, but that one state may be a 'more appropriate forum',[37] or 'clearly inappropriate forum'.[38] As this paper will examine some of the Internet defamation cases, it is worth to mention that the Regulation provides for a number of exceptions to the abovementioned general rule; one of these is Article 5(3), which states that in matters relating to tort, delict or quasi-delict,[39] a person domiciled in a Member State may be sued in another Member

[30] U.S. states have passed 'long-arm' statutes in order to facilitate the issue of writs for persons located in other states (both U.S. and overseas). The U.S. Supreme Court sanctioned these statues in *International Shoe Co v Washington* 326 US 310, in accordance with the U.S. Constitution (1787), Amendment XIV (1868), section 1. The "minimum contacts" rule provides that jurisdiction over a person shall only exist if the person has a minimum level of contacts with the state: per M. Saadat, '*Jurisdiction and the Internet after Gutnick and Yahoo!'*, 2005 (1) The Journal of Information, Law and Technology, *fn 64.*

[31] Council Regulation (EC) No 44/2001 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters ('Regulation').

[32] with the exception of Denmark.

[33] Para 11 of Regulation.

[34] Article 2(1) of Regulation.

[35] Article 4(1) of Regulation ("If the defendant is not domiciled in a Member State, the jurisdiction of the courts of each Member State shall, subject to Articles 22 and 23, be determined by the law of that Member State").

[36] Just a note that most civil law countries do not accept the principle of *forum non-conveniens:* see C. G. Lang, *'Forum Non Conveniens in Continental Europe' (*http://www.prager-dreifuss.com/system/document_des/78/original/Forum_Non_Conveniens_Cont_Europe_.pdf?1289378662)

[37] *Spiliada Maritime Corporation v Cansulex Ltd.* [1987] AC 46, *Piper Aircraft v Reyno*, 454 U.S. 235.

[38] *Voth v Manildra Flour Mills Pty Ltd* (1990) 97 CLR 124.

[39] This expression has an autonomous meaning and should not be interpreted simply as referring to the national law of one or other Convention State (***Kalfelis v Bankhaus Schroder,*** *Münchmeyer*,

State in the courts for the place where the harmful event occurred or may occur. This therefore permits a defendant domiciled within a Member State, exceptionally, to be sued in the court of another Member State. Defamation therefore falls within Article 5(3). The interpretation of Art.5(3) is especially relevant to the possibility of being sued in a Member State in which a website is merely available.[40]

Freedom of contract also allows persons to specify the jurisdiction within which disputes shall be contested, and therefore it is common for international business contracts to specify both the choice of court and law that will apply in the event of a legal dispute arising out of the contract.[41] Where an exclusive jurisdiction clause is provided for in a contract, common law courts have tended to exercise their discretion strongly in favour of giving effect to the contract agreed by the parties.[42] Australia is a country being part of the shared common law regime, where the Australian States and Territories share a common legal heritage with a single national final court of appeal, the High Court of Australia.[43] The choice of law rules, as concluded by the Australian Law Reform Commission ('Commission')[44] relate to the following questions (i) decision as to which State's law applies; (ii) applicable jurisdiction, which is a pre-requisite for any choice of law issues; and (iii) forum shopping. The relevant classification in international trade and commerce should be[45] (i) any relevant statute or international convention; (ii) express choice of law in the contract; (iii) implied intention[46]; (iv) in absence of express choice of law: closest and more real connection. One of the cornerstones of the conflict-of-law rules in matters of contractual obligations is the freedom

Hengst & Co [1988] E.C.R. 5565) per G Smith, '*Here, there or everywhere? Cross-border liability on the internet*' Computer and Telecommunications Law Review, 2007, 13(2), 41-51.

[40] G Smith, '*Here, there or everywhere? Cross-border liability on the internet*' Computer and Telecommunications Law Review, 2007, 13(2), 41-51.

[41] M. Saadat, '*Jurisdiction and the Internet after Gutnick and Yahoo!*', 2005 (1) The Journal of Information, Law and Technology.

[42] *Lewis Construction Co Pty Ltd v Tichauer (M) Societe Anonyme* [1966] VR 341; *Huddart Parker Ltd v Ship "The Mill" and Her Cargo* (195) 81 CLR 502.

[43] Paragraph 3.2 of The Law Reform Commission Choice of Law Report No. 58 (1992).

[44] The Law Reform Commission was established by the Law Reform Commission Act 1973 to review, modernise and simplify the Australian law.

[45] J. Levingston, *Choice of law, jurisdiction and ADR clauses*, 6th Annual Contract Law Conference Paper (26-28 February 2008).

[46] The question of the intention of the parties can be determined by a number of indicators. See *Bonython v Commonwealth of Australia* (1948) 75 CLR 589 per Dixon J at 624, 5: 'The interpretation of the transaction must be worked out from its character, from the elements which are contained within it. The nature and circumstances of the transaction must supply the grounds from which the so-called 'intention' must be deduced as a reasoned consequence. It may be called an implication.'

of the parties to choose the law applicable to their dealings. The general rule is that the governing law of a contract is the law which the parties have chosen and therefore any potential conflict of laws should be avoided by an express choice of law clause, with an express choice of forum. Choice of law can determine the validity and enforceability of a contract[47] and its terms and the extent of the rights and obligations which are not expressly set out. Further, the contract is unenforceable if it is illegal under the proper law or if it is illegal under the law of the forum.[48] In the EU, pursuant to the Regulation (EC) No 593/2008 of the European Parliament and of the Council on the law applicable to contractual obligations (Rome I Regulation), which is the most current and holistic piece of legal legislation directly applicable in the Member States of the European Union[49] as a source of the European Union law[50], the parties are entitled to submit their contractual obligations to the law of their choosing provided that such choice of law is either expressed or demonstrated with reasonable certainty by the parties in the circumstances of the case[51] as well as valid, i.e. it satisfies (i) the substantive requirements of the law applicable to the 'governing law' clause[52]; and (ii) the formal requirements set out in the law governing the obligations in question. The law chosen by the parties will govern issues such as interpretation and performance of the contract, limitations, and consequences of breach of obligations or nullity of the contract as well as contractual disputes. The freedom of choice provided for by the Regulation however is not absolute, but subject to certain exclusions, restrictions, and limitations including areas of insurance contracts, or when the chosen foreign law would interfere with the (EU) Community's interests especially if the chosen law is not the law of a Member State but all of the elements of the contract located in one or more Member States[53] and in relation to consumer contracts. In Australia, unless the matter is disputed, the courts will apply the law of the place where the court is sitting, that is the law of the forum[54]. When a party claims that the law of another State should be applied, the

---

[47] See *Saxby v Fulton* [1909] 2 KB 208.

[48] See *Boissevain v Weil* [1950] AC 327.

[49] apart from Denmark.

[50] Regulation (EC) No 864/2007 of the European Parliament and of the Council on the law applicable to non-contractual obligations (Rome II Regulation) excludes defamation from its scope, therefore the case law of the European Court of Human Rights on freedom and expression in the context of defamation will prevail.

[51] Article 3(1) of the Regulation.

[52] Article 3(5) of the Regulation.

[53] Article 3(4) of the Regulation.

[54] Lex fori or the forum law is the law of the place where the court of law is situated, the local or domestic law of the forum – Castel, Introduction to Conflict of Laws, 2nd ed, Butterworths, 1986.

court uses the choice of law rules to decide the issue.[55] Reasons which Australian courts have given for allowing parties to chose the law applicable to their contract[56] include familiarity with the chosen law[57], the perceived neutrality of that law[58], and that certain types of standard commercial contracts especially maritime contracts, have been developed in English commercial and legal practice, which then has been considered the rationale for allowing parties to choose English law[59]. The parties can chose the law applicable to the whole or part only of the contract with also subject to certain exclusions, restrictions, and limitations[60] such as (i) the requirement of choice of law being '*bona fides*', legal and not contrary to public policy;[61] (ii) statute law[62]; and (iii) operation of public policy and the principle of illegality.[63] It is important to note that different rules apply where one the parties is a consumer.[64] Where the parties have not indicated their choice of law in the contract, it is the law of the country with the 'closest and most real connection' with the transaction.[65] When examining the connections, the followings should be taken into consideration: (i) the habitual place of residence or business of the parties; (ii) the place where the relationship between the parties is centred; (iii) the place where the contract is made; and (iv) the place where the contract is to be performed; (v) the place where the contract is to be performed; (vi) the place where the steps necessary for the conclusion of the contract were taken;[66] (vii) the place where an

[55] Paragraph 1.3 of The Law Reform Commission Choice of Law Report No. 58 (1992).

[56] In *BHP Petroleum Pty Ltd v Oil Basin Ltd* [1985] VR 725 a Victorian court applied the principle of freedom of contract to uphold a choice of New York law.

[57] See *Vita Food Products Inc v Unus Shipping Co Ltd* [1939] AC 277.

[58] See *British Controlled Oil Fields v Staff* [1921] WN 319.

[59] Paragraph 8.4 of the Law Reform Commission, Choice of Law Report No 58 (1992).

[60] Paragraph 8.10 of the Law Reform Commission, Choice of Law Report No 58 (1992).

[61] See *Vita Food Products Inc v Unus Shipping Co Ltd* [1939] AC 277 yet, the Commission's recommendation was that limitation on parties autonomy on the ground of lack of bona fides should be replaced with rules to determine when parties cannot choose to evade the operation of a "mandatory law" of the place of closest connection – Paragraph 8.13 of the Choice of Law Report No 58 (1992).

[62] Perhaps the best example is the area of consumer protection. On 1 January 2011, the new Australian Consumer Law (ACL) commenced. The full text of the ACL is set out in Schedule 2 of the Competition and Consumer Act 2010 (Cth) which is the new name for the Trade Practices act 1974 (Cth) (TPA) that impose compulsory framework to the parties, who simply cannot opt-out from the application thereof.

[63] Whether or not a term of a contract or performance of a contractual obligation is 'illegal' is generally speaking governed by the proper law, which also determines whether or not the contract is unenforceable because of illegality – Paragraph 8.16 the Law Reform Commission, Choice of Law Report No 58 (1992).

[64] See Articles 15-17 of Regulation 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

[65] Paragraph 8.37 of the Law Reform Commission, Choice of Law Report No 58 (1992).

[66] See Article 8 (2) (a) of the Hague Convention on the Law Applicable to Contracts for the International Sale of Goods.

advertisement or invitation to enter into the contract was received or to which the offer or directed his commercial activities.[67]

As mentioned above, states will not always enforce the judgements of foreign courts. Non-enforcement is especially likely to occur in circumstances where a judgement has been handed down against a person that, either has no connection with the foreign state, or did not contest the proceedings in the foreign state.[68] States will more likely also not enforce foreign judgement involving taxation, penal or other public laws.[69] While a person is unlikely to be subject to the jurisdiction of a completely remote state, it is often the case that a person will have a degree of connection with a number of states. Moreover, among the many states that a person may have connection with, it is likely that a person will have a preferred jurisdiction for litigating.[70] An interesting case law regarding enforceability is the French *Yahoo* case[71] where LICRA, a French non-profit organisation dedicated to eliminating anti-Semitism, sent a 'cease and desist' letter to Yahoo!'s U.S. headquarters informing Yahoo! that the sale of Nazi memorabilia through its auction services violated French law. Although Yahoo! subsequently blocked the sale of Nazi memorabilia on its French website, certain items continued to be available on the main Yahoo! auction site. LICRA argued that because this main site was also accessible by French citizens, Yahoo! continued to be in violation of French law.[72] The court held that blocking French access on the main website was technically possible, and that because it could be viewed by French citizens, it fell within the jurisdiction of France and subsequently it ordered Yahoo! to comply. Yahoo! sought a declaratory judgement that the 'French Court's orders are neither cognizable nor enforceable under the laws of the United States.' Judge Fogel granted Yahoo!'s request for declaratory judgement. Substantively, this was to be expected. U.S. courts have previously denied enforcement of foreign judgements that have been deemed incompatible with the U.S. Constitution, including enforcement of foreign

[67] Article 15 (1) of the Regulation (EC) No 593/2008 of the European Parliament and of the Council on the law applicable to contractual obligations.

[68] *Emanuel v Symon* [1908] 1 KB 302 (CA).

[69] *United States of America v Inkley* [1988] 3 W.L.R. 304 (Ct. App.)

[70] M. Saadat, '*Jurisdiction and the Internet after Gutnick and Yahoo!*', 2005 (1) The Journal of Information, Law and Technology.

[71] *La Ligue Contre Le Racisme et l'Antisemitisme (LICRA) v Yahoo! Inc,* Tribunal de Grande Instance de Paris, November 20, 2000.

[72] M. Saadat, '*Jurisdiction and the Internet after Gutnick and Yahoo!*', 2005 (1) The Journal of Information, Law and Technology.

defamation judgements.[73] Judge Fogel held that: 'what is at issue here is whether it is consistent with the Constitution and laws of the United States for another nation to regulate speech by a United States resident within the United States on the basis that such speech can be accessed by Internet users in that nation … The modern world is home to widely varied cultures with radically divergent value systems. There is little doubt that Internet users in the U.S. routinely engage in speech that violates, for example, China's laws against religious expression, the laws of various nations against advocacy of gender equality or homosexuality, or even the United Kingdom's restrictions on freedom of the press.' Procedurally, however, Judge Fogel was found to have erred according to U.S. court[74], as it held in a majority judgement, that Yahoo!: 'must wait for the foreign litigants to come to the United States to enforce the judgement before its First Amendment claim may be heard by a U.S. court,' which implies that the decision has little practical impact for Yahoo! Even if LICRA were to seek enforcement of the French Court's decision in the U.S., it is unlikely that a U.S. court would give effect to the French Court's orders. While *Yahoo!* is a victory for free speech on the Internet, more importantly it demonstrates that the existing rules of jurisdiction, in their practical operation, do not have the effect of chilling speech on the Internet.

Traditional rules of jurisdiction vs. cyberspace law

There are fundamental difficulties in applying traditional localisation principles to a transaction which is effected via the Internet. As discussed above, the principles for establishing the applicable law and jurisdiction in the absence of choice of law provisions and in relation to cross-border transactions have been established via private international law or conflict of laws, mainly by determining whether a relevant element of the transaction can be localised in the jurisdiction in question.[75] How would this be carried out in terms of establishing where each element of a cyberspace transaction takes place? By doing so requires an identification of the physical place where the appropriate element of the transaction occurred, as a consequence of which jurisdiction can be established as being the state in whose territory that place is located or its law is applied.[76]

---

[73] *Matusevitch v Telnikoff,* 877 F Supp 1 (DDC, 1995) and *Bachchan v India Abroad Publications Inc*, 585 NYS 2d 661 (NY County SC, 1992) – both being British libel judgement not enforced in the U.S., per M. Saadat, '*Jurisdiction and the Internet after Gutnick and Yahoo!'*, 2005 (1) The Journal of Information, Law and Technology, fn 167.

[74] Court of Appeals for the 9th Circuit.

[75] C. Reed, *Internet Law*, Second Edition (2004) Cambridge University Press, pg. 218.

[76] C. Reed, *Internet Law*, Second Edition (2004) Cambridge University Press, pg. 223.

This is challenging as online activities are not tied to geographically proximate locations. Information in cyberspace is available simultaneously to anyone with a connection to the global network. The notion that the effects of an activity that takes place on that website radiate from a physical location over a geographic map in concentric circles of decreasing intensity is inapplicable to cyberspace.[77]

In the era of electronic technology, we increasingly rely on digital communication and information even though this may pose challenges to the existing legal regimes but would this necessitate that the law applicable to transactions in cyberspace be different law as that applicable to physical, geographically-defined territories? There is an apparent debate whether a distinct set of "cyberspace law" should be developed to solve the current predicaments faced by regulators[78] or to the contrary, arguing that the Internet is not a new and separate jurisdiction in which the rules and regulations of the physical world do not apply and therefore cyberspace transactions are no different from 'real-space' transnational transactions.[79]

It is important to determine whether the Internet allows people to do new things or whether it largely allows people to do existing things in new ways, albeit in greater volumes. This is a necessary distinction to be drawn, as the answer directly impacts upon the manner in which the Internet should be regulated.[80] Jack Goldsmith argues that 'cyberspace transactions are no different from "real-space" transnational transactions as they involve real people in one territorial jurisdiction either transacting with real people in other territorial jurisdictions or engaging in activity that causes real-world effects in another territorial jurisdiction. 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.'[81] To this extent, activity in cyberspace is functionally identical to transnational activity mediated by other means, such as mail or telephone

---

[77] S. Anil, '*Cyberspace and the law of defamation: developing a workable model'*, Computer and Telecommunications Law Review, 2001, 7(7), 175-183.

[78] S. Anil, '*Cyberspace and the law of defamation: developing a workable model',* Computer and Telecommunications Law Review, 2001, 7(7), 175-183.

[79] J. Goldsmith J, '*Against Cyberanarchy*' (1998) 65 *Chicago Law Review* 1239.

[80] M. Saadat, '*Jurisdiction and the Internet after Gutnick and Yahoo!'*, 2005 (1) The Journal of Information, Law and Technology.

[81] J. Goldsmith J, '*Against Cyberanarchy*' (1998) 65 *Chicago Law Review* 1239.

or smoke signal. There is case law[82] affirming this approach where peer-to-peer file-sharing computer networking software makers were not held to be vicariously liable for copyright infringement by users. The court[83] held that: "the introduction of new technology is always disruptive to old markets, … yet, history has shown that time and market forces often provide equilibrium in balancing interests, whether the new technology be … a video recorder … or an MP3 player. Thus, it is prudent for courts to exercise caution before restructuring liability theories for the purpose of addressing specific market abuses, despite their apparent present magnitude". It is contended therefore, that because, in principle, Internet conduct is functionally identical to real space conduct, the traditional rules of jurisdiction should (at least *prima facie*) apply. This approach is reflected in the High Court's decision in *Gutnick*[84] where Chief Justice Gleeson, and Justices McHugh, Gummow and Hayne in response to the suggestion that the Internet is different to any previous communications technology, held that: 'It was suggested that the World Wide Web was different from radio and television because the radio or television broadcaster could decide how far the signal was to be broadcast. It must be recognised, however, that satellite broadcasting now permits very wide dissemination of radio and television and it may, therefore, be doubted that it is right to say that the World Wide Web has a uniquely broad reach. It is no more or less ubiquitous than some television services. In the end, pointing to the breadth or depth of reach of particular forms of communication may tend to obscure one basic fact. 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.'[85]

On the other hand, this position is in direct opposition to many Internet legal scholars[86] who argue that events and transactions in real-space and cyberspace are not identical in many ways and that the Internet is 'exceptional' and that the questions raised by Internet conduct are different, than the analogous questions raised by its realspace counterpart and that the jurisdictional dilemmas cannot be resolved by applying the traditional legal tools developed for

[82] *Metro-Goldwyn Mayer Studios, Inc v Grokster Ltd* CV-01-8541.

[83] U.S. Ninth Circuit Court of Appeals.

[84] *Dow Jones & Company, Inc v Gutnick* [2002] HCA 56.

[85] *Dow Jones & Company, Inc v Gutnick* [2002] HCA 56, para 39.

[86] See D. Post, '*Against "Against Cyberanarchy"*', 17 *Berkley Technology Law Journal* (2002) 1371.

similar problems in realspace. These authors[87] consider that cyberspace could not lawfully be governed by territorially-based sovereigns and that the online world should create its own legal jurisdiction, and argue[88] that the nature of Internet destroys the significance of physical location, eliminating the possibility of a single, uniform legal standard and the lack of physical borders in cyberspace prevents effective rule-making by centralized government.[89] According to this view there is a need for an indigenous law of cyberspace which law would take into account many of the distinctive features of online interaction which means law formation and enforcement wherein cyberspace with its own self regulating jurisdiction.[90] Many legal principles applied to real space transactions are not workable to cyberspace transactions, which mean that there is need for new legal principles applicable and suitable for the new electronic environment.[91] There is an added concern however, namely that the concept of cyberspace originated in the U.S. and being so, their digital law tends to be more developed than the rest of the world. For example, section 230(c)(1) of the Telecommunications Act 1996, gave network owners a "good Samaritan Defence" which states that: "… no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information provider …" The above extract seems to indicate a progressive development of cyber-intended law, however it is a valid question that with the U.S. legal jurisprudence so commonly accepted to be the most developed, other jurisdictions could be overlooked in this process.[92] Traditional legal doctrine treats cyberspace as a mere transmission medium that facilitates the exchange of messages sent from one territorial sovereign to another. Scholars argue that a more legally significant border for "cyberlaw space" could be set up.[93] By recognising a legally significant border between cyberspace and physical space, regulators could conceive cyberspace as a distinct "place" for purposes of analysing legal issues.

---

[87] D. R. Johnson & D. Post, '*Law and Borders-The Rise of Law in Cyberspace*', 48 Stan. L. Rev. 1367 (1996).

[88] D. Post, '*Governing Cyberspace*', 43 Wayne L. Rev. 155 (1996).

[89] David G. Post, 'Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace', 1995 J. ONLINE L. 3.

[90] A. Mefford, '*Lex Informatica: Foundations of Law on the Internet*', 5 IND. J. of Global Legal Stud. 211, 236 (1997) (asserting that self-regulation is more legitimate than territorial law because users create "Net law").

[91] G. I. Zekos, '*State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction*', International Journal of Law and IT (2007) 15 (1), pg 5.

[92] S. Anil, '*Cyberspace and the law of defamation: developing a workable model*', Computer and Telecommunications Law Review, 2001, 7(7), 175-183.

[93] D. R. Johnson and D. Post, "*The Rise of Law on the Global Network*" in Borders in Cyberspace – Information Policy and the Global Information Infrastructure (The MIT Press, 1997).

The new boundary would consist of screens and passwords that separate the real world from the virtual world. Treating cyberspace as a separate "space" to which distinct laws apply is feasible according to David Post. Entry into this virtual world occurs through a screen and a password boundary.[94] Nobody can accidentally stray across the border into cyberspace. Application of a distinct "law of cyberspace" would be equitable to those who pass over the electronic boundary because the primary characteristic of a boundary is its ability to be perceived by the person who crosses it. Using this new approach will permit the development of laws that are better suited to the global phenomena of cyberspace. For example, these laws can address the rights to continued existence or protection of a pseudonym's reputation (electronic communications are not necessarily tied to real world identities). Furthermore, they are more likely to be legislated by authorities that understand and participate in the global phenomena. Enforcement is more likely to effectively utilise the new global communications media made available by cyberspace.[95]

Some say[96] that cyberspace is a supra-territorial phenomenon and the supra-territoriality of the medium results in part in a supra-territorial society, and that the protection of fairness for individual users in the global net-world will rely less upon the law of territorially based jurisdictions and more upon the actions of online communities. The rise of cyberspace brings forward the need for a revision of the meaning and substance of jurisdiction and sovereignty. Globalization brought increasing trans-national and supra-national governance and increasing mobility of persons and capital across geographical boundaries. Hence, the combination of cyberspace and globalisation brought a new order in humans' life, law and order, [97] which mean that there is a need for the adoption of a universal cyberspace jurisdiction.[98]

---

[94] D. R. Johnson, "*Travelling in Cyberspace*", Legal Times, April 3, 1995.

[95] S. Anil, '*Cyberspace and the law of defamation: developing a workable model'*, Computer and Telecommunications Law Review, 2001, 7(7), 175-183.

[96] J. C. Ginsburg, '*Global Use/Territorial Rights: Private International Law questions of the Global Information Infrastructure*', J. COPY. SOC. 318, 319-320.

[97] D. M. Curtin, '*Postnational Democracy: The European Union in Search of a Political Philosophy*' 4 (1997): ("*Just think of how global computer-based communications cut across territorial borders, creating a new realm of human activity and undermining the feasibility-and legitimacy-of applying laws based on geographic boundaries to this new sphere.*"). A. Appadurai, '*Disjuncture and Difference in the Global Cultural Economy, in Modernity at Large: Cultural Dimensions of Globalization*' 27, 27-29 (1996) ("*Today's world involves interactions of a new order and intensity. ... With the advent of the steamship, the automobile, the airplane, the camera, the computer and the telephone, we have entered into an altogether new condition of neighbourliness, even with those most distant from ourselves.*").

[98] G. I. Zekos, '*State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction*', International Journal of Law and IT (2007) 15 (1).

Further, it could also be argued that contract law more and more will become the primary law of cyberspace offering a way around jurisdictional puzzles by allowing parties to construct their own legal relations, opt for a particular set of legal rules, and choose the forum of their choice for dispute resolution. Moreover, creators of intellectual products are relying less on traditional intellectual property regimes to allow them to limit access to their material, and more on a combination of contractual rights and technological protections.[99] Self-governance through contractual relationships between cyberspace users and self-regulatory network providers can address the challenges of cyberspace transactions because it lessens the pressure to localise behaviour. Experience suggests that the community of online users and service providers is capable of developing a credible self-governance system.[100] For example, the current domain name system evolved from self-governing decisions made by engineers and the practices of ISPs.[101] Dispute resolution mechanisms suited to the new environment are beginning to prosper too.[102] The proposed self-regulatory approach treats the global network as a separate place. Each self-regulatory group would have its specific set of defamation law unique to the culture of its electronic community.[103]

Nevertheless, all self-regulatory organisations derive their authority from the traditional sovereigns; they are always subject to the sovereign imposing new regulations and enforcing them. It is difficult to envision territorial sovereigns deferring to the law of the cyberspace. Authorities would be unwilling to defer to self-regulatory organisations, as they fear subjecting themselves to conflicting laws legislated by self-regulators who are non-citizens (for example, laws that are not against national interests but against their political interests). Furthermore, self-regulated laws may be overridden by a variety of national mandatory law restrictions, such as common law vitiating minor users' contracts with self-regulators. Furthermore, there is difficulty in generating consent across different cyberspace networks.[104] Self-regulators have not worked out the technological and

[99] N. Weinstock Netanel, '*Locating Copyright Within the First Amendment Skein*', Oxford University Press 2007 Int J Law Info Tech (2007) 15 (1): 1.

[100] D. G. *Post, Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace* [1995] J. Online L. Art. 3, 10.

[101] A. M. Rutkowski, *Internet Names, Numbers and Beyond: Issues in the Coordination, Privatization and Internationalization of the Internet* (November 20, 1995).

[102] See H. H. Perritt, Jr, *Dispute Resolution in Electronic Network Communities*, 38 V.I.L.L. L. Rev. 349, 398-399 (1993).

[103] S. Anil, '*Cyberspace and the law of defamation: developing a workable model*', Computer and Telecommunications Law Review, 2001, 7(7), 175-183.

[104] H. Perritt, Jr, '*Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalism?*', *Berkeley Technology Law Journal*, Volume 12. (see: http://www.law.berkeley.edu/journals/btlj/articles/vol12/Perritt/html/reader.html).

conceptual details of consenting to and co-ordinating different legal regimes when users enter into different cyberspace networks.

One of the downsides of self-regulatory proposals is that communications in cyberspace often have consequences for persons outside the computer networks who have not consented to the self-regulation of the cyberspace community. *Ex ante* consent to a private legal regime from these non-users is not possible.[105] In the case of defamation, a chat room participant can defame a non-subscriber, in which scenario; the legal rights of the non-user could not be resolved satisfactorily in the self-regulatory framework because the available remedies may not apply to him since he has not subjected himself to the self-regulation framework that applies to subscribers.

Finally, in relation to the debate whether the Internet is 'no different'[106] or 'indeed different'[107] to real space in terms of jurisdictional, there is a third view[108] as to how regulate cyberspace according to which the Internet should be regulated in the same way as the other established 'international spaces' Namely Antarctica, outer-space and the high-seas.[109] Accordingly, jurisdiction should be determined according to the nationality of the parties. 'Unless it is conceived of as an international space, cyberspace takes all of the traditional principles of conflicts-of-law and reduces them to absurdity.' This indicates that because the Internet contains millions of websites, Internet conduct (whether it is akin to real space conduct or not), in potentially causing a nightmare conflict-of-laws scenario, needs to be regulated separately.[110]

Following the review of all these various concepts and ideas as to how to regulate cyberspace, this paper also intends to review some of the current approaches emerged from the Internet case law in relation to defamatory acts in various jurisdictions. Before we examine the cyberspace defamation cases, it is important to establish what defamation is. Defamation is essentially a tortious act by the defendant, which causes damage to the plaintiff. This damage must

---

[105] S. Anil, '*Cyberspace and the law of defamation: developing a workable model'*, Computer and Telecommunications Law Review, 2001, 7(7), 175-183.

[106] J. Goldsmith J, '*Against Cyberanarchy*' (1998) 65 *Chicago Law Review* 1239.

[107] D. Post, '*Against "Against Cyberanarchy"'*, 17 *Berkley Technology Law Journal* (2002) 1371.

[108] D Menthe, '*Jurisdiction in Cyberspace: A Theory of International Space'*, 4 *Mich. Telecomm. Tech. Law Review* 69 (1998).

[109] M. Saadat, '*Jurisdiction and the Internet after Gutnick and Yahoo!'*, 2005 (1) The Journal of Information, Law and Technology.

[110] D Menthe, '*Jurisdiction in Cyberspace: A Theory of International Space'*, 4 *Mich. Telecomm. Tech. Law Review* 69 (1998).

be caused by the fault of the defendant and must be a harm recognised as legal liability.[111] A general test needs to be applied to the alleged defamatory statement to establish its nature. As words may have more than one meaning, it is essential that they be taken in the context in which they were used. Defamation is essentially an attack on reputation and it needs not impute moral turpitude.[112]

Law of defamation through selected case law

The English case of *Godfrey v Demon Internet Limited*[113] concerned the issue of defamation on the Internet. Although the alleged defamatory material ('the posting') was uploaded to the Internet by a U.S. an unknown person, the English resident plaintiff brought action against the English Internet Service Provider ('ISP') hosting the posting on its servers claiming that the ISP published the posting by hosting it, in accordance with section 1 of the Defamation Act 1996. It was also submitted that the ISP's failure to remove the posting, after having been advised of its existence by the plaintiff, prevented ISP from availing themselves of the common law defamation defence of 'innocent dissemination.'[114] Justice Morland noted in his judgement that English law did not contain an equivalent of the U.S. statutory provision of 'precluding courts from entertaining claims that would place a computer service provider in a publisher's role.'[115] Initially, Justice Morland held that ISP 'was clearly not the publisher of the posting defamatory of the plaintiff within the meaning [of the Defamation Act]'. Despite this, because the plaintiff notified the IPS of the publication of the posting, they had an obligation to remove it, or else remain liable for defamation.

One of the most important cases involving jurisdiction on the Internet is the *Gutnick*[116] case, in which the High Court of Australia applied Australia's traditional rules of jurisdiction to

[111] John Cooke, '*Law of Tort'* (2nd ed., Pitman Publishing, 1995) per S. Anil, '*Cyberspace and the law of defamation: developing a workable model'*, Computer and Telecommunications Law Review, 2001, 7(7), 175-183, fn 1.

[112] S. Anil, '*Cyberspace and the law of defamation: developing a workable model'*, Computer and Telecommunications Law Review, 2001, 7(7), 175-183.

[113] [1999] EWHC QB 244.

[114] *Godfrey*, in [1999] EWHC QB 244, para 2, per M. Saadat, '*Jurisdiction and the Internet after Gutnick and Yahoo!'*, 2005 (1) The Journal of Information, Law and Technology, fn 99.

[115] M. Saadat, '*Jurisdiction and the Internet after Gutnick and Yahoo!'*, 2005 (1) The Journal of Information, Law and Technology, *fn. 100.*

[116] *Dow Jones & Company, Inc v Gutnick* [2002] HCA 56.

determine that Australian courts do have jurisdiction to adjudicate alleged defamation on the Internet. The case is considered especially important, as it was the first judgement of any nation's final appellate court on the jurisdiction issue in an international defamation case involving Internet-based publication.[117] Per the facts, Dow Jones prints and publishes the Wall Street Journal newspaper and Barron's magazine. Since 1996, Dow Jones has operated wsj.com, a subscription news site on the Internet. Those who pay an annual fee may have access to the information to be found at wsj.com. Those who have not paid a subscription may also have access if they register their details. Access is at all times only available with a user name and a password.[118] The publication contained an article referencing Gutnick on several occasions, which Gutnick claimed that it defamed him and hence he brought an action in the Supreme Court of Victoria against Dow Jones claiming damages for defamation. Gutnick lived and ran his business in Victoria (although some of his businesses were conducted outside of Australia, including the U.S., much of his social and business life could be said to be focused in Victoria). About subscribers 300 were in Victoria. Dow Jones has an office in the U.S. state of New Jersey, where servers hosting its wsj.com website are located. In bringing an action against Dow Jones, Gutnick confined his claim in respect of publication of the article that occurred in Victoria. In proceedings before the Supreme Court of Victoria, Dow Jones applied for an order that the plaintiff's service of writ and statement of claim be set aside, or an order that further proceedings in the matter be permanently stayed. Dow Jones contended that the Supreme Court of Victoria lacked jurisdiction in the matter, or alternatively, that the state of Victoria was a 'clearly inappropriate forum.'[119] Justice Hedigan concluded that the allegedly defamatory article was 'published in the state of Victoria when downloaded by Dow Jones subscribers who had met Dow Jones's payment and performance conditions and by the use of their passwords.'[120] Dow Jones's contention that the publication of the article occurred at their servers in New Jersey was rejected. In concluding that Gutnick was defamed in Victoria, Dow Jones's submission that Victoria was a clearly inappropriate forum was also rejected. The Court of Appeal was quick to conclude that Justice Hedigan's decision was 'plainly correct.'[121] As Australia's final appellate court, the High Court's decision to accept the appeal attracted a significant amount of

[117] M. Saadat, '*Jurisdiction and the Internet after Gutnick and Yahoo!*', 2005 (1) The Journal of Information, Law and Technology.

[118] *Dow Jones & Company, Inc v Gutnick* [2002] HCA 56, para 1.

[119] *Voth v Manildra Flour Mills Pty Ltd* (1990) 171 CLR 538 (that is, the argument of *forum non-conveniens*), per M. Saadat, '*Jurisdiction and the Internet after Gutnick and Yahoo!*', 2005 (1) The Journal of Information, Law and Technology, fn 107.

[120] *Gutnick v Dow Jones & Co, Inc* [2001] VSC 305, para 60.

[121] *Dow Jones & Company, Inc v Gutnick* [2001] VSCA 249.

international interest.[122] In a unanimous decision, the full court of the High Court affirmed the Victorian Supreme Court's decision, and denied Dow Jones's appeal. The appeal focussed on the critical question of where the article available was published. Although Australia's traditional rules of defamation quite clearly pointed to publication having occurred in Victoria (in each and every instance that the article was downloaded by a subscriber residing in the state), Dow Jones, urged the court to establish separate rules for Internet-based publications, arguing that the rule for Internet publication should be akin to the U.S. defamation 'single publication rule', and that an article should be deemed published when it is uploaded to a server (an approach labelled 'the law of the server'[123]). The location of the server, it was suggested, should determine the applicable choice of law and jurisdiction. Dow Jones, desperately sought to emphasise the special nature of the Internet, and argued that by virtue of being on the Internet, a publication should be subject to different rules and that Internet conduct is different because the scale of the Internet transforms otherwise analogous non-Internet conduct. It was further argued that unlike the situation of a newspaper being distributed (in hardcopy) abroad, 'with the Internet you cannot know' where a website will be viewed. Justice Kirby, in contrast to the other seven justices of the court, accepted the submission by Dow Jones, that the Internet is a unique medium,[124] as he held that 'the Internet is not simply an extension of past communications technology. It is a new means of creating continuous relationships in a manner that could not previously have been contemplated…'. Despite this, Justice Kirby held that it was the responsibility of the legislature to reform the common law rules of defamation, and that there were limits to 'judicial innovation.' With the exception of Justice Kirby, therefore, six of the seven High Court justices appear to have accepted Goldstone's 'un-exceptionalist' view of the Internet, as they did not find any inherent reasons why the Internet should be subject to different common law rules.[125] Dow Jones, in addition to arguing that the Internet is qualitatively different to previous communications technologies, advanced policy reasons for having a single publication rule for Internet material. Unless there was such a rule, it was suggested, there would be a 'chilling effect' on material available on the Internet, because Internet

---

[122] M. Saadat, '*Jurisdiction and the Internet after Gutnick and Yahoo!*', 2005 (1) The Journal of Information, Law and Technology.

[123] See D Menthe, "Jurisdiction in Cyberspace: A Theory of International Spaces", 4 *Mich. Telecomm. Tech. L. Rev* 69 (1998) arguing as to why the 'law of the server' would be undesirable.

[124] M. Saadat, '*Jurisdiction and the Internet after Gutnick and Yahoo!*', 2005 (1) The Journal of Information, Law and Technology.

[125] M. Saadat, '*Jurisdiction and the Internet after Gutnick and Yahoo!*', 2005 (1) The Journal of Information, Law and Technology.

publishers would be exposed to law suits anywhere in the world. Justice Kirby held that this would be a concern 'particularly in cases where the plaintiff has a substantial reputation in more than one legal jurisdiction and seeks to recover for the damage in all such jurisdictions in a single proceeding. In such a case, potential liability in defamation for the publication of material relating to such a person on the Internet may indeed have a chilling effect on free speech merely because one of those jurisdictions has more restrictive defamation laws than the others. This approach could subject Australian defendants to the more restrictive defamation laws of foreign jurisdictions.'[126] This concern was, however, rejected by a majority of the court on a twofold basis. Firstly, with respect to the suggestion by Dow Jones that the single publication rule for Internet material be centred on the location of the server hosting the material. The court held that this would allow: 'publishers … to manipulate the uploading and location of data so as to insulate themselves from liability in Australia, or elsewhere: for example, by using a web server in a "defamation free jurisdiction", or one which the defamation laws are tilted decidedly towards defendants.'[127] In terms of the implications for the Internet after *Gutnick*, some say[128] that the case will have 'the potential to chill freedom of speech' as 'foreign publishers may decide to water down or not publish material which has the potential to damage the reputations of Australians … or try to restrict Australians from having access to their site.'[129]

In the U.S. case of *Zippo*,[130] the court[131] adapted the minimum contacts test for specific personal jurisdiction in Internet cases. A 'sliding scale' test was developed for determining whether a defendant's conduct over the Internet allows a (U.S.) state to exercise personal jurisdiction over him.[132] The court held that the 'sliding scale is consistent with well developed personal jurisdiction principles. At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that

---

[126] Per M. Saadat, '*Jurisdiction and the Internet after Gutnick and Yahoo!*', 2005 (1) The Journal of Information, Law and Technology, fn 122.

[127] M. Saadat, '*Jurisdiction and the Internet after Gutnick and Yahoo!*', 2005 (1) The Journal of Information, Law and Technology, fn 121.

[128] See M Collins, '*The Law of Defamation and the Internet*' (New York: Oxford University Press, 2001).

[129] M Collins, 'Defamation on the Internet After *Dow Jones & Company Inc v Gutnick*', (2003) 8 *Media & Arts Law Review* 3, 181.

[130] 952 F Supp 1119 (WD Pa, 1997).

[131] Pennsylvania District Court.

[132] M. Saadat, '*Jurisdiction and the Internet after Gutnick and Yahoo!*', 2005 (1) The Journal of Information, Law and Technology.

involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. At the opposite end are situations where a defendant has simply posted information on an Internet Web site which is accessible to users in foreign jurisdictions. A passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise personal jurisdiction. The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site.' Furthermore, the Pennsylvania court made it clear that, irrespective of one's conception of the Internet, 'when a defendant makes a conscious choice to conduct business with the residents of a forum state, "it has clear notice that it is subject to suit there".' Australian courts however do not apply a sliding scale test. In the case of passive websites, therefore, defendants before Australian courts will need to mount an argument of *forum non-conveniens* in order to have proceedings stayed. A passive website with real connections to only one or two states (that is, the states in which the website was created and/or is hosted) should not ordinarily be subject to the jurisdiction of other states, simply because the website is able to be downloaded from those states. Fortunately, states that seek to claim jurisdiction over all material on the Internet (simply because a computer within the jurisdiction is able to download material from anywhere on the Internet) will be prevented from *effectively* exercising such jurisdiction.[133] It is relevant to mention the Attorney General for the U.S. State of Minnesota, who issued a memorandum in 1995 stating that 'persons outside of Minnesota who transmit information via the Internet knowing that information will be disseminated in Minnesota are subject to jurisdiction in Minnesota courts for violations of state criminal and civil laws.'[134] Even if this memorandum continued to be a valid expression of Minnesota law, there are significant practical limits to Minnesota's ability to assert its jurisdiction. Similarly to the effort of the French judges in the French Yahoo! case, the Attorney General of Minnesota will probably not succeed in imposing their law on the entire Internet as there are important practical limits to their powers.

---

[133] M. Saadat, '*Jurisdiction and the Internet after Gutnick and Yahoo!*', 2005 (1) The Journal of Information, Law and Technology.

[134] Memorandum of Minnesota Attorney General (July 18, 1995).

One of the most cited cases in the U.S. is *CompuServ*[135] where CompuServ, one of America's largest ISP was sued for alleged defamatory comments made on one of their electronic forums. CompuServe ran an electronic library that carries a host of publications and collects membership fees from its subscribers in return for access. This being so, the inconsistent application of a higher standard of liability to an electronic news distributor than that which is applied to a traditional distributor would impose an undue burden on the free flow of information. The appropriate standard of liability to be applied is whether CompuServe knew or had reason to know of the alleged defamatory statements. The claimants argued that the court should hold CompuServ as publisher liable. CompuServ contended that it was only a distributor, as opposed to a publisher of the statements, and that as a distributor, it could not be held liable on the claim because it neither knew nor had reason to know of the alleged defamatory statements.[136] This case had reassured the ISP community that they were not liable for defamatory contents of their networks unless they knew or had reason to know of the specific material.[137]

Stratton Oakmont Inc. v. Prodigy Services Co.[138] set out to create new turbulence in the ISP community. Prodigy was a family-oriented ISP which 'held itself out to the public and its members as controlling the content of its computer bulletin boards'.[139] The court pointed out that Prodigy had given the impression that it exercised editorial control and as such the facts were markedly different from those in *CompuServ.* Prodigy was held liable by the court for the defamatory contents of one of their electronic bulletin boards.

In *Lunney v Prodigy*[140], the U.S. Court held that a party could not be held liable for a defamatory message where it had not 'participated in preparing the message, exercised any discretion or control over its communication, or in any way assumed responsibility'. Further, even if Prodigy was a publisher, it was entitled to qualified privilege in the same way that telephone

[135] *Cubby Inc. v. CompuServ Inc.* 776 F. Supp. 135, [S.D.N.Y. 1991].

[136] 'Normally, "one who repeats or otherwise republishes defamatory matter is subject to liability as if he had originally published it". (Restatement (Second) of Torts § 578 (1977); *Cianci v. New Times Publishing Co.,* 639 F. 2d 54, 61 (2d Cir. 1980))', per S. Anil, '*Cyberspace and the law of defamation: developing a workable model'*, Computer and Telecommunications Law Review, 2001, 7(7), 175-183, fn 28.

[137] S. Anil, '*Cyberspace and the law of defamation: developing a workable model'*, Computer and Telecommunications Law Review, 2001, 7(7), 175-183, fn 28.

[138] 1995 WL 323710, 1995 N.Y. Misc. LEXIS 229, 23 Media Law Rep. 1794 (N.Y. Sup. Ct. May 26, 1996).

[139] This quote was used as part of advertisements promoting Prodigy.

[140] 94 N.Y. 2d 242, 723 N.E. 2d 539, 701 N.Y. 2d 684 (1999).

companies are protected from claims for defamation. The key features of the decision were: (i) that qualified privilege is based upon the fact that a party plays a passive role in publication; (ii) the possible distinction between liability for defamatory emails as opposed to bulletin board messages, as sufficient control in the latter could amount to publishing; and (iii) Lunney's claim that Prodigy had been negligent in allowing defamatory remarks to be attributed to the claimant, rejected in this case, may be a possible cause of action on different facts. Given the development of the Godfrey case, the U.S. cases seem to imply a greater readiness to adapt common law principles to ensure that a 'publisher' of a statement is conditional upon significant editorial control being exercised over it.[141]

In the Canadian case of *Barrick Gold Corporation v Lopehandia*,[142] which concerned two Canadian residents (plaintiff being the resident of the province of Ontario, while the defendant resided in the province of British Columbia), the court[143] held that defendant's conduct to be 'malicious and high handed … unremitting and tenacious' involving 'defamatory publications that are vicious, spiteful, wide-ranging in substance, and world-wide in scope' the decision of first instance which stated that 'the defendant had extensively and maliciously defamed the plaintiff online' but in relation to the first instance refusal of punitive damages and denial for an injunction against the defendant on the ground that the defendant did not have assets in Ontario, and the courts of Ontario could not supervise the enforcement of the injunction against the defendant in British Columbia, however the on appeal the court granted punitive damages and injunction holding that there was a real and substantial connection between the matter and Ontario (the defamatory statements caused damage to Barrick's reputation in Ontario, were read by residents of Ontario and were accessible on an Internet message board operated by an Ontario ISP); Ontario ISPs could be stopped from distributing the plaintiff's defamatory messages; and the order 'may be enforceable in British Columbia'. This decision established not only 'that Canadian courts are willing to adapt

[141] S. Anil, '*Cyberspace and the law of defamation: developing a workable model'*, Computer and Telecommunications Law Review, 2001, 7(7), 175-183.

[142] [2004] O.J. No. 2329.

[143] Ontario Court of Appeal.

traditional legal principles to respond to the exigencies of the Internet',[144] but it highlighted the level of harm that actions in cyberspace can cause in real space.

Conclusion

As noted, cyberspace challenges prescriptive jurisdiction, adjudicative jurisdiction and enforcement jurisdiction because it is difficult to localise legally relevant conduct occurring in cyberspace. Self-regulation has the potential to resolve many, but not all of the jurisdictional problems posed by cyberspace activities, however it appears that traditional legal doctrine is still needed to fill in the legal gaps created by the structure of self-regulation.

The author is of the opinion that through harmonisation of laws, the doctrine of comity should provide guidance for reconciling disputes arising between the local territorial law and the law applicable to particular activities on the Internet as territorial sovereigns would enforce cyberspace law as a matter of comity and allow the development of self regulating cyberspace rules and law making as long as there is no threat to the sovereignty and territory of a state but is very useful for the development of e-commerce. As noted, the global phenomenon of cyberspace creates problems that cannot be dealt with by territorial-based legal systems. The author agrees with scholars[145] who argue that cyber market creates slowly its own electronic *lex mercatoria*, which is reflected in the new state and international laws regulating electronic transactions.

---

[144] B Freedman, '*Ontario Court Issues Injunction Against Internet Defamation*', CLE Society of British Columbia (available at http://www.cle.bc.ca/CLE/Analysis/Collection/04-12345-barrick). S. Anil, '*Cyberspace and the law of defamation: developing a workable model'*, Computer and Telecommunications Law Review, 2001, 7(7), 175-183.

[2004] O.J. No. 2329.

Ontario Court of Appeal.

B Freedman, '*Ontario Court Issues Injunction Against Internet Defamation*', CLE Society of British Columbia (available at http://www.cle.bc.ca/CLE/Analysis/Collection/04-12345-barrick).

[145] See for example G. I. Zekos, in '*State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction*', International Journal of Law and IT (2007) 15 (1).