Published on e-First 2 October 2018

SKETCHING THE MARGINS OF A BORDERLESS WORLD

Examining the Relevance of Territoriality for Internet Jurisdiction

The concept of jurisdiction in international law has served as a divisive and contentious subject among academics and practitioners alike. With the advent of the Internet, which serves as a revolutionary, borderless medium of communication, the controversies in this field have further increased. The lack of international consensus in the area of Internet jurisdiction is acutely demonstrated by the varying practices of municipal courts in addressing the offences of hate speech and criminal defamation. This paper will examine the applicability of traditional bases of jurisdiction to cyberspace, focusing particularly on the territorial principle. It will also recommend a refinement to the territorial principle in order to alleviate the jurisdictional problems posed by the unique nature of cyberspace.

CHIA Chen Wei*
LLB (Hons) (Singapore Management University).

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

I. Introduction

1 The Internet has been said to be the most important invention in the history of mankind.[2] While it has served as an invaluable tool for generating jobs, promoting cross-border trade and facilitating the flow of information, the regulation of this medium has proven problematic

* This article is based on a directed research paper written under the supervision of Associate Professors of Law Chen Siyuan and Warren B Chik in the author's third year of study. The author thanks both Professors Chen and Chik for their invaluable guidance and support. Any errors and omissions remain his.

1 John Perry Barlow, "A Declaration of the Independence of Cyberspace" (1996).

2 John Brockman, *The Greatest Inventions of the Past 2,000 Years* (Simon and Schuster, 2000) at p 51; Jason Whittaker, *The Internet: The Basics* (Psychology Press, 2002) at p xi; Wei Xiang, Kan Zheng & Xuemin (Sherman) Shen, *5G Mobile Communications* (Springer, 2016) at p 677.

due to its revolutionary nature. Traditional notions of jurisdiction, when applied in the realm of cyberspace, have resulted in individuals being subjected to the concurrent, overlapping jurisdiction of multiple states. While concurrent jurisdiction *per se* may be par for the course in international law,[3] the borderless nature of the Internet potentially allows for hundreds of different states to claim jurisdiction over any given act committed in cyberspace; this causes confusion over the applicable legal regime in many situations. This problem is compounded when one scrutinises the nature of offences such as hate speech and criminal defamation – how strictly any particular State regulates such offences is highly dependent on their individual cultures, contexts and histories.[4] That being the case, is it fair to subject an alleged wrongdoer to multiple, potentially conflicting legal regimes? Should we deviate from traditional principles of jurisdiction when examining offences that occur over the Internet?

2 This article seeks to answer these questions by delving into the jurisprudence surrounding international law jurisdiction in cyberspace. It examines the approaches undertaken by various states, focusing specifically on the areas of hate speech and criminal defamation. The examination begins with the introduction of the concept of jurisdiction under international law.[5] Subsequently, the relevance of the territorial principle in the context of cyberspace is examined by comparing its usefulness with other bases of international law jurisdiction.[6] While it may appear counterintuitive to utilise the territorial principle for the borderless medium of cyberspace, this article will show that the former remains an important cornerstone of international law. In doing so, the nature of hate speech and criminal defamation will be examined in detail. The next part[7] analyses whether the subjective territorial principle should apply to the exclusion of the objective territorial principle, or *vice versa*. Finally, the article will suggest calibrated improvements to refine the application of the territorial principle in cyberspace, while assessing whether such refinements accord with established principles of jurisdiction under international law.[8]

3 Dan Jerker B Svantesson, *Private International Law and the Internet* (Kluwer Law International, 2007) at p 246; Cedric Ryngaert, *Jurisdiction in International Law* (Oxford University Press, 2nd Ed, 2015) at p 14.

4 Michael Saadat, "Jurisdiction and the Internet after Gutnick and Yahoo!" (2005) (1) JILT 1 at 19; Dragos Cucereanu, *Aspects of Regulating Freedom of Expression on the Internet* (Intersentia, 2008) at p 16; Natalie Alkiviadou, "Regulating Internet Hate: A Flying Pig?" (2016) 7 JIPITEC 216 at 221, para 12.

5 See paras 3–15 below.

6 See paras 16–48 below.

7 See paras 49–71 below.

8 See paras 72–89 below.

II. Concept of jurisdiction under international law

A. Definition of "jurisdiction"

3 In our context, jurisdiction, as stated by James Crawford, refers to "a state's competence under international law to regulate the conduct of natural and juridical persons".[9] It is "one of the most obvious forms of the exercise of sovereign power",[10] with states being able to exercise three different forms of jurisdiction: prescriptive, enforcement, and adjudicative jurisdiction.

4 Prescriptive jurisdiction refers to a State's power to legislate and make law.[11] In the past, states were afforded wide-ranging discretion in exercising prescriptive jurisdiction. This was encapsulated in the seminal decision in *The Case of the SS Lotus*[12] ("*SS Lotus*") by the Permanent Court of International Justice in 1927, where the court declared that states may exercise their jurisdiction however they please unless there were specific "prohibitive rules" that operated to restrict that exercise.[13] However, the tide of international law has since turned.[14] Now, states may only exercise jurisdiction extraterritorially when they can avail themselves of a recognised head of jurisdiction under international law.[15] Similar considerations apply to the concept of adjudicative jurisdiction, which will be examined below.[16]

9 James Crawford, *Brownlie's Principles of Public International Law* (Oxford University Press, 8th Ed, 2012) at p 537.

10 *Legal Status of Eastern Greenland (Denmark v Norway)* (1933) PCIJ Series A/B No 53 at 48; Cedric Ryngaert, *Jurisdiction in International Law* (Oxford University Press, 2nd Ed, 2015) at p 26.

11 James Crawford, *Brownlie's Principles of Public International Law* (Oxford University Press, 8th Ed, 2012) at p 456; Malcolm Shaw, *International Law* (Cambridge University Press, 7th Ed, 2014) at p 679; Cedric Ryngaert, *Jurisdiction in International Law* (Oxford University Press, 2nd Ed, 2015) at p 5.

12 (1927) PCIJ Series A No 10.

13 *The Case of the SS Lotus* (1927) PCIJ Series A No 10 at 19.

14 *Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v Belgium)* (2002) ICJ Rep 3 (Separate Opinion of Guillaume J) at [4]; James Crawford, *Brownlie's Principles of Public International Law* (Oxford University Press, 8th Ed, 2012) at pp 456–457.

15 *Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v Belgium)* (2002) ICJ Rep 3 (Separate Opinion of Guillaume J) at [4]; James Crawford, *Brownlie's Principles of Public International Law* (Oxford University Press, 8th Ed, 2012) at pp 456–457.

16 *Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v Belgium)* (2002) ICJ Rep 3 (Separate Opinion of Guillaume J) at [4].

5 Enforcement jurisdiction refers to the ability of a State to take executive action to enforce its laws.[17] States that seek to exercise their enforcement jurisdiction in a foreign state's territory usually rely on mutual legal assistance treaties in order to justify their taking of executive action outside their territorial boundaries.[18]

6 Finally, adjudicative jurisdiction refers to a State's ability to take judicial action pursuant to the laws of a country.[19] For a State to exercise extraterritorial adjudicative jurisdiction, it must avail itself of a recognised head of jurisdiction under international law; in this sense, it is much like prescriptive jurisdiction.[20] This concept of adjudicative jurisdiction will form the central focus of this article.

B. Heads of jurisdiction

7 Under international law, states may only claim adjudicative jurisdiction over an individual when they have a substantial connection to him or her.[21] Such a substantial connection exists when "links between a person, property, or an event and a state are sufficiently strong to give the state regulatory power over that person, property, or event", and is required for states to justify the extension of their powers beyond their territorial boundaries.[22] There are five internationally recognised heads of jurisdiction that serve to establish a substantial

17 James Crawford, *Brownlie's Principles of Public International Law* (Oxford University Press, 8th Ed, 2012) at p 456; Malcolm Shaw, *International Law* (Cambridge University Press, 7th Ed, 2014) at p 680; Cedric Ryngaert, *Jurisdiction in International Law* (Oxford University Press, 2nd Ed, 2015) at p 5.

18 United Nations Office on Drugs and Crime, *Manual on Mutual Legal Assistance and Extradition* (2012) <https://www.unodc.org/documents/organized-crime/Publications/Mutual_Legal_Assistance_Ebook_E.pdf> (accessed 8 December 2017); Yonatan Moskowitz, "MLATS and the Trusted Nation Club: The Proper Cost of Membership" (2016) 41 Yale J Int'l L Online 1 at 3.

19 James Crawford, *Brownlie's Principles of Public International Law* (Oxford University Press, 8th Ed, 2012) at p 456; Malcolm Shaw, *International Law* (Cambridge University Press, 7th Ed, 2014) at p 680; Cedric Ryngaert, *Jurisdiction in International Law* (Oxford University Press, 2nd Ed, 2015) at p 5.

20 *Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v Belgium)* (2002) ICJ Rep 3 (Separate Opinion of Guillaume J) at [4].

21 *Fisheries Case (UK v Norway)* (1951) ICJ Rep 116 at 131–134; *Nottebohm Case (Second Phase) (Liechtenstein v Guatemala)* (1955) ICJ Rep 4 at 23; *Barcelona Traction, Light and Power Co, Ltd* (1970) ICJ Rep 3 at 35; Cedric Ryngaert, *Jurisdiction in International Law* (Oxford University Press, 2nd Ed, 2015) at p 119.

22 Diane Rowland, Uta Kohl & Andrew Charlesworth, *Information Technology Law* (Routledge, 4th Ed, 2012) at p 29. See also Alex Mills, "Rethinking Jurisdiction in International Law" (2014) 81(1) BYBIL 187 at 207; Dan Svantesson, "A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft" (2015) 109 AJIL 69 at 73; and Dan Svantesson, *Private International Law and the Internet* (Wolters Kluwer, 3rd Ed, 2016) at p 10.

connection between a State and an individual: the territorial principle, the nationality principle, the protective principle, the universality principle and the passive personality principle.[23] Each head will be briefly described.

(1) Territoriality principle

8 The notion of territorial jurisdiction stems from the principle of sovereign equality of states.[24] Under this principle, states, being equal members of the international community,[25] possess equal rights and responsibilities, including the inviolable right to their territorial integrity and political independence.[26] Crucial to a State's inviolable right to its territorial integrity and political independence is its ability to exercise exclusive adjudicative jurisdiction within its territory.[27] States are, after all, responsible for the conduct of law and the maintenance of good order within their territory.[28]

9 Thus, where a crime or offence is committed within a State's territory,[29] it will naturally have the right to exercise its adjudicative jurisdiction over it.[30] The importance of the territorial principle as a base of jurisdiction has been emphasised on various occasions, in cases such as the *Island of Palmas Case (Netherlands v USA)*,[31] *Barcelona Traction, Light and Power Co, Ltd*[32] and *Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v Belgium)*[33] ("*Arrest Warrant*"). As Guillaume J stated in *Arrest Warrant*, states are presumed to have

23 James Crawford, *Brownlie's Principles of Public International Law* (Oxford University Press, 8th Ed, 2012) at pp 458–463; Cedric Ryngaert, *Jurisdiction in International Law* (Oxford University Press, 2nd Ed, 2015) at p 22.

24 James Crawford, *Brownlie's Principles of Public International Law* (Oxford University Press, 8th Ed, 2012) at p 12; Cedric Ryngaert, *Jurisdiction in International Law* (Oxford University Press, 2nd Ed, 2015) at p 25.

25 Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations (UN Doc A/RES/25/2625) (24 October 1970).

26 Charter of the United Nations (1 UNTS XVI) (24 October 1945; entry into force 31 August 1965) Art 2.

27 United Nations General Assembly, Non-interference in the Internal Affairs of States (UN Doc A/RES/34/101) (14 December 1979).

28 Carlson Anyangwe, *Criminal Law: The General Part* (Langaa RPCIG, 2015) at p 131.

29 It must be noted that applying the concept of "territory" to cyberspace brings about a unique set of challenges; for instance, numerous Internet service providers that are located in various jurisdictions may be involved in any given Internet publication. The problem of concurrent jurisdiction will be addressed in greater detail at paras 72–89 below.

30 *The Case of the SS Lotus* (1927) PCIJ Series A No 10 at 18.

31 (1928) 2 RIAA 829 at 838.

32 (1970) ICJ Rep 3 at [42].

33 (2002) ICJ Rep 3 (Joint Separate Opinion of Higgins, Kooijmans and Buergenthal JJ) at [49].

"exclusive competence in regard to [their] own territory".[34] Having said that, while a State's jurisdiction is closely linked with its territory, it is not exclusively so.[35] Jurisdiction is "certainly territorial",[36] but the territoriality principle is not the only base through which a State may exercise jurisdiction.

(2) Nationality principle

10 Nationality has been described by the International Court of Justice ("ICJ") to be a "legal bond having as its basis a social fact of attachment, a genuine connection of existence, interests and sentiments, together with the existence of reciprocal rights and duties".[37] This formulation has been widely recognised by states.[38] It is through these reciprocal rights and duties that a State possesses adjudicative jurisdiction over its citizens. Thus, a State may assert jurisdiction over an individual who was a national at the time the offence was committed.[39]

11 While the presence of the territoriality and nationality principles may result in situations where multiple states possess concurrent jurisdiction over an individual (for instance, where an individual from State A commits an offence within the territory of State B), this may limit rather than increase international conflict. As noted by Cedric Ryngaert, "the territorial State might arguably welcome the exercise of jurisdiction by the State of nationality of the offender, as this may relieve it of the task of harnessing its resources to prosecute the offense".[40]

34 *Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v Belgium)* (2002) ICJ Rep 3 (Separate Opinion of Guillaume J) at [4].

35 Malcolm Shaw, *International Law* (Cambridge University Press, 7th Ed, 2014) at p 679.

36 *The Case of the SS Lotus* (1927) PCIJ Series A No 10 at 18.

37 *Nottebohm Case (Second Phase) (Liechtenstein v Guatemala)* (1955) ICJ Rep 4 at 23.

38 *Nottebohm Case (Second Phase) (Liechtenstein v Guatemala)* (1955) ICJ Rep 4 at 23.

39 Harvard Research on International Law, "Draft Convention on Jurisdiction with Respect to Crime" (1935) 29 AJIL 439 at 519; Michael Akehurst, "Jurisdiction in International Law" (1972–1973) 46 BYBIL 145 at 156; James Crawford, *Brownlie's Principles of Public International Law* (Oxford University Press, 8th Ed, 2012) at p 460.

40 Cedric Ryngaert, *Jurisdiction in International Law* (Oxford University Press, 2nd Ed, 2015) at p 82.

(3) Protective principle

12 Issues of national security are of utmost importance to a State. The protective principle provides that states may claim extraterritorial adjudicative jurisdiction over acts committed abroad that are prejudicial to the security of the particular State concerned,[41] such as incidents of drug smuggling or the counterfeiting of foreign currency.[42] While the protective principle is well established under international law, it may be easily abused; states may claim extravagant extraterritorial jurisdiction, also known as excessive extraterritorial jurisdiction, simply because they deem an act to constitute a serious threat to their security.[43]

(4) Universality principle

13 The universality principle is unique in that it does not focus specifically on drawing a substantial connection between a particular State and an offence. Instead, it is based "solely on the nature of a crime",[44] deriving its legitimacy from the basis that there are certain crimes that are "regarded as particularly offensive to the international community as a whole".[45] Hence, the universality principle may only be invoked as a basis for extraterritorial jurisdiction in situations involving heinous crimes, such as genocide and crimes against humanity.[46]

(5) Passive personality principle

14 The passive personality principle, which has been described as potentially "the most aggressive basis for extraterritorial jurisdiction",[47]

41 *Joyce v Director of Public Prosecutions* [1946] AC 347 at 358; *United States v Yousef* 327 F 3d 56 at 110, [148] (2nd Cir, 2003); Malcolm Shaw, *International Law* (Cambridge University Press, 7th Ed, 2014) at p 690.

42 Criminal Procedure Code of the Kingdom of Belgium 1808 Arts 10, 2 and 3; *United States v Newball* 524 F Supp 715 at 716 (1981); *United States v Cardales* 168 F 3d 548 at 553 (1999).

43 James Crawford, *Brownlie's Principles of Public International Law* (Oxford University Press, 8th Ed, 2012) at p 462; Malcolm Shaw, *International Law* (Cambridge University Press, 7th Ed, 2014) at p 689.

44 Cedric Ryngaert, *Jurisdiction in International Law* (Oxford University Press, 2nd Ed, 2015) at p 88.

45 Malcolm Shaw, *International Law* (Cambridge University Press, 7th Ed, 2014) at p 690.

46 *Jorgic v Germany* [2007] ECtHR 74613/01 at [69]; Institut de Droit International, "Seventeenth Commission: Universal Criminal Jurisdiction over Genocide, Crimes against Humanity and War Crimes" (2005) http://www.idi-iil.org/app/uploads/2017/06/2005_kra_03_en.pdf (accessed 8 December 2017).

47 Cedric Ryngaert, *Jurisdiction in International Law* (Oxford University Press, 2nd Ed, 2015) at p 83.

can be considered as the most controversial head of jurisdiction.[48] Under this principle, the nationality of the victim constitutes a sufficient jurisdictional link under international law even if the offending conduct takes place outside a state's territory; thus, State A may claim jurisdiction over a citizen of State B if the latter injures a citizen of State A, even if the injury took place within State B's territory.[49] Given the passive personality principle's scope of application, it is unsurprising that it has been vehemently criticised as disrespecting the territorial sovereignty of a foreign State and increasing uncertainty in international law.[50] Nevertheless, recent state practice has carved out a niche for the passive personality principle in the form of *aut dedere aut judicare* (obligation to extradite or prosecute) provisions in international conventions to address offences involving international terrorism.[51] However, this principle remains highly controversial outside of this specific field.

15 While all of the aforementioned bases of jurisdiction are distinct from each other, they serve to fulfil the "cardinal principle" of establishing a substantial connection between the subject matter of jurisdiction and the reasonable interests of the State in question in order for the latter to claim regulatory competence.[52] The territorial principle, by virtue of its versatility, has cemented its place in international law as an indispensable base of jurisdiction for establishing this substantial connection. However, the importance of the territorial principle has been challenged in recent times, particularly with regard to its applicability in cases concerning the Internet.

48 Donnedieu de Vabres, *Les Principes Modernes du Droit Penal International* (Librairie du Recueil Sirey, 1928) at p 170; James Crawford, *Brownlie's Principles of Public International Law* (Oxford University Press, 8th Ed, 2012) at p 461.

49 James Crawford, *Brownlie's Principles of Public International Law* (Oxford University Press, 8th Ed, 2012) at p 461; Cedric Ryngaert, *Jurisdiction in International Law* (Oxford University Press, 2nd Ed, 2015) at p 83.

50 James Crawford, *Brownlie's Principles of Public International Law* (Oxford University Press, 8th Ed, 2012) at p 461; Cedric Ryngaert, *Jurisdiction in International Law* (Oxford University Press, 2nd Ed, 2015) at p 83.

51 Convention on Offences and Certain Other Acts Committed on Board Aircraft (220 UNTS 10106) (14 September 1963; entry into force 4 December 1969) Art 4(b); Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (222 UNTS 29004) (10 March 1988; entry into force 1 March 1992) Art 6(2)(b); Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (1465 UNTS 85) (4 February 1985; entry into force 26 June 1987) Art 5(1)(c).

52 James Crawford, *Brownlie's Principles of Public International Law* (Oxford University Press, 8th Ed, 2012) at p 457.

III. Relevance of territorial principle in cyberspace

A. Inapplicability of territorial principle in a borderless world?

16 It has been argued that the territorial principle is ill-suited to apply to the revolutionary medium of the Internet. Alex Mills, for instance, posits that:[53]

> The primacy of territorial regulation is coming under challenge as a result of (arguably) 'de-territorialised' communications technologies, in particular the internet, although the extent to which such developments pose more than a complex problem of application for the existing legal framework remains contentious.

17 Similarly, Phillip Kastner and Frederic Mégrét state that:[54]

> It is evident that the territoriality principle, one of the principles on which national criminal jurisdiction is usually based, is only of limited use in the context of cybercrime. There may be no single *locus delicti* in the traditional sense; several offenders may act together yet from different locations; experienced crackers can route their activities through portals in jurisdictions without specific legislation; and digital evidence may be dispersed on servers located in different jurisdictions.

18 The prevailing concern about the continued usefulness of the territorial principle naturally leads to the question of whether there is an alternative base of jurisdiction that should dethrone the territorial principle in cyberspace cases.

B. Relying on alternative bases of jurisdiction

19 Commentators have argued for either the principle of universal jurisdiction or the protective principle to assume greater importance in the realm of cyberspace.

(1) Assessing universal jurisdiction

20 The main argument for the principle of universal jurisdiction is that it allows states to act swiftly in prosecuting cybercrimes without being hampered by overly legalistic considerations of jurisdiction;

53 Alex Mills, "Rethinking Jurisdiction in International Law" (2014) 81(1) BYBIL 187 at 197.

54 Philip Kastner & Frédéric Mégret, "International Legal Dimensions of Cybercrime" in *Research Handbook on International Law and Cyberspace* (Nikolaos Tsagourias & Russell Buchan eds) (Edward Elgar Publishing, 2015) at p 201.

the need for "a truly universal jurisdiction" is derived from "the very nature of cybercrime".[55] This rationale is clearly based on concerns of practicality.

21 However, the very basis of universal jurisdiction is grounded on the recognition by the international community of universally condemned offences.[56] Such offences must be so egregious that they "shock the conscience of humanity".[57] It is unlikely that cybercrimes such as hate speech, which involves the incitement of hatred or violence against persons,[58] or criminal defamation, which involves damage to an individual's dignity and reputation,[59] would be viewed by the international community as a whole to be equivalent to the heinousness of crimes such as genocide. It is especially difficult to obtain an international consensus on the degree of prohibition of hate speech and criminal defamation because of the varying degrees to which freedom of expression is allowed in different jurisdictions.[60] As Natalie Alkiviadou aptly stated:[61]

> A State's approach to the issue of restricting forms of expression will be affected by its own 'political, moral, cultural, historical and constitutional values' and it is, in fact, this sharp divergence of legal culture in the realm of speech between the USA and Europe which has hindered the efficacy of any regulatory measures …

22 The US in particular has consistently and repeatedly ruled that there is no hate speech exception to the First Amendment, which guarantees the right to freedom of expression.[62] Thus, in the recent

55 Hans Corell, Under-Secretary-General for Legal Affairs, The Legal Counsel of the United Nations, "The Rule of Law in the Global Village: Issues of Sovereignty and Universality", introductory and concluding remarks at the Symposium on the Occasion of the Signing of the United Nations Convention against Transnational Organised Crime: Panel on "The Challenge of Borderless Cyber-crime" (14 December2000) <http://legal.un.org/ola/media/info_from_lc/cybercrime.pdf> (accessed 8 December 2017).

56 William Stahl, "The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity" (2011) 40 Ga J Int'l & Comp L 247 at 269.

57 Paul Stockton & Michele Golabek-Goldman, "Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat" (2014) 25 Stan L & Pol'y Rev 211 at 246.

58 *Gündüz v Turkey* [2004] ECtHR 35071/97 at [40]; *Vejdeland v Sweden* [2012] ECtHR 1813/07 at [44]; *Delfi AS v Estonia* [2015] ECtHR 64569/09 at [110].

59 Benedict John Anstey, "Criminal Defamation and Reputation As 'Honour': A Cross-jurisdictional Perspective" (2017) 9 *Journal of Media Law* 132 at 134.

60 Michael Saadat, "Jurisdiction and the Internet after Gutnick and Yahoo!" (2005) 1 JILT 1 at 19.

61 Natalie Alkiviadou, "Regulating Internet Hate: A Flying Pig?" (2016) 7 JIPITEC 216 at 221, para 12.

62 *National Socialist Party of America v Village of Skokie* 432 US 43 at 44 (1977).

Supreme Court of the United States ("SCOTUS") case of *Matal v Tam*,[63] the court unequivocally stated that "the proudest boast of our free speech jurisprudence is that we protect the freedom to express 'the thought that we hate'".[64]

23 In sharp contrast, the European Court of Human Rights ("ECtHR") has consistently emphasised the need to guard against hate speech. Article 10 of the European Convention on Human Rights[65] clearly imposes limits on speech to protect "the reputation or rights of others",[66] which has been interpreted by the ECtHR on multiple occasions to stand for a prohibition against hate speech and criminal defamation.[67] In the ECtHR case of *Gündüz v Turkey*,[68] for instance, it was stated that instances of hate speech, which "spread, incite, promote or justify hatred based on intolerance", "are not protected under Article 10 of the Convention [on Human Rights]".[69]

24 States are similarly divided over the offence of criminal defamation. In the UK, for instance, criminal defamation laws, although subsisting, have fallen into disuse; since the 1970s, there have not been any public or private prosecutions for criminal defamation.[70] In contrast, the state of South Australia, which recognises criminal defamation under s 237(1) of the Criminal Law Consolidation Act of 1935,[71] has brought prosecutions for criminal defamation as recently as in 2009.[72] Given these sharply contrasting legal backdrops, it is highly doubtful that there would be unified consensus on a doctrine of universal jurisdiction for hate speech and criminal defamation. The application of universal jurisdiction would be more apt for cybercrimes such as the

63 137 SCt 1744 (2017).

64 *Matal v Tam* 137 SCt 1744 at 1764 (2017).

65 Convention for the Protection of Human Rights and Fundamental Freedoms (Eur TS No 5, 213 UNTS 221, 1953 UKTS No 71) (4 November 1950; entry into force 3 September 1953).

66 Convention for the Protection of Human Rights and Fundamental Freedoms (Eur TS No 5, 213 UNTS 221, 1953 UKTS No 71) (4 November 1950; entry into force 3 September 1953) Art 10.

67 *Gündüz v Turkey* [2004] ECtHR 35071/97 at [40]; *Vejdeland v Sweden* [2012] ECtHR 1813/07 at [44]; *Delfi AS v Estonia* [2015] ECtHR 64569/09 at [110].

68 [2004] ECtHR 35071/97.

69 *Gündüz v Turkey* [2004] ECtHR 35071/97 at [40]–[41].

70 Article 19 (Global Campaign for Free Expression), "Briefing Note on International and Comparative Defamation Standards" (February 2004) <https://www.article19.org/data/files/pdfs/analysis/defamation-standards.pdf> (accessed 8 December 2017).

71 Act No 2252/1935.

72 Craig Burgess, "Criminal Defamation in Australia: Time to Go or Stay?" (2013) 20 *Murdoch University Law Review* 1 at 3.

online distribution of child pornography, which has been widely recognised as an abhorrent offence in a large number of jurisdictions.[73]

25 The lack of international consensus on the offence of hate speech is evinced in how the latter had to be relegated to the Budapest Convention on Cybercrime's[74] ("Budapest Convention") Additional Protocol, rather than included in the main body of the convention, which contained offences such as fraud, copyright and child pornography.[75] The Budapest Convention is the first and only successful international treaty pertaining to cybercrime; it had to circumscribe the scope of its framework to achieve its success, thus demonstrating the difficulties of achieving international consensus and substantive legal harmonisation towards the regulation of cybercrimes.[76] These very same difficulties continue to hinder the international community's broader efforts to establish a global convention against cybercrime that comprehensively regulates different aspects of cyber activity.[77]

(2) Assessing the protective principle

26 The allure of the protective principle's application in cyberspace is that it would, similarly to the universal jurisdiction principle, "reduce the number of conflicting jurisdictional claims" and provide nations with stronger capabilities to prosecute cybercrimes.[78] The protective principle, as earlier mentioned, would only apply to cybercrimes that endanger a nation's security interests.[79] Cybercrimes that do not rise to

73 Convention on Cybercrime (Eur TS No 185) (23 November 2001; entry into force 1 July 2004) Art 9; Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA. See also Crimes and Criminal Procedure 18 USC § 2251 and s 474.20 of the Australian Criminal Code Act 1995 (Act No 12 of 1995).

74 Convention on Cybercrime (Eur TS No 185) (23 November 2001; entry into force 1 July 2004).

75 Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (Eur TS 189) (28 January 2003; entry into force 1 March 2006).

76 Diane Rowland, Uta Kohl & Andrew Charlesworth, *Information Technology Law* (Routledge, 4th Ed, 2012) at p 26.

77 United Nations, Twelfth United Nations Congress on Crime Prevention and Criminal Justice, *Recent Developments in the Use of Science and Technology by Offenders and by Competent Authorities in Fighting Crime, Including the Case of Cybercrime* (UN Doc A/CONF.213/9) (2010) at paras 16 and 19–23; Jonathan Clough, "A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation" (2015) 40(3) *Monash University Law Review* 698 at 733.

78 Paul N Stockton & Michele Golabek-Goldman, "Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat" (2014) 25 Stan L & Pol'y Rev 211 at 249.

79 See para 12 above.

that level, such as those that result only in economic damage, are excluded from the ambit of this principle.[80]

27 Given the above, the protective principle is likely to be confined to situations of cyberterrorism that target critical state infrastructure, such as the national defence capabilities of a State.[81] Needless to say, cases involving hate speech or criminal defamation would fall outside this ambit. Accordingly, while the two aforementioned bases of jurisdiction may play an important role in allowing for states to exercise jurisdiction over specific types of cybercrimes, namely those of a highly heinous or destructive nature, the vast majority of cybercrimes, including criminal defamation and hate speech, are nevertheless more appropriately governed by the territorial principle.

28 This approach which emphasises the continued pervasiveness of the territorial principle is also consistent with the aforementioned Budapest Convention. Article 22 of the Budapest Convention expressly affirms the application of the territorial principle and the nationality principle, with territoriality serving as the main jurisdictional principle.[82] This has been followed in a number of other multilateral legal instruments.[83]

C. Continued application of territorial principle

29 Having demonstrated the continuing appeal of the territorial principle as a base of jurisdiction for most, if not all, cybercrimes, this article will now explore the different ways in which it applies. Traditionally, the territorial principle may manifest in two forms: (a) subjective territoriality; and (b) objective territoriality.[84] A State may

80 *Barcelona Traction, Light and Power Co, Ltd* (1970) ICJ Rep 3 at [87]; Paul Stockton & Michele Golabek-Goldman, "Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat" (2014) 25 Stan L & Pol'y Rev 211 at 257.

81 Gabriel Weimann, "Cyberterrorism: How Real Is the Threat?" *United States Institute of Peace* (December 2004) <https://www.usip.org/sites/default/files/sr119.pdf> (accessed 8 December 2017). See also Marianne Wade & Almir Maljevic, *A War on Terror? The European Stance on a New Threat, Changing Laws and Human Rights Implications* (Springer Science & Business Media, 2009) at p 66.

82 Convention on Cybercrime (Eur TS No 185) (23 November 2001; entry into force 1 July 2004) Art 22; Cedric Ryngaert, *Jurisdiction in International Law* (Oxford University Press, 2nd Ed, 2015) at p 53.

83 Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, Art 9(1)(a); Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, Art 10(1)(a).

84 Diane Rowland, Uta Kohl & Andrew Charlesworth, *Information Technology Law* (Routledge, 4th Ed, 2012) at p 30; Malcolm Shaw, *International Law*

(*cont'd on the next page*)

avail itself of the subjective territorial principle when an act has been initiated in the territory of a State, but completed abroad.[85] This is to be contrasted with the objective territorial principle, under which a State may assert jurisdiction if any essential constituent element of a crime is consummated within a State's territory.[86] The operation of these two principles has been illustrated by Anders Henrikson, with reference to the 11 September 2001 terrorist attacks in the US:[87]

> As the attacks were completed on US territory, the Americans had jurisdiction over the attacks on the basis of objective territoriality. But since a substantial part of the planning and preparation of the attacks occurred elsewhere, most notably in Afghanistan and Germany, other states could derive a claim of jurisdiction on the basis of subjective territoriality.

30 Thus, they operate as two halves of a whole, with James Crawford observing that "the effect of the two principles combined is that whenever the constituent elements of a crime occur across an interstate boundary both states have jurisdiction".[88] These formulations will be examined according to their use and application by various jurisdictions in the context of cyberspace. Specifically, jurisprudence from the US, European Union states and Australia will be examined. Reference will be made not only to criminal cases, but also civil cases, due to the relatively underdeveloped state of transnational criminal law jurisprudence in the field of the Internet; such transnational civil cases apply international law principles of jurisdiction consistently with transnational criminal law cases.

(1) Subjective territorial principle

31 Commentators have described the operation of the subjective territorial principle over Internet-related offences as the "country of origin" approach.[89] The offences of hate speech or criminal defamation over the Internet are commonly accepted to have been initiated from the

(Cambridge University Press, 7th Ed, 2014) at p 684; Cedric Ryngaert, *Jurisdiction in International Law* (Oxford University Press, 2nd Ed, 2015) at p 52.

85 Cedric Ryngaert, *Jurisdiction in International Law* (Oxford University Press, 2nd Ed, 2015) at p 52.

86 James Crawford, *Brownlie's Principles of Public International Law* (Oxford University Press, 8th Ed, 2012) at p 458; Cedric Ryngaert, *Jurisdiction in International Law* (Oxford University Press, 2nd Ed, 2015) at p 52.

87 Anders Henrikson, *International Law* (Oxford University Press, 2017) at p 88.

88 James Crawford, *Brownlie's Principles of Public International Law* (Oxford University Press, 8th Ed, 2012) at p 459.

89 Chris Reed, *Internet Law: Text and Materials* (Cambridge University Press, 2004) at p 230; Uta Kohl, *Jurisdiction and the Internet: Regulatory Competence over Online Activity* (Cambridge University Press, 2007) at p 164; Graham Smith, *Internet Law and Regulation* (Sweet & Maxwell, 2007) at p 507.

State that hosts a particular website (through the presence of data servers within that State's territory).[90] Thus, in states that host a large amount of data servers, the subjective approach is "of great practical importance in fighting … international cybercrime".[91]

32 In the US, the Telecommunications Act of 1996[92] applies to regulate content hosted by websites located in data servers in the US; § 508, for instance, indicates that the jurisdiction of the State extends to those "using any facility or means of interstate or foreign commerce, including the mail, or within the special maritime and territorial jurisdiction of the United States".[93] Similarly, in Europe, there has been acceptance of the country of origin approach in the European Directive on Electronic Commerce.[94] While this directive focuses on the regulation of electronic commerce rather than Internet content, this nevertheless evinces the acceptance of the country of origin approach as a basis of jurisdiction on the Internet. In Australia, the use of the subjective territorial principle to regulate cyberspace may be seen in Sch 7 to the Broadcasting Services Act 1992.[95] Specifically, the Australian Communications and Media Authority has the responsibility and ability to regulate Internet content hosts, with it being able to issue take down notices to hosts that are found to be hosting "prohibited content" in Australia.[96]

33 However, the subjective territorial principle alone does not offer a satisfactory solution to the problem of Internet jurisdiction, especially when dealing with the offences of hate speech and criminal defamation. First, relying solely on the subjective territorial principle would result in a situation where only a few states may exercise jurisdiction over the crimes of hate speech and criminal defamation. Multinational companies that operate Internet-related businesses place a premium on the criteria of fiscal benefits and infrastructural support when deciding on the placement of their data servers: Ireland, for instance, has proven to be extremely popular given its generous tax laws, temperate climate

90 Uta Kohl, *Jurisdiction and the Internet: Regulatory Competence over Online Activity* (Cambridge University Press, 2007) at p 164; Graham J H Smith, *Internet Law and Regulation* (Sweet & Maxwell, 2007) at p 507.

91 Anders Henrikson, *International Law* (Oxford University Press, 2017) at p 88.

92 47 USC (US).

93 Telecommunications Act of 1996 47 USC § 508 (2012).

94 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market, Art 3. Article 3 states: "[T]he information society services provided by a service provider established on its territory comply with the national provisions applicable in the Member State".

95 Broadcasting Services Act 1992 (No 110 of 1992) Sch 7.

96 Broadcasting Services Act 1992 (No 110 of 1992) Sch 7, cll 47(2), 56(2) and 62(2).

(for the cooling of data systems) and pro-business policies.[97] Data servers on its territory support the operations of technological giants like Apple, Google and Facebook.[98] A strict application of the subjective territorial principle without regard to other bases of jurisdiction would result in a situation where only Ireland would have jurisdiction over offences of hate speech or criminal defamation occurring over Facebook, regardless of whether these posts are read within or outside Ireland, which would constitute an absurd result.

34 Secondly, the subjective territorial principle could result in certain jurisdictions becoming safe havens for hate speech or criminal defamation. As earlier mentioned, the US, by virtue of the First Amendment to the US Constitution, does not criminalise hate speech.[99] In the same vein, there are no federal laws in the US providing for the offence of criminal defamation; in fact, the SCOTUS has on previous occasions declared several state-level criminal defamation laws as unconstitutional.[100] However, the US hosts a large number of data servers across its 50 states; in the state of Virginia, there is an estimated 4.6m square feet of commissioned data centre space.[101] A strict application of the subjective territorial principle would result in companies such as Amazon, which use data servers in Virginia to conduct a substantial portion of their web services,[102] not having to concern themselves over the issue of hate speech occurring on their platform simply because the US does not recognise hate speech as an offence. All things considered, there is a need to utilise both the objective territorial principle as well as the subjective territorial principle.

97 Mila Gascó, *Proceedings of the 12th European Conference on e-Government* (Academic Conferences Ltd, 2012) at p 292; Ina Kerschner & Maryte Somare, *Taxation in a Global Digital Economy* (Linde Verlag GmbH, 2017) at p 130; Host in Ireland website <http://hostinireland.com/faqs/> (accessed 8 December 2017).

98 Henry McDonald, "Ireland Is Cool for Google as Its Data Servers Like the Weather" *The Guardian* (23 December 2012); John Kennedy, "Ireland Is the Data Capital of Europe, Says Google" *Silicon Republic* (4 February 2016) <https://www.siliconrepublic.com/enterprise/google-ireland-data-capital-europe-crown> (accessed 8 December 2017).

99 See para 21 above.

100 *Garrison v Louisiana* 379 US 64 at 77–78 (1964); *Ashton v Kentucky* 384 US 195 at 198 (1966).

101 Rich Miller, "Northern Virginia: America's Largest Data Center Market" *Data Center Frontier* (16 March 2017) <https://datacenterfrontier.com/northern-va-ready-for-a-data-center-building-boom/> (accessed 8 December 2017).

102 Ingrid Burrington, "Why Amazon's Data Centers Are Hidden in Spy Country" *The Atlantic* (8 January 2016); Ingrid Burrington, "Up to 70 Percent of Global Internet Traffic Goes through Northern Virginia" *Nextgov* (8 January 2016) <http://www.nextgov.com/big-data/2016/01/70-percent-global-internet-traffic-goes-through-northern-virginia/124976/> (accessed 8 December 2017).

(2) Objective territorial principle

35 The application of the objective territorial principle in cyberspace is known as the "country of destination" approach.[103] Where a website has been accessed within a State, that particular State would have jurisdiction over any offence that has occurred through this access.[104] This is because the element of publication is a constituent element of the offences of defamation and hate speech.[105] Thus, where an online post that amounts to hate speech or criminal defamation is accessed in countries A, B and C, the objective territorial principle would apply to grant each of those states jurisdiction, providing a starkly different result from the subjective territorial approach which only provides for a single instance of publication from the jurisdiction hosting the data servers. This principle has been applied in a large number of states.

(a) Application of objective territoriality – UK

36 In the UK, the objective territorial principle has been applied to various cybercrimes. This is demonstrated in the field of obscene publications, for instance.[106] Section 2(1) of the Obscene Publications Act 1959[107] ("OPA"), which provides for criminal liability in the form of a fine and imprisonment sentences, extends to those that publish obscene material or, in the case of electronic material, transmit data containing or embodying that material.[108]

37 In *R v Waddon*,[109] the defendant was charged under s 2(1) of the OPA for the offence of publishing obscene computer images. An undercover police officer had signed up for the paid service of a website entitled "xtreme-perversion" and accessed certain graphic images of pornographic material. It was later found that the defendant was the director of the group that ran the website and was the one responsible for uploading the pornographic data. The defendant argued that the court lacked jurisdiction to try him for the alleged offence as the

103 Uta Kohl, *Jurisdiction and the Internet: Regulatory Competence over Online Activity* (Cambridge University Press, 2007) at p 115.

104 Diane Rowland, Uta Kohl & Andrew Charlesworth, *Information Technology Law* (Routledge, 4th Ed, 2012) at p 30.

105 It is uncontroversial that publication is a requisite element for these offences to be made out. See generally s 6 of the New South Wales Defamation Act 2005 (Act 77 of 2005); s 8 of the UK Defamation Act 2013 (c 26); and *Delfi AS v Estonia* [2015] ECtHR 64569/09 at [110].

106 Matthew Richardson, *Cyber Crime: Law & Practice* (Wildly, Simmonds & Hill Publishing, 2014) at p 144.

107 c 66 (UK).

108 Obscene Publications Act (c 66) (UK) ss 1(3)(b) and 2(1).

109 [2000] WL491456 (No 99/5233/Z3 CA).

publication of the aforementioned pornographic images took place outside the UK. This argument was premised on the fact that the website's content, including the pornographic images, was stored in a data server in the US and was only transmitted to viewers in the UK when they logged into the website. This was effectively an argument grounded on the application of the subjective territorial principle. The Court of Appeal of England and Wales nevertheless held that publication had taken place within their jurisdiction:[110]

> As it seems to us, there can be a publication on a website abroad, when images are there uploaded; and there can be further publication when those images are downloaded elsewhere. That approach is, as it seems to us, underlined by the provisions of section 1(3)(b) as to what is capable of giving rise to publication where matter has been electronically transmitted.

38 In doing so, the court characterised the argument that there could be only a single instance of publication for Internet material as "a fallacy".[111] A similar result was reached in the later case of *R v Perrin*,[112] which was also decided by the Court of Appeal. This was another situation involving an offending website that contravened s 2(1) of the OPA through its purported publication of obscene images within the UK. The defendant was the owner of the website "www.sewersex.com", which displayed images related to coprophilia, coprophagia and oral sex between males; such images were accessed by a police officer from the Obscene Publications Unit.

39 The defendant put forth three arguments, one of which was that the publication of an allegedly obscene website should only be said to have occurred in a jurisdiction where there had been "major steps towards publication".[113] Reliance was placed on the worldwide accessibility of the Internet and its international, geographically borderless nature. It was further submitted that requiring publishers to comply with the numerous statutory requirements of individual states would result in them catering to only the most restrictive laws on Internet content, thus negatively impacting the right to freedom of expression.[114] The court, having applied its mind to the argument, dismissed it by affirming the position earlier stated in *R v Waddon*; as long as a website was accessed within a State, there would be publication for the purposes of s 2(1) of the OPA and hence jurisdiction for the court.[115]

110 *R v Waddon* [2000] WL491456 (No 99/5233/Z3 CA) at [12].
111 *R v Waddon* [2000] WL491456 (No 99/5233/Z3 CA) at [12].
112 [2002] EWCA Crim 747.
113 *R v Perrin* [2002] EWCA Crim 747 at [41].
114 *R v Perrin* [2002] EWCA Crim 747 at [34].
115 *R v Perrin* [2002] EWCA Crim 747 at [51].

(b) Application of objective territoriality – France

40 The objective territorial principle was accepted and applied by the High Court of Paris in *LICRA v Yahoo!*.[116] The case was brought by a French organisation called International League against Racism and Anti-Semitism ("LICRA") against Yahoo! for the latter's hosting of auctions for Nazi memorabilia on the US Yahoo! website. Such memorabilia were easily accessible by French users. LICRA claimed that the sale and promotion of pro-Nazi works and materials offended Art R645-1 of the French Penal Code 1992, which criminalises the exhibit or display of Nazi emblems.[117] Despite the fact that the US Yahoo! auction site was written in English, directed at US users and reliant on servers located in California, the court held that Yahoo!, in "permitting these objects to be viewed in France and allowing surfer[s] located in France to participate in such a display of items for sale … [was] therefore committing a wrong in the territory of France".[118] This essentially amounted to a recognition that the mere access to the US Yahoo! auction website from within France was sufficient to constitute the promotion of such auctions in France. This conclusion was reached despite Yahoo!'s protests that they lacked the technological capabilities to prevent French web surfers from accessing the site.[119]

(c) Application of objective territoriality – Germany

41 The application of the objective territorial principle in Germany is demonstrated through the 2001 *In Re Töben*[120] case heard by the Federal Court of Justice. The defendant, Frederick Töben, was an Australian national who had posted comments denying the Holocaust on a website hosted by Australian data servers. He was arrested during a vacation in Germany and charged under s 130 of the German Criminal Code 1998 for the offence of disrupting the public peace through Holocaust denial.[121] Despite the fact that Töben's comments were made in English, the court nevertheless found jurisdiction. In doing so, it relied on the facts that the statements were directed to the German public and that the website was accessible within Germany. It further reasoned that these facts, together with the high likelihood that such online publications would disrupt public peace, were sufficient to justify

116 (2000) Pl's Compl 17, Yahoo! II (No 00-21275).
117 French Code Pénal (1992) Art R645-1.
118 *LICRA v Yahoo!* (2000) Pl's Compl 17, Yahoo! II (No 00-21275) at 5.
119 Marc Greenberg, "A Return to Lilliput: The *LICRA v Yahoo!* Case and the Regulation of Online Content in the World Market" (2003) 18(4) Berkeley Tech LJ 1191 at 1207.
120 (2000) Urt v 12.12.2000 – 1 StR 184/00, reported in 54(8) NJW (2001) at 624–638.
121 Michail Vagias, *The Territorial Jurisdiction of the International Criminal Court* (Cambridge University Press, 2014) at p 146.

its assertion of jurisdiction over the defendant. Interestingly, this court arrived at this conclusion despite there being no evidence of actual instances of German users accessing the website. This was clear support of the operation of the objective territorial principle, in that because the inflammatory comments could be and were likely to have been accessed in Germany, a constituent element of the offence under s 130 was present.

(d) Application of objective territoriality – Australia

42 *Dow Jones & Co Inc v Gutnick*[122] ("*Dow Jones v Gutnick*") was heard by the High Court of Australia. While the court did not expressly refer to the principle of objective territoriality in its written decision, it was evident that it was applied. This decision, being the first by any nation's apex court on issues of jurisdiction concerning international Internet-based defamation, generated much interest worldwide and has been scrutinised heavily. Dow Jones & Co Inc ("Dow Jones") operated WSJ.com, an online subscription news site that was hosted on data servers in New Jersey, US, and accessible worldwide. It posted an article on its website entitled "Unholy Gains", which Gutnick contended defamed him. Gutnick lived and had established his business headquarters in Australia, although he regularly conducted business outside Australia and contributed to charities in the US and Israel. The court had multiple questions to consider, among which was whether the element of publication within Australia was satisfied. Dow Jones contended for the country of origin approach to apply, that an article should be deemed published when it is uploaded to a data server.[123] The court rejected this contention, instead holding that publication occurred in Australia when the allegedly defamatory article was downloaded by Dow Jones subscribers. In doing so, it implicitly affirmed the application of the objective territorial principle. Crucial to the court's decision were three reasons.

(i) AVOIDING RESTRICTIVE DEFAMATION LAWS OF FOREIGN JURISDICTIONS

43 First, the court stated that an application of the country of origin approach would result in Australian defendants being subjected to the more restrictive defamation laws of foreign jurisdictions, such as the US. Additionally, the court opined that publishers would attempt to

122 [2002] HCA 56.

123 *Dow Jones & Co Inc v Gutnick* [2002] HCA 56 at [18]; Michael Saadat, "Jurisdiction and the Internet after Gutnick and Yahoo!" (2005) 1 JILT at 5.

adopt "locational stratagems" to avoid liability if there were only a single State that had jurisdiction over them.[124]

44 The court reached this conclusion despite Dow Jones' qualification of its argument, that where a publisher has acted "opportunistic[ally]" in deliberately locating its data servers in a restrictive jurisdiction, the country of origin approach would be waived.[125] The court reasoned that such an approach would invite legal uncertainty in determining whether a publisher's actions were "adventitious" or "opportunistic",[126] and in ascertaining a publisher's intentions in utilising a particular data server of a State. This was so, especially considering the difficulty of separating "prudent business decisions" from attempts to avoid defamation liability.[127]

(II) PREVENTING FRAGMENTATION OF LAW ON DEFAMATION

45 Secondly, the court expressed an unwillingness to fragment the law of defamation. Dow Jones mounted a number of arguments in an attempt to convince the court to depart from its traditional notion of publication (that publication occurs when certain material is read). Its key policy argument was that the application of the latter would result in onerous obligations on Internet publishers; Internet publishers would "be bound to take account of the law of every country on earth, for there were no boundaries which a publisher could effectively draw to prevent anyone, anywhere, downloading the information it put on its web server".[128] This was essentially an argument based on the scope and scale of Internet communication – that a different approach to jurisdiction should be taken due to the exceptional nature of the Internet compared to traditional forms of communication.

46 The court rejected this argument on the basis that Internet publishers were aware of the consequences of publishing content in cyberspace. The majority opinion relied on the underlying rationale of the law of defamation in balancing society's interest in freedom of expression against an individual's interest in maintaining his or her reputation to do so.[129] They held that the Internet's "uniquely broad reach" was not a sufficiently compelling reason to justify a departure

124 *Dow Jones & Co Inc v Gutnick* [2002] HCA 56 at [117].
125 *Dow Jones & Co Inc v Gutnick* [2002] HCA 56 at [20].
126 *Dow Jones & Co Inc v Gutnick* [2002] HCA 56 at [21].
127 *Dow Jones & Co Inc v Gutnick* [2002] HCA 56 at [21].
128 *Dow Jones & Co Inc v Gutnick* [2002] HCA 56 at [20].
129 *Dow Jones & Co Inc v Gutnick* [2002] HCA 56 at [23].

from the traditional framework of defamation.[130] They went on to state:[131]

> 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*. [emphasis added]

47 The fact that Dow Jones actively solicited subscribers for its website, while publishing articles that could be accessed and viewed worldwide, was thus sufficient to ascribe responsibility to them.[132] Moreover, the court emphasised that the problem of widely disseminated communications was not unique to the Internet; reference was made to other technological innovations like newspapers, magazines, radios and the television. Implicit in this was the court's reluctance to carve out liberal legal exceptions to new forms of technology in order to preserve consistency in the law.[133] The need to prevent fragmentation of the law has been echoed on other occasions, with an emphasis on the idea that the difference in scope that the Internet provides does not render it "exceptional" and thus exempt from a traditional framework.[134]

(III) LACK OF ENFORCEABILITY OF JUDGMENTS

48 Thirdly, the court declared that the practical hurdle of enforcing judgments would serve to dissuade plaintiffs from bringing defamation actions in jurisdictions. Defamation actions would only be brought in jurisdictions where a publisher had assets;[135] this would allow for publishers to anticipate the jurisdictions from which suits against them may arise and allow for greater certainty in their publications.

130 *Dow Jones & Co Inc v Gutnick* [2002] HCA 56 at [38]–[39].
131 *Dow Jones & Co Inc v Gutnick* [2002] HCA 56 at [43].
132 Michael Saadat, "Jurisdiction and the Internet after Gutnick and Yahoo!" (2005) 1 JILT at 7.
133 Michael Saadat, "Jurisdiction and the Internet after Gutnick and Yahoo!" (2005) 1 JILT at 6.
134 Jack Goldsmith, "Against Cyberanarchy" (1998) 65 U Chi L Rev 1239 at 1239; Michael Saadat, "Jurisdiction and the Internet after Gutnick and Yahoo!" (2005) 1 JILT at 2.
135 *Dow Jones & Co Inc v Gutnick* [2002] HCA 56 at [53].

IV. Subjective or objective territorial principle – Never the twain shall meet?

49 Having surveyed the case law on the application of both the subjective territorial and objective territorial principles in cases involving the Internet, it appears that regulatory control over Internet publishers would be either too relaxed (the subjective territorial approach) or too harsh (the objective territorial approach). The natural question that springs to mind is the following: Which principle should take precedence?

50 As earlier demonstrated,[136] adopting the country of origin approach would favour publishers of controversial material, be it obscene content, defamatory material or hate speech. This is because such publishers would be subject to the regulations of only one State (the State in which the data servers hosting their content are located). It is thus no surprise that publishers of online content such as "Yahoo!" would push for such an approach to apply. In contrast, the application of the objective territorial principle results in publishers being potentially liable in any and every State that their material may be accessed from.

51 The courts of various jurisdictions have generally affirmed the application of the objective territorial principle.[137] The UK courts in particular, through *Richardson v Schwarzenegger*[138] and *King v Lewis*,[139] have often affirmed that there is no warrant for drawing a distinction in the law for the medium of the Internet.[140] It is nevertheless important to note that these affirmations were not accompanied by any pronouncement on the inapplicability of the subjective territorial principle.

52 Faced with these decisions, one may argue that the choice of various courts in different jurisdictions to affirm the application of the objective territorial principle is sufficient to resolve the question of whether the subjective or objective territorial principle should take precedence. However, such an argument would be flawed because the application of the objective territorial principle presents a number of problems.

136 See para 33 above.
137 See paras 36–48 above.
138 (2004) EWHC 2422 (QB).
139 (2004) EWCA Civ 1329.
140 Eric Barendt, "Jurisdiction in Internet Libel Cases" (2006) 110 Penn St L Rev 727 at 732; Graham Smith, *Internet Law and Regulation* (Sweet & Maxwell, 2007) at p 476.

A. Flaws of applying objective territorial principle

53 The key drawback of using the objective territorial principle in cyberspace is that it would result in onerous burdens on publishers of online content. As earlier mentioned,[141] they are taken to be aware of the domestic legislation of any State from which their content can be accessed, by virtue of their knowledge of the Internet as a borderless medium. This would presumably apply regardless of the publisher's status; a multinational company like Yahoo! would be treated the same way as an individual running a personal blog. It would be especially onerous to require the latter to require a working knowledge of the state regulations worldwide whenever he or she posts controversial content online that may be legal in his or her home State, but illegal abroad. This would inevitably create a chilling effect on free speech worldwide and greatly stem the significance of the Internet as a tool to promote cross-border discourse and learning.[142] The oppressive nature of such a burden is well articulated by Graham Smith:[143]

> It is by no means obvious that every defendant should be automatically responsible for every publication that takes place when someone goes to its website and downloads an article. That approach may be superficially attractive when the defendant is an international American media company. *But what of the church newsletter, the garden club magazine, the schoolgirl blogger*? Are they to be characterised as a "global publisher" and exposed to worldwide liability because they are taken to know the reach of the medium on which they have chosen to publish? The current doctrine [of objective territoriality] can be seen to do less than justice when viewed in that context … [emphasis added]

54 As was noted by Kirby J in his minority opinion in *Dow Jones v Gutnick*, the application of traditional rules of jurisdiction to the novel medium of the Internet hence exposes "real defects" in the law due to the "ubiquity, universality and utility" of the Internet.[144] While the majority viewed the Internet as similar to previous technological innovations such as the radio and the newspaper, Kirby J saw the Internet as differing not only in terms of scale, but also in introducing a "new means of creating continuous technology in a manner that could not previously have been contemplated".[145] Legal commentators have

141 See para 45 above.

142 *Dow Jones & Co Inc v Gutnick* [2002] HCA 56 at [152]; Marc Greenberg, "A Return to Lilliput: *The LICRA v. Yahoo!* Case and the Regulation of Online Content in the World Market" (2003) 18(4) Berkeley Tech LJ 1191 at 1231; Graham Smith, *Internet Law and Regulation* (Sweet & Maxwell, 2007) at pp 476–477.

143 Graham Smith, *Internet Law and Regulation* (Sweet & Maxwell, 2007) at pp 476–477.

144 *Dow Jones & Co Inc v Gutnick* [2002] HCA 56 at [78] and [137].

145 *Dow Jones & Co Inc v Gutnick* [2002] HCA 56 at [118].

also expressed similar views;[146] Menthe, for instance, states that "unless it is conceived of as an international space, cyberspace takes all the traditional principles of conflicts-of-law and reduces them to absurdity".[147]

55 It is submitted that Kirby J's view of the Internet should be preferred over that of the majority in *Dow Jones v Gutnick*. The objective territorial principle possesses an inherent limiter – that there had to be a constituent element of the crime that occurred within a State's territory. Thus, while there may have been situations in the past where states possessed concurrent jurisdiction, such as in the infamous example of a man firing a gun across a border to kill someone located in another State,[148] such jurisdiction would be limited to only a few states given the physical nature of the act. Similarly, the printing of newspapers and the broadcast of radio programs are geographically limited as well – a newspaper publisher, if he wishes for his circulation to reach an overseas audience, has to deliberately arrange for the international shipping of his product to a specific country and its subsequent distribution. In contrast, online publications are, by default, available to the world at large. This is summed up succinctly by Diane Rowland, Uta Kohl and Andrew Charlesworth:[149]

> The problem of extending *Lotus*[150] to non-physical effects is that innumerable states may be affected by the same foreign event, thus giving rise to innumerable concurrent regulatory rights by destination states, and this is precisely the competence dilemma caused by the internet.

56 The loss of the objective territorial principle's limiter in the form of intra-territoriality brings it dangerously close to the effects doctrine, which has been widely criticised as a controversial base of jurisdiction.[151]

---

146 Darrel Menthe, "Jurisdiction in Cyberspace: A Theory of International Spaces" (1998) 4 Mich Telecomm & Tech L Rev 69 at [71]; Morris Lipson, Article 19, "Regulating Hate Speech Content for the Internet: The Legal Jurisdiction Puzzle", presentation at the Conference on Guaranteeing Media Freedom on the Internet (27 August 2004), available at http://www.osce.org/fom/36097 (accessed 8 December 2017).

147 Darrel Menthe, "Jurisdiction in Cyberspace: A Theory of International Spaces" (1998) 4 Mich Telecomm & Tech L Rev 69 at 70–71.

148 *Restatement Second, Foreign Relations Law of the United States* (1965) § 18, Illustration 2.

149 Diane Rowland, Uta Kohl & Andrew Charlesworth, *Information Technology Law* (Routledge, 4th Ed, 2012) at p 29.

150 The reference to the *Lotus* principle by Rowland, Kohl and Charlesworth in this context refers to the application of the objective territorial principle to the medium of the Internet, rather than the legal proposition that states may exercise their jurisdiction however they please unless there are specific prohibitive rules that operate to restrict that exercise. The latter principle is addressed at para 4 above.

151 Alan Vaughan Lowe, "Blocking Extraterritorial Jurisdiction: The British Protection of Trading Interests Act, 1980" (1981) 75 AJIL 257 at 262; Gary Born, *International*

(*cont'd on the next page*)

The effects doctrine, which had its genesis in the anti-trust regulations of the US, essentially allowed for its courts to exercise extravagant jurisdiction; jurisdiction was exercised over foreign cartel arrangements and collusions on the basis that these foreign acts had produced some substantial effects in the US.[152] Thus, a situation where every State in the world may claim jurisdiction over a particular website simply because that website could be accessed and read within its territory, thus producing certain effects within the State, gives each State far-reaching extraterritorial powers akin to an application of the effects doctrine.

57 Some would no doubt argue that the solution to this conundrum would be the implementation of tools to exclude access to certain websites from certain jurisdictions, also known as geoblocking tools. However, this approach results in a number of problems. First, this would encourage the strict segmentation of the Internet, a body which was meant to be an open and borderless space for the sharing and discussion of ideas and opinions.[153] Secondly, not all publishers may have access to geoblocking measures on their utilised platforms. For instance, the 359 million bloggers using the microblogging website "Tumblr" have the option to block specific users from viewing their website but are unable to deny general access to users based on the latters' location.[154] Thirdly, even where geoblocking tools are utilised, they can be easily circumvented through the use of various tools to disguise a user's access location. Examples of such tools include proxy servers, virtual private networks and anonymity browsers; the latter are especially powerful devices that also grant their users the ability to access the dark web – a set of non-publicly available websites that facilitate the trade of contraband material such as drugs and child pornography.[155]

Civil Litigation in US Courts: Commentary and Materials (Kluwer Law International, 1996) at p 506; *The Resurgence of the State: Trends and Processes in Cyberspace Governance* (Myriam Dunn Cavelty, Sai Felicia Krishna-Hensel & Victor Mauer eds) (Ashgate Publishing, 2007) at p 64.

152 *United States v General Electric Co* 82 F Supp 753 at 891 (1949); *Mannington Mills v Congoleum Corp* 595 F 2d 1287 at 1292 (1979); *The Resurgence of the State: Trends and Processes in Cyberspace Governance* (Myriam Dunn Cavelty, Sai Felicia Krishna-Hensel & Victor Mauer eds) (Ashgate Publishing, 2007) at p 64.

153 Ignio Gagliardone, *et al*, *Countering Online Hate Speech* (UNESCO Publishing, 2015) at p 15.

154 Tumblr Help Centre, "Blocking Users" https://tumblr.zendesk.com/hc/en-us/articles/231877648-Blocking-users (accessed 8 December 2017).

155 Nihad Ahmad Hassan & Rami Hijazi, *Data Hiding Techniques in Windows OS: A Practical Approach to Investigation and Defense* (Syngress, 2016) at p 170; Axel Bugge, "Dark Web Drug Market Growing Rapidly in Europe: Report" *Reuters* (29 November 2017).

58 The difficulty of using geoblocking tools to prevent access to a particular site by users was also a point acknowledged by Kirby J in *Dow Jones v Gutnick* – that the nature of Internet Protocol addresses that can be frequently changed results in there being "no effective way … to determine, in every case, the geographic origin of the Internet user seeking access to the website".[156] This difficulty of preventing access to all users from a particular region has also taken centre stage in criticisms of the aforementioned decisions of *Licra v Yahoo!* and *In Re Töben*.[157]

59 Another argument that may be mounted in favour of the objective territoriality approach applying would be the lack of enforcement jurisdiction against defendants from a different State. As stated by the court in *Dow Jones v Gutnick*, judicial proceedings may not be instituted against an individual if the eventual judgment that is rendered is of little practical value.[158] The court reasoned that where a defendant lacked assets in a particular jurisdiction, such an action was unlikely to be brought.

60 However, it must be noted that these comments were made in the context of a civil proceeding rather than a criminal one. In criminal cases concerning hate speech or criminal defamation, the full force of state machinery may be brought to pursue proceedings against an individual once he or she enters the State's territory. Frederick Töben found himself in such a situation when he was vacationing in Germany, leading to his prosecution by German authorities. Hence, there remains the real possibility of individuals being subject to a State's criminal proceedings should they decide to travel to that State in the future. As a result, the application of the objective territorial principle in its traditional form to the medium of the Internet remains a real problem.

B. Formulation of new jurisdictional rules for Internet publications

(1) Using subjective territorial approach with publisher self-regulation

61 One way to address the flaws of the objective territorial principle would be to adopt the subjective territorial approach towards jurisdiction over online publishers while trusting the platforms on

156 *Dow Jones & Co Inc v Gutnick* [2002] HCA 56 at [84].

157 Marc Greenberg, "A Return to Lilliput: The *LICRA v. Yahoo!* Case and the Regulation of Online Content in the World Market" (2003) 18(4) Berkeley Tech LJ 1191 at 1221; Michail Vagias, *The Territorial Jurisdiction of the International Criminal Court* (Cambridge University Press, 2014) at p 148.

158 *Dow Jones & Co Inc v Gutnick* [2002] HCA 56 at [121].

which such publications are made to engage in self-regulation for controversial content such as hate speech and criminal defamation. Internet intermediaries, who republish user content on a daily basis, have long emphasised the self-sufficiency of such an approach; social media company Facebook, for instance, which allows users to create online profiles to interact and share content with each other over the Internet,[159] has advocated for the primacy of self-regulation and minimal governmental intervention.[160] The preference for such an approach is echoed by various human rights organisations. For instance, Article 19, a non-governmental organisation that has regularly been invited to conduct presentations and speeches at the Organisation for Security and Co-operation in Europe ("OSCE"),[161] believes that excessive regulations over online content would curb the right to freedom of expression.[162]

62 Such an approach is, however, untenable for three major reasons. First, it is difficult to ensure that online platforms practice strict self-regulation. This problem is especially acute for Internet intermediaries that have to deal with large amounts of user content on their platform. While platforms such as Facebook, Twitter and YouTube possess community standards and guidelines with which to regulate user content, not all of them do so satisfactorily. The recent results of a European Commission evaluation showed that only 40% of reported incidents of hate speech were taken down by online media platforms within 24 hours, which constituted a failure to meet the standards of

159 BBC Webwise, "What is Facebook?" (10 October 2012) http://www.bbc.co.uk/webwise/guides/about-facebook (accessed 8 December 2017).

160 John Fraedrich Ferrell, *Business Ethics: Ethical Decision Making & Cases* (Cengage Learning, 2012) at p 294; Jon Brodkin, "Google and Facebook Lobbyists Try to Stop New Online Privacy Protections" *Ars Technica* (25 May 2017) <https://arstechnica.com/tech-policy/2017/05/google-and-facebook-lobbyists-try-to-stop-new-online-privacy-protections/> (accessed 8 December 2017).

161 Article 19 website, "About Us" https://www.article19.org/about-us/ (accessed 8 December 2017); Morris Lipson, Article 19, "Regulating Hate Speech Content for the Internet: The Legal Jurisdiction Puzzle", presentation at the Conference on Guaranteeing Media Freedom on the Internet (27 August 2004) <https://www.osce.org/fom/36097> (accessed 8 December 2017); Dr Agnes Callamard, Executive Director, Article 19, "Freedom of Expression and Press Freedom: Protecting and Respecting Human Security", keynote speech at the Supplementary Human Dimension Meeting on Freedom of the Media (13 July 2006) <https://www.osce.org/odihr/19935> (accessed 8 December 2017).

162 Morris Lipson, Article 19, "Regulating Hate Speech Content for the Internet: The Legal Jurisdiction Puzzle", presentation at the Conference on Guaranteeing Media Freedom on the Internet (27 August 2004) <http://www.osce.org/fom/36097> (accessed 8 December 2017).

compliance required by the European Union Code of Conduct on Countering Hate Speech.[163]

63 Secondly, online platforms are ill-equipped to determine complex issues of hate speech and criminal defamation themselves. The determination of whether a piece of user content amounts to hate speech or criminal defamation, or is merely provocative, engages the delicate balancing exercise between the right to freedom of expression and the rights and reputations of individuals and communities. Thus, as stated by the United Nations Special Rapporteur on Freedom of Opinion and Expression and the OSCE Representative on Freedom of the Media, such determinations should be left to judicial bodies with the requisite expertise, rather than online platforms.[164]

64 Thirdly, such an approach would leave many states powerless to act. As earlier mentioned, the subjective territorial principle only allows for a State to exercise jurisdiction over a piece of content if it hosts the data server from which that piece of online content was uploaded. The application of such a rule would be inherently unacceptable to many states given their inability to take actions against unlawful content that is targeted at their State from abroad.

(2) The Zippo *sliding-scale test*

65 An alternative to the use of the subjective territorial principle in conjunction with publisher self-regulation would be the *Zippo* sliding-scale test in the US. In 1997, the US decision of *Zippo Manufacturing Co v Zippo Dot Com, Inc*[165] ("*Zippo*") set out a wholly new jurisdictional test for Internet jurisdiction over websites located extraterritorially.[166] The *Zippo* sliding-scale test based the exercise of jurisdiction over the degree of interactivity between a website and the forum; where a "passive Web site … does little more than make information available to those who are interested in it",[167] a court would be unable to exercise jurisdiction over it. In contrast, a court would readily find jurisdiction

163 Amar Toor, "Facebook, Twitter, and Google Are Still Failing to Curb Hate Speech, EU Says" *The Verge* (5 December 2016) <https://www.theverge.com/2016/12/5/13841162/facebook-twitter-google-microsoft-hate-speech-eu-report> (accessed 8 December 2017); European Commission, "Countering Online Hate Speech – Commission Initiative with Social Media Platforms and Civil Society Shows Progress" (1 June 2017) <http://europa.eu/rapid/press-release_IP-17-1471_en.htm> (accessed 8 December 2017).

164 Organisation for Security and Co-operation in Europe, "Joint Declaration on Freedom of Expression and the Internet" (1 June 2011) <http://www.osce.org/fom/78309> (accessed 8 December 2017).

165 952 F Supp 1119 (1997).

166 *Zippo Manufacturing Co v Zippo Dot Com, Inc* 952 F Supp 1119 at 1124 (1997).

167 *Zippo Manufacturing Co v Zippo Dot Com, Inc* 952 F Supp 1119 at 1124 (1997).

over a website that was highly interactive.[168] Since then, the *Zippo* sliding-scale test has been adopted in countless cases, with many academics and commentators recognising the *Zippo* decision as a seminal case on Internet jurisdiction; the test itself has even been described as "the most influential test pertaining to Internet jurisdiction".[169]

66 An example of the application of the *Zippo* test would be in *Alitalia-Linee Aeree Italiane SpA v Casinoalitalia.com*.[170] In that case, it was held that a Virginian court could exercise jurisdiction over an interactive casino gambling website that repeatedly conducted business transactions over the Internet with Virginia residents. This was because gambling was "an inherently interactive activity" which required players to purchase credits to play.[171] Conversely, in *Dawson v Pepin*,[172] it was found that the website of a Canadian resident that contained nothing but information on a particular product was a passive one; the court hence decided that it would be inappropriate to exercise jurisdiction.[173]

67 However, there are two major problems with the application of this test of Internet jurisdiction. First, the *Zippo* test is tied to the characteristics of a particular website rather than its connection with a particular State. Thus, even the mere existence of an interactive site is enough to subject an out-of-State defendant to a court's jurisdiction.[174] This is particularly problematic when one considers that the vast majority of websites in the 21st century are interactive in nature. Thus, in *Kindig-It Design, Inc v Creative Controls Inc*,[175] the court stated:[176]

> The weakness of the Zippo approach becomes ever more apparent in today's digital age. The ability to create and maintain an interactive website is no longer the sole domain of technologically sophisticated corporations. Virtually all websites, even those created with only minimal expense, are now interactive in nature. It is an extraordinarily

168 *Zippo Manufacturing Co v Zippo Dot Com, Inc* 952 F Supp 1119 at 1124 (1997).

169 Dennis T Yokohama, "You Can't Always Use the *Zippo* Code: The Fallacy of a Uniform Theory of Internet Personal Jurisdiction" (2005) 54 DePaul L Rev 1147 at 1149. See also Eric C Hawkins, "General Jurisdiction and Internet Contacts: What Role, if Any, Should the *Zippo* Sliding Scale Test Play in the Analysis?" (2006) 74 Fordham L Rev 2371 at 2371 and Dan Jerker B Svantesson, *Private International Law and the Internet* (Kluwer Law International, 2007) at p 139.

170 128 F Supp 2d 340 (2001).

171 *Alitalia-Linee Aeree Italiane SpA v Casinoalitalia.com* 128 F Supp 2d 340 at 350 (2001).

172 WL 822346 (2001) (unreported).

173 *Dawson v Pepin* (2001) WL 822346 (unreported); Graham J H Smith, *Internet Law and Regulation* (Sweet & Maxwell, 2007) at p 670.

174 *3DO Co v Poptop Software Inc* 49 USOQ2D 1469 at 1472 (ND Cal, 1998).

175 WL 247574 (2016) (unreported).

176 *Kindig-It Design, Inc v Creative Controls Inc* WL 247574 (2016) (unreported) at 9.

> rare website that does not allow users to do at least some of the following: place orders, share content, 'like' content, 'retweet', submit feedback, contact representatives, send messages, 'follow', receive notifications, subscribe to content, or post comments.

68 The *Zippo* test was formulated in 1997, during the Web 1.0 era, when most websites were static and non-interactive; users were often confined to the "passive viewing of information that was provided to them".[177] At the time, the decision of a website operator to make concerted efforts in interacting with users from a particular State, for instance, through the conducting of business transactions, must have been viewed as a form of purposeful availment that justified the exercise of extraterritorial jurisdiction.[178]

69 This problem is exacerbated when one considers that there is little guidance provided by the court as to the precise degree of interactivity required before jurisdiction would be founded. This resulted in judges making findings on jurisdiction based on intuition rather than established legal principles;[179] in *Cable News Network v GoSMS.com*,[180] for instance, a judge in the Southern District of New York found jurisdiction over a passive website despite findings of fact that a website's services were not used in the State.[181] He did so because it was "intuitively apparent" that website's services would have been used.[182]

70 Secondly, the *Zippo* test is wholly inappropriate for the offences of criminal defamation or hate speech.[183] While the *Zippo* test may be appropriate for offences such as Internet fraud (which require continued

---

177 Elza Dunkels, *Youth Culture and Net Culture: Online Social Practices* (IGI Global, 2010) at p 43; Management Association, Information Resources, *Digital Literacy: Concepts, Methodologies, Tools, and Applications* (IGI Global, 2012) at p 737; David Boud & Elizabeth Molloy, *Feedback in Higher and Professional Education: Understanding It and Doing It Well* (Routledge, 2013) at p 127.

178 Frank Arenas, "Cyberspace Jurisdiction and the Implications of Sealand" (2002–2003) 88 Iowa L Rev 1165 at 1186; Eric C Hawkins, "General Jurisdiction and Internet Contacts: What Role, if Any, Should the *Zippo* Sliding Scale Test Play in the Analysis?" (2006) 74 Fordham L Rev 2371 at 2376; Pavan Mehrota, "Back to the Basics: Why Traditional Principles of Personal Jurisdiction Are Effective Today and Why Zippo Needs to Go" (2010) 12 NCJL & Tech 229 at 233.

179 *Cable News Network v GoSMS.com* WL 1678039 (2000) (unreported) at 3; Mark Sableman & Michael Nepple, "Will the *Zippo* Sliding Scale for Internet Jurisdiction Slide into Oblivion?" (2016) 20 *Journal of Internet Law* 3 at 3.

180 WL 1678039 (2000) (unreported).

181 *Cable News Network v GoSMS.com* WL 1678039 (2000) (unreported) at 3.

182 *Cable News Network v GoSMS.com* WL 1678039 (2000) (unreported) at 3.

183 Julia Alpert Gladstone, "Determining Jurisdiction in Cyberspace: The '*Zippo*' Test or the 'Effects' Test?" (2003) 3 *Informing Science & IT Education Conference* 143 at 150.

interactions between the victim and the offender), publications relating to criminal defamation or hate speech can take place on websites or blogs that offer no opportunity for interaction. Allowing for a court to claim jurisdiction only when a hate speech website allows for comments to be posted in response would be absurd.

(3) Refining objective territorial principle

71 A third approach, which this paper submits is the most viable option, is to refine the use of the objective territorial principle, such that it would be used alongside the subjective territorial principle. The subjective territorial principle would still play a role in granting a State jurisdiction where the data servers hosting the website are located within its territory, but other states would also have jurisdiction if the requirements of the objective territorial principle are met. Hence, the subjective and objective territorial principles would both apply to publishers – as long as the objective territorial principle is refined such as to mitigate the harshness towards publishers. The adoption of such a flexible approach towards the objective territorial principle would reflect the continuing development of jurisdictional principles in international law. Indeed, as several ICJ judges themselves noted, the contours of international law jurisdiction are "in constant evolution".[184]

V. Refinements to application of territorial principle in cyberspace

A. Element of targeting

72 There should be an additional requirement of "targeting" when considering the application of the objective territorial principle for issues of publication over the Internet. This would re-establish the "limiting function" of the objective territorial principle, which has been rendered obsolete by the unique borderless nature of the Internet.[185] Adopting this requirement would mean that the mere accessibility of a piece of content within a State would not be considered as sufficient for that State to exercise its jurisdiction; it must also be shown that one

184 *Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v Belgium)* (2002) ICJ Rep 3 (Joint Separate Opinion of Higgins, Kooijmans and Buergenthal JJ) at [75]. See also Dan Jerker B Svantesson, *Solving the Internet Jurisdiction Puzzle* (Oxford University Press, 2017) at pp 36–37.

185 *The Resurgence of the State: Trends and Processes in Cyberspace Governance* (Myriam Dunn Cavelty, Sai Felicia Krishna-Hensel & Victor Mauer eds) (Ashgate Publishing, 2007) at p 75.

"specifically aim[ed] its online activities at a [State]" before that State may avail itself of jurisdiction.[186]

73 Such an approach has been described as either the "reasonable effects" doctrine or the "directing and targeting" approach by commentators.[187] Whether the defendant had targeted a particular jurisdiction would depend on the application of a multi-factorial test to the objectively ascertainable factual circumstances.[188] The factors to be taken into consideration when assessing if a State was targeted by the defendant would include:[189]

(a) the content of the publication;

(b) the context of the publication;

(c) the proportion of the overall publication that took place within a state; and

(d) the foreseeable effect of the publication upon the territory.

74 This would hence be an objective assessment of the defendant's subjective intentions. By virtue of the publisher's act of targeting a particular State, that State would have a stronger claim to jurisdiction relative to other states as it would possess a substantial connection to the publication.

75 Such an approach may be viewed as being broadly similar to other international tests for jurisdiction, such as the *Spiliada* framework used under private international law for determining the appropriateness of a particular forum in hearing a transnational dispute.[190] As stated by Lord Goff, the *Spiliada* framework is concerned with whether "some other available forum, having competent jurisdiction … is the appropriate forum for the trial of the action, *ie* in which the case may be tried more suitably for the interests of all the parties and the ends of

186 Brian Boone, "Bullseye!: Why a 'Targeting' Approach to Jurisdiction in the E-Commerce Context Makes Sense Internationally" (2006) 20 Emory Int'l L Rev 241 at 266.

187 Graham J H Smith, *Internet Law and Regulation* (Sweet & Maxwell, 2007) at p 480; Diane Rowland, Uta Kohl & Andrew Charlesworth, *Information Technology Law* (Routledge, 4th Ed, 2012) at p 39.

188 Graham J H Smith, *Internet Law and Regulation* (Sweet & Maxwell, 2007) at p 477.

189 *Calder v Jones* 465 US 783 (1984); *Young v New Haven Advocate* F 3d WL 31780988 (2002); Richard Garnett, "*Dow Jones & Company Inc v Gutnick*: An Adequate Response to Transnational Internet Defamation?" (2003) 4 Melb J Int Law 196 at 210; Graham Smith, "Directing and Targeting – The Answer to the Internet's Jurisdiction Problems" (2004) 5 *Computer Law Review International* 145 at 150.

190 *Spiliada Maritime Corp v Cansulex Ltd* [1987] AC 460 at 476.

justice".[191] Similarly, the ascertainment of whether an individual targeted a particular State must necessarily be done in comparison with other states. Thus, both the targeting approach and the *Spiliada* framework are dependent on the willingness of states to respect and be sensitive to the interests of other states.[192]

76 The targeting approach is not unprecedented. It has been acknowledged by various municipal courts as being a viable test of jurisdiction for publications over the Internet. In *R v Sheppard and Whittle*,[193] the English Court of Appeal stated that apart from the country of origin and the country of destination approaches, the "directing and targeting" theory approach was also possible.[194] This was despite the line of authority established in the earlier cases of *R v Waddon* and *R v Perrin*, namely that the country of destination approach was to be utilised for online publications.[195]

77 The targeting approach was explicitly used in the New York Supreme Court case of *People v World Interactive Gaming Corp*.[196] While this case involved the offering of online gambling services to New Yorkers rather than the publication of defamatory content or hate speech over the Internet, it nevertheless provides guidance for the assessment of whether a defendant targeted a particular jurisdiction. The court examined the defendant's website before finding that the gambling business, which was operated from computer servers based in Antigua, had been targeting the US through online and offline advertising campaigns.[197] A similar analysis was undertaken by the Scottish Court of Sessions in *Bonnier Media v Greg Lloyd Smith*.[198] In that case, the court held that it had jurisdiction over the defendants, as their acts of setting up a website to engage in trademark infringement

191 *Spiliada Maritime Corp v Cansulex Ltd* [1987] AC 460 at 476. See also Jonathan Garson, "Handcuffs or Papers: Universal Jurisdiction for Crimes of *Jus Cogens*, or Is There Another Route?" (2007) 4 J Int'l L & Pol'y 1 at 17.

192 Jessica Almqvist & Carlos Esposito, *The Role of Courts in Transitional Justice: Voices from Latin America and Spain* (Routledge, 2013) at p 220; Tomer Broude, Marc L Busch & Amelia Porges, *The Politics of International Economic Law* (Cambridge University Press, 2011) at p 286; Malcolm D Evans, *International Law* (Oxford University Press, 4th Ed, 2014) at p 337; Cedric Ryngaert, "The Concept of Jurisdiction in International Law" in *Research Handbook on Jurisdiction and Immunities in International Law* (Alexander Orakhelashvili ed) (Edward Elgar, 2015) at p 51.

193 (2010) EWCA Crim 65.

194 *R v Sheppard and Whittle* (2010) EWCA Crim 65 at [33].

195 Matthew Richardson, *Cyber Crime: Law & Practice* (Wildly, Simmonds & Hill Publishing, 2014) at p 149.

196 *People v World Interactive Gaming Corp* (1999) 714 NYS 2d 844.

197 Diane Rowland, Uta Kohl & Andrew Charlesworth, *Information Technology Law* (Routledge, 4th Ed, 2012) at p 40.

198 *Bonnier Media v Greg Lloyd Smith* (2002) ETMR 86.

were "clearly aimed at the [claimant's] business which was centred in Scotland".[199]

B. Flaws of targeting approach

(1) Is departure from traditional jurisdictional principles justified?

78 It must be admitted that the pedigree of the targeting approach pales in comparison to the established traditional principles of subjective territoriality and objective territoriality. However, while it may depart from the traditional conception of the objective territorial principle, namely in that what is required is only a constituent element of an offence to occur within a State's territory, it conforms with the underlying rationale for jurisdiction under international law – the need for a substantial connection between a State and the offence.[200] It is hence submitted that the very nature of the targeting approach, which assesses the strength of the connection between a State and an extraterritorial offence relative to other states, adheres to principles of international law.

(2) Problem of concurrent jurisdiction

79 Even with the requirement of targeting, the problem of concurrent jurisdiction continues to persist. It arises in two situations: first, where a publication targets multiple jurisdictions; and second, where it does not target any jurisdiction. This issue is more likely to arise in the context of hate speech rather than criminal defamation. This is because hate speech, which involves the incitement of hatred against a particular group,[201] is more likely to affect multiple states than the offence of criminal defamation, which typically targets the reputation of specific government officials or public figures in a State.[202]

(a) Multiple targeted jurisdictions

80 In the first scenario, where multiple jurisdictions have been targeted by a publication, each targeted State would be able to claim jurisdiction. The following statement would constitute a clear example

199 *Bonnier Media v Greg Lloyd Smith* (2002) ETMR 86 at [H12].
200 See para 7 above.
201 See para 21 above.
202 Robert Post, "The Social Foundations of Defamation Law: Reputation and the Constitution" (1986) 74 Cal L Rev 691 at 705–706; Elena Yanchukova, "Criminal Defamation and Insult Laws: An Infringement on the Freedom of Expression in European and Post-communist Jurisdictions" (2003) 41 Colum J Transnat'l L 861 at 861; Benedict John Anstey, "Criminal Defamation and Reputation As 'Honour': A Cross-jurisdictional Perspective" (2017) 9 *Journal of Media Law* 132 at 134.

of a publication that targets multiple jurisdictions: "The Jews are absolute trash. We, as glorious citizens of Europe, should end them once and for all."

81 Assuming that this statement was posted in the French language on a European online forum, an application of the targeting approach would point towards certain European states like France and Belgium, which have French as an official language, as possessing jurisdiction. Although such a statement may be accessible in the State of Australia, it would be inappropriate for the State of Australia to claim jurisdiction even though there are Jewish persons within its territory; this is so due to the fact that Australia was not targeted by the statement. Thus, while states such as Australia are excluded from taking jurisdiction, there would nevertheless be concurrent jurisdiction over the offence by other states such as France and Belgium.

82 However, the root of the problem with concurrent jurisdiction is essentially that it introduces uncertainty in international law.[203] Where an individual posts inflammatory material online, is he to be treated as a person that has violated the laws against hate speech in multiple jurisdictions, all of which possess differing standards for defamation or hate speech?

83 While a natural result of the targeting approach is that multiple states may concurrently take jurisdiction over an individual, there is greater certainty afforded by this approach as compared to the traditional objective territorial principle. As stated in *Dow Jones v Gutnick*, "what is important is that publishers can act with confidence, not that they be able to act according to a single legal system".[204] Thus, this approach mitigates the problems associated with concurrent jurisdiction.

(b) Untargeted publications

84 The situation where a publication does not target any specific State is more problematic. For instance, a website may host several statements made in English that repeatedly call for the "eradication of all Muslim people worldwide". Apart from the application of the subjective territorial principle (which grants jurisdiction to the State hosting such content), it may be argued that since the statement was not directed to any State, no State has jurisdiction under the targeting approach.

203 Brandeis Institute for International Judges, "Issues of Concurrent Jurisdiction" (2012) https://www.brandeis.edu/ethics/pdfs/internationaljustice/biij/Con_Juris_2012.pdf (accessed 8 December 2017); Cherif Bassiouni, *International Extradition: United States Law and Practice* (Oxford University Press, 2014) at p 492.

204 *Dow Jones & Co Inc v Gutnick* [2002] HCA 56 at [24].

Conversely, it could also be said that the statement was directed to every State that has Muslims living within its territory.

85 However, while such publications may not be "targeted" *per se*, the aforementioned multi-factorial jurisdictional test for targeting[205] may still be of use – the central inquiry of international law jurisdiction, namely whether a State possesses a substantial connection to an individual that justifies its assertion of jurisdiction over him or her,[206] may still be addressed by this test.

86 For instance, for the statement calling for the "eradication of all Muslim people worldwide", a State applying the multi-factorial targeting test may decide to place more emphasis on the two factors of "the proportion of the overall publication that took place within a state" and "the foreseeable effect of the publication upon the territory", rather than the content and context of the publication. A State could decide to take jurisdiction on the basis that the website hosting the statement was heavily frequented by its citizens, or that the statement had the potential to incite hatred and violence given the State's sensitive socio-cultural history.

87 Moreover, it must be emphasised that the territorial principle is not the only potentially applicable head of jurisdiction with regard to untargeted Internet publications. Other jurisdictional principles such as the aforementioned nationality principle would be readily applicable if the original author of the statement can be identified. Furthermore, as a practical solution, states may elect to block access to such sites by citizens within their State, although this would almost certainly involve issues relating to the freedom of information.[207]

C. Conclusion

88 Ultimately, while the adoption of the targeting approach may alleviate some of the jurisdictional problems posed by the unique nature of cyberspace, it cannot be considered a silver bullet. Nevertheless, the certainty and fairness that it allots to states and individuals alike should be seen as a positive step towards achieving the delicate balance between free speech and the need for public order.

---

205 See para 73 above.

206 See para 15 above.

207 United Nations Educational, Scientific and Cultural Organization, "About Freedom of Information" http://www.unesco.org/new/en/communication-and-information/freedom-of-expression/freedom-of-information/about/ (accessed 8 December 2017).

89 As Sir Malcolm Evans astutely noted, the jurisdictional principles of international law "are truly principles, and not rules".[208] While we must be wary of unnecessarily fragmenting the law in the face of continually emerging new technologies, the sheer scale of the Internet renders it necessary to modify and adapt traditional legal principles in a manner that preserves certainty in the law, lest absurd results arise. Such incremental improvements are indispensable to the development and improvement of international law.

208 Malcolm Evans, *International Law* (Oxford University Press, 4th Ed, 2014) at p 337.