KING'S College LONDON

Is Enforcement in the Domain Name System a Legitimate Solution to the Jurisdiction Problem seen in Google v Equustek

James Taylor

Contents

1. Introduction

"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace … you have no sovereignty where we gather."

John P. Barlow[1]

Getting to grips with intellectual property rights (IPR) enforcement on the territory-averse Internet presents a challenge to the philosophy of jurisdiction. 'Cyberspace' has fundamentally changed the way humans share information; we are able to seamlessly disseminate educative, creative and communicative content electronically across the globe. Perhaps inevitably, it is also used to facilitate illegal activity; online piracy and counterfeiting are unquestionably a plague upon the economy.[2] Whilst technology advances at pace, the law is sluggish.[3] *Google v Equustek* demonstrates that the borderless Internet facilitates and assists cross-border IPR infringement, whilst forcing judiciaries to commit jurisdictional overreach by enjoining a domestic injunction on a global network. Both these situations are dangerous. It is necessary to find the way between Scylla and Charybdis, by ensuring adequate IPR enforcement whilst respecting sovereignty.

This paper will examine jurisdiction on the Internet and demonstrate how an international dispute resolution mechanism with remedial power through the Domain Name System (DNS), applying internationally recognised minimum standards of IPR protection, can legitimately address the jurisdictional conflicts that arise in IPR protection on the Internet. Inquiring whether this presents 'legitimate' solutions to the jurisdictional and comity issue necessitates discussion on the practical effectiveness of DNS enforcement. In this regard, we see that whilst DNS enforcement can be beneficial at law, it may not be so for Internet technicians; however, other methods of tackling IPR infringement are generally more evadible. By accepting universal takedown as the most

---

[1] John Barlow, 'A Declaration of the Independence of Cyberspace' (1996) EFF <https://www.eff.org/cyberspace-independence>

[2] World Intellectual Property Organisation, *Intellectual Property on the Internet: A Survey of Issues* (December 2002)

[3] Mojdeh Bower, 'Cyberspace, The Final Frontier: Examining the International Trade Commission's Jurisdiction Over Digital Information' (2018) 27 FCBJ 213

effective way of tackling IPR breaches, we then must avoid clashes between States' differing IPR standards. Arbitration can provide the solution, as the jurisdiction of a dispute resolution body comes from the consent of the parties involved, rather than notions of territory.

2. Domain Name System

2.1 Introduction

The DNS is an expansive and complex ecosystem of protocols,[4] governing the accessibility and portability of the Internet.[5] The predominant function of the DNS is the conversion of an Internet Protocol (IP) address (represented by a string of numbers), into an alphanumeric sequence: a 'domain name' that is easier for humans to recall and use.[6] Within the DNS is an array of institutions and technical systems that underpin its functioning.[7] The syntax of domain names consists of a 'second level domain' which is generally the primary indicator (the 'Google' in www.google.com), and the 'top level domain' which is then categorised as either 'generic' (gTLD (e.g. '.org')) or 'country code' (ccTLD (e.g. '.fr' for France)). The registration and management of domain names is accomplished through 'registrars' and 'registries' respectively.[8] Whilst there are differences between the two, 'registrars' and 'registries' both act as Internet intermediaries and are targeted similarly by the law.[9]

2.2 ICANN

The Internet Corporation for Assigned Names and Numbers (ICANN) is a labyrinthine non-profit 'partnership of people'[10] formed in 1998. Initially part of the US Department of Commerce, ICANN is now a global independent entity, overseen only by its stakeholders.[11] The development of policy within ICANN is rooted in its many internal

---

[4] Samantha Bradshaw, 'The politicization of the Internet's Domain Name System: Implications for Internet security, universality, and freedom' (2018) 20 NM&S 332, 334
[5] Sebastien Schwemer, 'On Domain Registries and Website Content' (2018) CIR <https://ssrn.com/abstract=3107547>
[6] Bradshaw, *supra* n.4
[7] ibid.
[8] Schwemer, *supra* n.5
[9] Compare, for example, *Cartier International AG v Nominet UK* (2013) Claim HC13 B04781 (against a registry) with the *Universal Music v Key-Systems GmbH* case *infra* (against a registrar)
[10] ICANN, 'What Does ICANN Do?' <https://www.icann.org/resources/pages/what-2012-02-25-en>
[11] The US is now represented as a member of the Governmental Advisory Committee (GAC), equal in power to other countries

and external bodies: such as the Supporting Organisations[12], Advisory Committees[13] and the Regional Internet Registries[14]. The technical function of ICANN is paramount to the worldwide web; it supervises the Internet Assigned Numbers Authority functions (IANA),[15] encompassing the DNS and IP address system, which dictate users' navigation of the Internet.[16] ICANN coordinates both gTLDs and ccTLDs and the mechanisms behind them.[17] It is this crucial technical mandate that ICANN is seen as the most powerful 'regulatory' body for the Internet.

2.2.1 Multi-Stakeholder Model

Whilst the myriad of stakeholder organisations involved in ICANN lacks transparency,[18] its 'bottom-up' and 'decentralised' approach "allows for community-based consensus-driven policy-making"[19]. This in theory puts "individuals, industry, non-commercial interests and government on an equal level"[20]; a suitably open and equitable forum for driving Internet policy. However, as Bridy opines, this structure does not reassure participation from individuals and public interest groups.[21] In fact, those corporate entities with more economic resources still prevail, due to the superior knowledge of the internal powers at ICANN that "savvy lobbyists"[22] retain, whilst the investment (time and money) necessary for 'less powerful' stakeholders bars their voices from being heard.[23] Further, enforcement agreements entered into with corporate rightsholders and online intermediaries are exclusive, meaning individuals have unequal standing.[24] It is worrying, therefore, that with the potential regulatory power of ICANN, policymaking

---

[12] Internal bodies that aid policy making with regards to the DNS and IP system
[13] Consists of four advisory committees including the GAC
[14] Represent geographic areas and are responsible for IP addresses within their respective regions
[15] ICANN, 'IANA Functions: The Basics' <https://www.icann.org/en/system/files/files/functions-basics-07apr14-en.pdf>
[16] Cecilia Testart, 'Understanding ICANN's complexity in a growing and changing Internet' (2014), 2
[17] ibid., 6-7
[18] Annemarie Bridy, 'Notice and Takedown in the Domain Name System: ICANN's Ambivalent Drift into Online Content Regulation' (2017) 74 W&L L Rev 1345, 1350-1351
[19] ICANN, 'Beginner's Guide to Participating in ICANN' (2013) <https://www.icann.org/en/system/files/files/participating-08nov13-en.pdf> 2
[20] ibid.
[21] Bridy, *supra* n.18
[22] ibid., 1352 (Using "commercial actors like the MPAA and [RIAA]", who are members to an internal body within ICANN, as an example.)
[23] ibid., 1351-1352
[24] Annemarie Bridy, 'A Response to Paul Vixie's "Notice, Takedown, Borders and Scale"' (2017) <http://cyberlaw.stanford.edu/blog/2017/03/response-paul-vixie%E2%80%99s-notice-takedown-borders-and-scale%E2%80%9D>

on the Internet could be subject only to powerful corporations. Concerns over corporate rightsholders disproportionately having greater influence than individual rightsholders must not be dismissed as merely 'complaints against corporatism'[25], especially where one envisages the freedoms provided by the Internet being at the behest of solely economically-driven corporations.

2.2.2 Web of Contracts

In response to US enforcement actions in 2010, ICANN emphasised that it has "no technical or legal authority" to take down domains, which is instead an "issue of national authority".[26] However, governments and private entities are increasingly using ICANN's web of contracts with DNS intermediaries to impose blocking measures.[27] An eminent example is the 'Trusted Notifier' program instigated in the new gTLD roll-out.[28] Domain name registries Donuts and Radix have partnered with the Motion Picture Association of America (MPAA), along with an agreement between Radix and the Recording Industry Association of America (RIAA), to allow special 'expeditious' treatment for notifications made by 'industry representatives'.[29] There is no requirement for a registry to investigate the complaint, thus allowing for a "rubber stamp approach" to takedowns.[30] This scheme has been made possible by 'trickle-down'[31] clauses in ICANN's contracts with registries,[32] which have been enhanced by initiatives such as the 'Public Interest Commitments'[33] and 'Healthy Domain Initiative'[34].

IPR enforcement on the DNS should not be generated through the backdoor.[35] Left ungoverned, private entities such as the MPAA and RIAA are free to over-enforce, likely

---

[25] Paul Vixie, 'Notice, Takedown, Borders and Scale' (2017) <http://www.circleid.com/posts/20170301_notice_takedown_borders_and_scale/#add_comment>
[26] ICANN, 'ICANN Doesn't Take Down Websites' (2010) <https://www.icann.org/news/blog/icann-doesn-t-take-down-websites>
[27] Bridy, *supra* n.18
[28] ibid., 1371
[29] ibid., 1372
[30] ibid., 1373
[31] For example, the requirement to include Specification 11 terms in contracts between registry services and registrars, which then is included in contracts between registrars and registrants
[32] Hong Xue, 'Caveats of Intermediary Liability in Domain Name System' (2014) GigaNet, Annual Symposium 2014
[33] Bridy, *supra* n.18, 1365
[34] ibid., 1364
[35] Bridy, *supra* n.24

causing drastic cooling-effects on creativity.[36] A coalition of private bodies, such as the Trusted Notifier program, must have some outside public influence to ensure the 'checks and balances' of powers. Whilst this author highlights that the judiciary and government are susceptible to the problem of jurisdiction, this does not amount to any support of private 'shadow regulation' that 'reshapes' the Internet with no input from its users.[37]

2.3 Intermediary Accountability: From Google to Registrars

As will be evidenced in *Google v Equustek*, attaching liability to intermediaries is an attractive proposition for governments and law courts alike, as intermediaries are global and lack oversight measures,[38] allowing for remedies previously unattainable with traditional boundaries.[39] Intermediaries have been the target of IPR litigation since the early phases of the Internet.[40] Considering that the intermediary is easier to track down[41] and has "deeper pockets" than the malfeasant themselves,[42] it is not surprising that cases involving online copyright infringement and counterfeiting evolved into disputes over intermediary liability.[43]

An 'internet intermediary' "[facilitates] transactions between third parties on the Internet … they give access to, host, transmit and index content … or provide Internet-based services".[44] This includes Internet Service Providers (ISPs), search engines and domain name registrars.[45] As quasi-regulators, intermediaries enforce IPRs 'voluntarily' in the absence of legislative provisions.[46] In practice, however, there is very little 'voluntary' about intermediaries' regulatory actions; pressure from both government and private interest parties, in addition to the threat of legal action, persistently looms over Internet intermediaries.[47] Liability for infringing content is an ever increasing

---

[36] ibid.
[37] EFF, 'Shadow Regulation' <https://www.eff.org/issues/shadow-regulation>
[38] Natasha Tusikov, 'Internet Firms as Global Regulators' (2018) GigaNet, Annual Symposium 2017, 15
[39] ibid., 5
[40] See *Religious Tech. v Netcom On-Line* (1995) 907 F. Supp. 1361
[41] See, for example, hidden WHOIS registrations that hide the identity of the registrant; Ian Block, 'Hidden Whois and Infringing Domain Names: Making the Case for Registrar Liability' (2008) 12 UCLF 431
[42] Sharon Bar-Ziv et al., 'Behind the Scenes of Online Copyright Enforcement: Empirical Evidence on Notice & Takedown' (2017) 50 CLR, 9
[43] ibid.
[44] OECD, 'The Economic and Social Role of Internet Intermediaries' (April 2010) 9
[45] ibid.
[46] Tusikov, *supra* n.38, 1
[47] ibid.

risk;[48] they are expected to monitor content on their services or platforms, despite how economically burdensome and theoretically difficult this is in a dynamic cyber-landscape.[49] Domain name registration and hosting services[50] are increasingly targeted as accountable intermediaries.[51] This trend is particularly apparent in the above-mentioned regulatory measures in the new ICANN gTLDs program, which introduces procedures that could hold registries accountable for third-party infringements.[52]

There are guidelines for safe practice regarding intermediaries' liability. In 1998, a piece of American legislation, the Digital Millennium Copyright Act (DMCA), created a 'safe harbour' for internet intermediaries, striking a balance between protecting the economic interests of intermediaries and IPRs.[53] The DMCA regime has influence around the world, having served as the template for many similar safe harbour provisions, including those of the European Union, United Kingdom and China.[54] The DMCA is the foundation of notice and takedown requests, a system that "bypasses judicial oversight", therefore also bypassing the jurisdiction issue.[55] The issue with notice and takedown methodology, as it exists in the DMCA, is that intermediaries too often are unable to process a multitude of DMCA requests or are simply unwilling to uphold IPRs.

3. *Google v Equustek*

3.1 Facts of the Case

[48] Hazel Murphy, 'The Role of a Domain Name Registrar as an Internet Intermediary' Tilburg Uni., 15 <http://arno.uvt.nl/show.cgi?fid=141685>
[49] See, for example, *Universal Music v Key-Systems GmbH* [2014] Regional Court Saarbrücken
[50] See, for example, *Louis Vuitton Malletier, S.A. v Akanoc Solutions, Inc.* (2001) 658 F.3d 9th. Circuit
[51] Wendy Larson, 'Internet Service Provider Liability: Imposing a Higher Duty of Care' (2014) 37 CJL&A 573, 574-575
[52] Xue, *supra* n.32
[53] Bar-Viz, *supra* n.42, 8
[54] Daniel Seng, 'The State of the Discordant Union: An Empirical Analysis of DMCA Takedown Notices' (2014) 18 Uni. Virginia 370, 374
[55] ibid., 376

Equustek, a small Canadian technology company, brought action against Datalink for various intellectual property breaches. Datalink used confidential information to develop a rival product and had sold Equustek products as its own. The first injunction was granted in 2011, ordering the return of possessions amongst other reparative actions. In 2012, Datalink was found to be non-compliant with the injunction. After subsequently leaving the Canadian jurisdiction, Datalink set up "a myriad of shell corporations in different jurisdictions" and continued commerce.[56] A Mareva injunction, shortly followed by an interlocutory injunction, were granted, with the judges citing a 'drastic' reduction in Equustek's earnings in its reasoning.[57] The court orders did not have the desired effect of curtailing Datalink's commerce which had instead grown worldwide.[58]

The most problematic part of this dispute was how to remedy the issue. Having left Canada, Datalink continued to breach Equustek's IPRs by continuing its business online based in an unknown location. By simply creating new pages to host the offending content, Datalink evaded takedowns with ease, meaning any prohibitory orders were reduced to a game of worldwide whack-a-mole. Google, the market-leading online search engine,[59] were brought into the dispute due to its perceived 'enabling' of Datalink's business: although an innocent party, Google made Datalink's website accessible through hosting links in its search results.[60] Google agreed to de-index a substantial number of pages linked to Datalink's website, but this had little practical effect.[61] A British Columbia court thus ordered an interlocutory injunction entailing the de-indexing of all parts of Datalink's website on all Google domains.[62] Google's de-indexing had up to this point been limited to google.ca. The Supreme Court of Canada heard Google's appeal in *Google v Equustek*, with the legitimacy of the above injunction questioned. The foundations of Google's concerns about the injunction were the principles of international comity and jurisdiction.[63]

---

[56] *Google Inc. v Equustek Solutions Inc.*, 2017 SCC 34 [2017] 1 S.C.R 824, [8]
[57] ibid. [9]
[58] ibid. [11]
[59] A market share of 86% as of April 2018 (Statista)
<https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/#0>
[60] *Equustek Solutions Inc. v Jack*, 2014 BCSC 1063, [8]-[9]
[61] *Google v Equustek*, *supra* n.56, [16]
[62] ibid. [17]-[18]
[63] ibid. [36]

3.1.1 Problem A: Court's Jurisdiction

The internet is not totally blind to existing geographical boundaries (i.e. IP addresses), although they are transposed onto the internet minus the strict governance of their physical counterparts.[64] Further, e-commerce enables situations to exist where many different jurisdictions can reasonably claim to have authority to hear a private commercial dispute. In this light, a territorial approach to establishing jurisdiction does not smoothly accommodate the Internet.[65]

The arguments around how Google, a Delaware incorporated company headquartered in California with no offices in British Columbia, became answerable to the *prima facie* dispute provide an interesting prelude to the discussion on the jurisdictional issues of the injunction. Determination of personal jurisdiction (jurisdiction over the parties involved) generally abides by rules enshrined in geographical location.[66] However, by finding that Google did carry out business in British Columbia, the "world-wide nature of Google's business" had to be considered.[67] Google's services permeate international boundaries in a non-traditional manner: this was noted in *Equustek v Jack* where it was accepted that "use of the Internet in the course of conducting business does not mean the business … is carried on globally for the purposes of a territorial competence analysis" (as per *Thumbnail v Blu*).[68] Collecting data of users in British Columbia and the subsequent selling of advertising space were held to sufficiently satisfy the requirement of a 'real and substantial' connection between Google's operations and the Court's jurisdiction.[69] The notion that Google offers a 'merely passive' website in British Columbia was rejected. However, the Court appreciated the difficulties in coming to this conclusion,[70] and cited cases that provided a semblance of guidance, including the criticised American *Zippo* case which set a vague threshold of 'interactivity' in its

---

[64] Marketa Trimble, 'Geoblocking and "Legitimate Trade"' (2018) (*Intellectual Property and Obstacles to Legitimate Trade*, Wolters Kluwer, forthcoming 2018)
[65] Michael Douglas, 'A Global Injunction Against Google' (2018) LQR 183
[66] Alan Tramwell, 'Personal Jurisdiction and the "Interwebs"' (2015) 100 Cornell L. Rev. 1129, 1131
[67] Douglas, *supra* n.65
[68] *Equustek v Jack*, *supra* n.60, [35]
[69] Douglas, *supra* n.65, 182
[70] *Equustek v Jack*, *supra* n.60, [37]

jurisdictional analysis.[71] The Google website was apparently 'interactive' due to the predictive suggestions that appear when a user begins to type a search query.[72] To what extent this reasoning should be followed in future cases is unclear: not only does it ignore the intricacies of how the Google search engine works,[73] it is unclear whether the Court correctly applied *Zippo*, or indeed whether it meant to at all.[74] The Court also distinguished the *Van Breda* case which stated that "advertising in a jurisdiction is not by itself … sufficient … to establish territorial competence": instead Google had been "engaging in the business of selling advertising space" which should be treated differently.[75]

The judgment borrowed some reasoning from European courts, particularly *Google Spain*,[76] regarding Google's amenability to non-American jurisdictions.[77] The British Columbia court's use of *Google Spain* in finding 'establishment' to claim jurisdiction is flawed, given the difference in nature between the disputes in *Equustek* and *Google Spain*. Whilst the jurisdictional issues in the two cases bare resemblance, in *Google Spain*, the protection of privacy (as a fundamental right) can be seen as 'universal' in nature.[78] Rather than protecting fundamental rights, the *Equustek* case involves a private intellectual property dispute; in fact the European Court itself, in *Google France v Louis Vuitton*, refrained from attributing responsibility to Google in an intellectual property dispute.[79] The position of the European Court on intermediary accountability in private tort actions is based upon a European Union Directive, which would have been more appropriate for the British Columbia judges to draw upon, given that it has

[71] ibid. [42]-[46]. The Court in *Zippo*, a trade mark case, found that a subscription website had been conducting e-commerce because of the 'interactivity' of the website (as opposed to being a 'passive' website) and was therefore under jurisdiction of the Court
[72] Sophie Stoyan, 'Just a click away? Jurisdiction and virtually carrying on business in Canada' (2017) J. Private Intl. L. 602, 615
[73] ibid., 616
[74] ibid.
[75] *Equustek v Jack*, *supra* n.60, [52]
[76] C-131/12 *Google Spain SL, Google Inc. v Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez* [2014] CJEU
[77] Krystyna Kowalik-Banczyk 'Migration of European Judicial Ideas concerning Jurisdiction over Google on Withdrawal of Information' (2016) 17 German L.J. 315, 327
[78] ibid., 328
[79] ibid., 329-330

previously facilitated injunctions against intermediaries in disputes resembling *Equustek*.[80]

The Court also gave little credence to Google's 'floodgate' defence (that this case sets a precedent exposing Google to limitless litigation across the world), stating that "jurisdiction will be confined to issues closely associated with the forum"; this is a reasonable assessment, but perhaps puts too much faith in the strength of the threshold.[81] The requirement for a 'real and substantial' association comes from Canadian domestic law (s3(e) Court Jurisdiction and Proceedings Act, S.B.C (2003)), and so is not necessarily representative of how other jurisdictions will establish the necessary nexus. Instead, customary international law simply dictates that "a State may not exercise its jurisdiction when it has no legitimate interest in or … is not affected by an activity."[82]

3.1.2 Problem B: Extraterritorial Remedy

Conflicts between the laws of nations, and how judicial bodies deal with those conflicts in cross-border private disputes, is not a new challenge.[83] The principle of *comitas gentium*, as expounded by Huber in the seventeenth century, stipulates that the recognition of another sovereign's laws is part of sovereignty itself.[84] This has developed into what is now considered 'international comity' (the respect for other nation's laws), a doctrine that is not part of international law, but is customary in the conflict of laws between nations.[85] Where a court order has extraterritorial effect, conflict can occur where that order is inconsistent to another country's value structure.[86] Take for example the 'right to be forgotten' as espoused in *Google Spain* and enforced in *Google France*,[87] which has been expressly described as "not recognised"[88] in the US, criticised

---

[80] E-Commerce Directive (2000/31/EC). See, for example, *L'Oreal v eBay* (C-324/09) finding that eBay could be injuncted as the Art. 14 defence could not be applied

[81] *Equustek v Jack*, *supra* n.60, [64]

[82] Cedric Ryngaert, *Jurisdiction in International Law* (Oxford University Press, 2008) 21

[83] Irina Getman-Pavlova, 'The concept of "comity" in Ulrich Huber's conflict doctrine' (2012) National Research University <https://f-origin.hypotheses.org/wp-content/blogs.dir/818/files/2013/04/The-concept-of-%E2%80%9Ccomity%E2%80%9D-in-Ulrich-Huber%E2%80%99s-conflict-doctrine.pdf>

[84] ibid. [13]

[85] Joel Paul, 'The Transformation of International Comity' (2008) 17 Law & Cont. P 19

[86] Brian Benko, 'Russia and Allofmp3.com: Why The WTO And WIPO Must Create a New System for Resolving Copyright Disputes in the Digital Age' (2016) 1 AIPJ 299, 305

[87] National Commission on Informatics and Liberty, 'CNIL Orders Google to Apply Delisting on All Domain Names of the Search Engine' (12 June 2015) <https://www.cnil.fr/en/cnil-orders-google-apply-delisting-all-domain-names-search-engine>

in the Corte Constitucional of Colombia,[89] and has caused unease in the judiciary of Japan.[90] *LICRA v Yahoo!* is a seminal Internet jurisdiction case that showcased a skirmish between European and American attitudes towards freedom of speech.[91] The sale of Nazi memorabilia on the Yahoo website, illegal under French law,[92] facilitated a debate over 'localisation' of the infringing content (Yahoo servers physically located in the US) versus their 'visualisation' (computer screens in France).[93]

The Google order, affecting searches on all Google domains, is effectively a global injunction. By giving this order, the Canadian Supreme Court authorises an equitable remedy that has extraterritorial implications, with little credence given to comity.[94] The Court referenced other types of injunctions that have international effect, such as *Norwich* orders, which also require cooperation from third-parties.[95] The Court dismissed international comity issues as 'theoretical' and therefore unnecessary to adjudicate upon.[96] This included, in this case correctly, the dismissal of freedom of speech arguments made by Google, saying it is not "accepted that freedom of expression requires the facilitation of the unlawful sale of goods."[97] This is not the first time the Court has grappled with the interplay between private international law, equitable remedy, and the Internet. In *Pro Swing v ELTA Golf*, the Canadian Supreme Court stated that "extraterritoriality and comity cannot serve as a substitute for a lack of worldwide trademark protection", accepting a tendency for equitable relief to include an element of judicial overreach due to the nature of the Internet.[98] Other countries exercise caution with extraterritorial orders. English courts have appreciated the intricacies of imposing

---

[88] Reporters Committee for Freedom of the Press, *Statement on Case C-507/17* (29 Nov 2017) 9 <https://www.rcfp.org/sites/default/files/2017-11-29-Googe-v-CNIL.pdf>
[89] Colombian Constitutional Court, judgment of 12 May 2015, No. T277 *Gloria v. Casa Editorial El Tiempo*, p45
[90] 12th Civil Division of the Tokyo High Court, judgment of 12 July 2016, No. 192, *Google Inc. v. Mr. M*
[91] Raphael Cohen-Almagor, 'Freedom of Expression, Internet Responsibility, and Business Ethics: The Yahoo! Saga and Its Implications' (2012) 106 J Bus Ethics 353
[92] ibid.
[93] Joel Reidenberg, 'Yahoo and Democracy on the Internet' (2001) 42 Jurimetrics 261, 266
[94] Christina Etteldorf, 'Canadian Supreme Court on Google: Effective Legal Protection Tops Jurisdictional Boundaries' (2017) 3 EDPLR 384, 385
[95] Stephen Brown-Okruhlik, 'The New Frontier of Jurisdiction: Supreme Court of Canada Upholds Worldwide Injunction Against Google' (2017) McMillan <https://mcmillan.ca/Files/199962_The-New-Frontier-of-Jurisdiction.pdf>
[96] ibid.
[97] *Google v Equustek*, *supra* n.56 [48]
[98] Brown-Okruhlik, *supra* n.95

injunctions on third-parties whose operations extend abroad.[99] For example, in *Babanaft Int'l, v Bassante*, Nicholls LJ highlighted the "extraterritorial vice" that accompanies unqualified injunctions,[100] and Kerr LJ stated that the important aspect is "whether there is international reciprocity for the recognition and enforcement of the … order".[101] The final decision was to grant an injunction qualified by its enforcement at local law, so as not to assume extraterritorial jurisdiction.[102] Also, in the Australian case of *Macquarie v Berg*, restraint was shown: a New South Wales court expressed fears of 'superimposing' its laws onto other territories when "restraining publication on the Internet".[103] Interestingly, Fenlon J, who ordered the *Equustek* injunction, refrained from issuing an injunction in *Niemela v Malamas* on the grounds that it would go against comity, citing the US Communications Decency Act ('CDA') of 1996 as a statute that would prevent the injunction taking hold in the US.[104] This author highlights the difference with orders that may restrict freedom of speech (as with *Niemela*, a defamation case), in contrast with the restriction of counterfeiting (as with *Equustek*) which does not implicate restriction of fundamental rights. This is, as can be implied from *Equustek*,[105] a predominant reason for the discrepancy between *Niemela* and *Equustek* in the application of comity.

The Canadian Supreme Court stated that it would consider evidence demonstrating the *Equustek* injunction contradicting other nation's laws if Google provided such evidence.[106] Google was subsequently granted preliminary relief in the US, where a Californian District Court decided the *Equustek* injunction contradicted the aforementioned CDA 1996,[107] which effectively grants immunity to 'interactive

---

[99] ibid.
[100] *Babanaft International Co. SA v Bassante* [1989] 1 All ER 433, 454
[101] ibid., 440
[102] ibid.
[103] *Macquarie Bank Limited & Anor v Berg* [1999] NSWSC 526 [14]
[104] *Niemela v Malamas* [2015] BCSC 1024 [33]
[105] *Google v Equustek*, *supra* n.61, [45]
[106] Mark Weston, 'Google v. Equustek: United States Federal Court Declares Canadian Court Order Unenforceable' (2017) < https://jolt.law.harvard.edu/digest/google-v-equustek-united-states-federal-court-declares-canadian-court-order-unenforceable>
[107] Robert MacDonald, 'The Google Inc. v. Equustek Solutions Inc. Decision' (2017) < https://gowlingwlg.com/en/insights-resources/articles/2017/google-inc-v-equustek-solutions-inc-decision/>

computer services' against third-party breaches.[108] With this evidence, Google applied for modification of the *Equustek* injunction in British Columbia, yet this motion was rejected. The court maintained that the *Equustek* injunction did not violate US law, rather it 'only' restricted "ability to exercise certain rights",[109] and that the US finding would not "restrict the ability of this Court to protect the integrity of its own process … over [parties] it has personal jurisdiction [over]."[110] Although displaying little regard for international comity, the British Columbia court acknowledged that the US order allows "no action [to] be taken against Google to enforce the injunction in US courts."[111] This interaction between Canadian and US courts demonstrates the difficulty in consolidating the judicial decisions of different jurisdictions.

3.2 Sovereignty and Territory

A strict adherence to territory-based jurisdiction principles is difficult to reconcile with policing content on the Internet.[112] In contrast, the IPRs that we wish to enforce, such as trade marks and copyright, are intrinsically territorial. The issue at hand is complex, as is finding the adequate solution in international law. However, the principles underpinning international law should not be given absolutist credentials or mistaken for hard-law.[113] For example, sovereignty (i.e. power that is not subject to outside actors)[114], retains a more 'underlying' role in the current practices of international law.[115] Therefore, it cannot be categorically said that sovereignty is a 'right' that can be violated,[116] although evidence exists to suggest it does operate as a source of dispute in absence of other violations.[117] Taking an extreme 'separatist' view of the Internet would disregard these concepts altogether, though this is demonstrably implausible

---

[108] Brent Arnold, 'Equustek Again: BC Supreme Court Upholds Worldwide Injunction Despite US Refusal To Enforce' (2018) < https://gowlingwlg.com/en/insights-resources/articles/2018/equustek-again-bc-supreme-court-upholds-injuction/#_ftn8>
[109] *Equustek Solutions Inc. v Jack* (2018) BCSC 610 [20]
[110] ibid. [22]
[111] ibid.
[112] Dan Svantesson, 'Lagom Jurisdiction – What Viking Drinking Etiquette Can Teach Us About Internet Jurisdiction and Google France' (2018) 12 Mas. UJL&T 29, 33
[113] ibid., 34
[114] See Grotius and Westphalian definition of 'sovereignty'; Benjamin Straumann, 'Early Modern Sovereignty and Its Limits' (2015) 16 TIL 423, 424
[115] Gary Corn & Robert Taylor, 'Sovereignty in the Age of Cyber' (2017) AJIL 111, 208
[116] Svantesson, *supra* n.112, 38
[117] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn CUP 2017) 215

methodology.[118] A balance between accepting the implications of enhanced global data liquidity and giving due credence to the established and legitimate concepts of the State, jurisdiction and sovereignty is necessary.

The 'State' is effectively an "imagined community" which expresses the *Volksgeist* and fulfils a shared communion of values.[119] This communion is demarcated by its arbitrary territory.[120] The Westphalian idea of territorial sovereignty comes from both the 'monopoly of violence' within the State, and the external equality between States (or the 'Westphalian equilibrium').[121] It is with this 'equilibrium' that comity exists; the non-intervention of other States' rule of law out of respect for the coequality in "the global task of judging".[122] However, it is not unprecedented for an equitable remedy to enjoin onto 'unconscionable' conduct which occurs outside the court's jurisdiction; this is hypothetically justified because 'equity' is universal.[123] However, equity, in practice, is applied differently across nations.[124] A global delisting order against Google necessitates that the domestic court in *Sovereign X* is restricting content accessible within S*overeign Y*, therefore depriving *Sovereign Y* primacy over the exercise of that State function.[125] This, in theory, is an interference with the classical exposition of sovereignty.

The 'territoriality' principle, intrinsically linked with sovereignty,[126] is the primary principle in ascertaining a *bona fide* connection between the dispute and the State.[127] As seen in the *Viewfinder*[128] case however, its application is too rigid to accommodate for data liquidity.[129] The enforcement of a French award of damages for copyright violations committed by an American company was rejected by a New York court due to the First

---

[118] Joel Reidenberg. 'Technology and Internet Jurisdiction' (2005) 153 U.PennLR 1951, 1958
[119] Thomas Schultz, 'Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface' (2008) 19 EJIL 799, 805
[120] ibid., 807
[121] ibid., 814
[122] Anne-Marie Slaughter, 'Judicial Globalization' (2000) 40 VJIL 1103, 1112
[123] Douglas, *supra* n.65
[124] Michael Akehurst, 'Equity and General Principles of Law' (1976) 25(4) ICLQ 801
[125] Svantesson, *supra* n.112, 39
[126] Marieke Koekkoek et al., 'Internet and Jurisdiction After Google Spain: The Extra-territorial Reach of the EU's "Right to be Forgotten"' (2015) KU Leuven Working Paper 152, 11
[127] John Currie, *Public International Law* (Irwin 2001) p.300
[128] *Louis Feraud Int'l SARL v Viewfinder Inc.* (SDNY 2005) 406 F Supp 2nd 274
[129] Schultz, *supra* n.119, 811

Amendment.[130] The New York court used the 'subjective territorial principle' to reject an encroachment onto its authority "to regulate activity originating within its territory".[131] The extension of this decision would open significant loopholes; infringers could forum-shop for weak IPR enforcement States, which would protect them from liability, and allow for the continuation of their infringements in the target State.[132] The 'effects' principle, meanwhile, allows States to "regulate behaviour which takes place outside its territory insofar as it produces substantial effects within its territory".[133] Thus, in the *Yahoo France* case, even though the auction of offending Nazi memorabilia was not being hosted in France, the fact that it has effects on the State due to its visibility within France was enough for the court to assume jurisdiction.[134] The effects principle logically suits cases involving antitrust or data privacy, but its implementation is generally controversial,[135] particularly with territorial rights such as IPRs. In addition, the effects principle in Internet cases could be limitlessly scalable, to the extent that it becomes impractical.[136] This was elucidated by Google in its 'floodgate' arguments against the *Equustek* injunction, stating it would be subject to enforcement jurisdiction from an unlimited amount of States.[137] A middle ground between 'territoriality' and 'effects' is the 'targeting' methodology, which takes into account where the offending website target audience is stationed. The 'targeting' criteria has benefits in establishing personal jurisdiction, allowing for localisation within State boundaries logically. On the other hand, ascertaining what 'targeting' is precisely, and indeed whether it existed in each case, adds another layer of complexity.[138]

The 'separatist' theory of the Internet promulgates the most minimum application of local laws as possible and amounts to a denial of classic jurisdiction.[139] As mentioned, the complete denial of jurisdiction made by separatism is simply not practicable and goes against established rules of public order.[140] For example, the separatist arguments

---

[130] ibid.
[131] ibid.
[132] ibid.
[133] Koekkoek, *supra* n.126, 12
[134] Schultz, *supra* n.119, 811
[135] Koekkoek, *supra* n.126, 13
[136] Schultz, *supra* n.119, 813
[137] *Equustek v Jack*, *supra* n.60, [64]
[138] Schultz, *supra* n.119, 815
[139] Reidenberg, *supra* n.118, 1953
[140] ibid., 1958

used by Yahoo in the *Yahoo France* case make ineffective France's genuine right to uphold its value structure.[141] However, this author believes a total rejection of separatist ideas is a denial of the true nature of the Internet. Like the open fora of ancient Greece where thought and ideas could be expressed, the Internet can be seen as a corollary of 'the public' and heavily linked with the idea of 'democracy' itself.[142] Another analogy could be made towards the Internet being an 'international space', much like the high seas,[143] where Grotius' *mare liberum* could be used as an example of the functioning of non-territorial space.[144] However, this author disagrees with this separation of cyberspace from real space: the Internet is more a 'tool' than a 'space',[145] servers and domain name registries for example are still physically located within a territory, as is the Internet end-user. Instead, we must recognise the complex 'heterotopia'[146] of the Internet, as opposed to debating Internet as a 'separate space' or a 'continuation of space'.[147] It is necessary therefore to reject the 'separatist' and 'realist' extremes, as neither are practical; a balance must be agreed upon.

4. DNS and Jurisdiction

4.1 The Case for Universality

Whilst courts are confined to dealing with borders, the DNS is borderless, and domain names as transliterations of IP addresses intrinsically abide by the 'universality principle'.[148] In establishing personal jurisdiction through the 'targeting' method, courts can logically find the nexus necessary to adjudicate. However, due to the global interconnectivity of the Internet, there is no way to fully stem cross-border encroachments resulting from one country's remedial orders.[149] Instead, we should focus on developing methodology that has more fidelity to the true nature of the Internet. The jurisdictional issues are caused by the awkward application of local laws

---

[141] Cohen-Almagor, *supra* n.91
[142] Zizi Papacharissi, 'The virtual sphere' (2002) 4 NM&S 9, 10
[143] Darrel Menthe, 'Jurisdiction in Cyberspace: A Theory of International Spaces' (1998) 5 MTTLR 69, 70
[144] Mireille Hildebrandt, 'Extraterritorial Jurisdiction to Enforce in Cyberspace? Bodin, Schmitt, Grotius in Cyberspace' (2013) 63 U TLJ 196, 211
[145] Jonathan Zittrain, 'Be Careful What You Ask For: Reconciling a Global Internet and Local Law' (2003) Berkman Center No. 2003-03, 8
[146] Hilderbrandt, *supra* n.144, 202; describing 'heterotopian' cyberspace as "spaces … which ordinary rules … may be suspended" and (at 198) that it "[crosses] over into the landscape of territorial jurisdiction while … evading … boundaries"
[147] ibid.
[148] Vixie, *supra* n.25
[149] Dan Svantesson, *Solving the Internet Jurisdiction Puzzle* (2017) 184

onto a ubiquitous global stratum of data flow.[150] Creating a *sui generis* body of law for the Internet has been supported by separatists,[151] but the differences in principle between, *inter alia*, countries such as Russia and China that have stricter control over Internet content,[152] suggest that common ground would be scarce. The Working Group on Internet Governance (WGIG) under the auspices of the United Nations underlined the importance of addressing 'limits of state competences', stating that "there are different views on the precise nature of the balance" between rightsholders and Internet users.[153] The censorship agendas of some countries could have serious extraterritorial effects; without the intervention of society-orientated organisations (as opposed to 'technical coordinators')[154] a sovereign state would attempt to "recreate the … control [of] traditional territorial media" on a grand scale.[155]

Fragmentation of the Internet has been on the agenda of governments and ISPs alike.[156] Theoretically, a 'balkanised' Internet allows for the application of sovereign value structures, utilising the Internet's already fragmented physical and logical infrastructure.[157] The DNS is under threat from the very jurisdictional problems *Equustek* portrays. However, instead of balkanising the DNS, the DNS can be used to promote interoperability, and therefore sustain the Internet's inherently cross-border functionality.[158] In some areas of Internet-related crime, tensions have been eased by cooperative treaties, such as the Budapest Convention.[159] Further fragmentation would put a strain on ISPs, unless the infrastructure of the Internet fully delineates.[160] This would represent a dangerous and unnecessary paradigm shift. The argument against harmonisation is that it could facilitate repressive policies,[161] but this author posits that

---

[150] Zittrain, *supra* n.145
[151] ibid.
[152] Alexandra Perloff-Giles, 'Transnational Cyber Offences: Overcoming Jurisdictional Challenges' (2018) 43 YJIL 191, 224
[153] Joanna Kulesza, 'Internet Governance and the Jurisdiction of States: Justification of the Need for an International Regulation of Cyberpaces' (2008) GigaNet, Annual Symposium 2008, 20
[154] Milton Mueller, *Networks and States: The Global Politics of Internet Governance* (MIT Press, 2010) p.201
[155] ibid., p.197
[156] Sergio Alves, 'Internet Governance 2.0.1.4: The Internet Balkanization Fragmentation' (2014) <https://ssrn.com/abstract=2466222>
[157] Laura DeNardis, 'One Internet: An Evidentiary Basis for Policy Making on Internet Universality and Fragmentation' (2016) CIGI Paper Series No. 38, 4
[158] ibid., 6
[159] Convention on Cybercrime (2001); see ibid.
[160] This would remove a layer of unpredictability for ISPs, see; Alves, *supra* n.156
[161] DeNardis, *supra* n.157, 6

the opposite approach (fragmentation) similarly facilitates repressive policies, albeit with the qualification of sovereignty. Instead, a "bottom-up approach" can involve many stakeholders in the process of producing desirable policy, namely that which protects IPRs and the access to information.[162] This is where international cooperation, having similar substantive enforcement as the Canadian courts in *Equustek* insisted upon, can solve the jurisdictional problem.

4.2 The ccTLD Fallacy

The issue in *Equustek*, with targeting Google as an intermediary, is that the separate 'country specific' domains (namely the various ccTLDs) can be construed to create pseudo-jurisdiction, which can logically be extended to create pseudo-territorial rights. Delisting across all Google domains means impeding access to the same domain name in each of these pseudo-jurisdictions. The delegation of ccTLDs stems from the DNS root zone files, held on servers around the world,[163] which is requested by an Internet user from potentially anywhere: it is inherently jurisdiction-neutral, with no State having any claim to it more than another.[164] The idea of jurisdictional competence manifested in a ccTLD delegation is irrational on basic grounds. Firstly, the delegation of ccTLDs is based on ISO-3166 alphabetic code for geographical territories,[165] not sovereign nations (a contentious example is the .cat ccTLD for Catalonia, the target of blocking orders from the Spanish government)[166]. Secondly, the link between a geographic territory and a ccTLD is merely semantic: it is not, and was never intended to be,[167] a way of apportioning administration to separate countries. Extending the principle that a state may claim jurisdiction over a resource or service purely due to its semantics would lead to preposterous results.[168] However, Google rightly points to statistics that the vast majority of those using a specific ccTLD are users within that territory.[169] This statistic should remain confined to arguments of 'effectiveness of the injunction', instead of being

---

[162] ibid.
[163] ICANN, 'There are not 13 root servers' (2007) <https://www.icann.org/news/blog/there-are-not-13-root-servers>
[164] Milton Mueller et al., 'Governing Internet Territory: ICANN, Sovereignty Claims, Property Rights, and Country Code Top-Level Domains' (2017) 18 Colum. S&TLR 435, 458
[165] ibid., 460
[166] Schwemer, *supra* n.5
[167] Mueller, *supra* n.164, 463
[168] Mueller, *supra* n.164, 462-463
[169] Peter Fleischer, 'Implementing a European, Not Global, Right to be Forgotten', Google Europe Blog (30 July 2015)

misused to construe pseudo-territorial rights in the DNS.[170] This thorny façade of 'Google-jurisdiction' can be removed from the debate in *Equustek*: instead, the intrinsically universal DNS provides a more solid theoretic foundation for adjudication. It is now necessary to examine the implications of DNS enforcement on a practical level.

5. Pushback Against DNS Enforcement

5.1 Issues Brought to Light by Failed US Legislation

The sinking of various bills that would have heightened DNS enforcement measures in the US demonstrate the various drawbacks of blocking, filtering or seizing directly on the DNS. Both the Stop Online Piracy Act (SOPA) and the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PROTECT IP) would have added DNS-redirecting to the governmental enforcement arsenal, as well as mandating cooperation from online intermediaries and ISPs.[171] Aspects of DNS filtering caught the attention of many critics of the proposed legislation, raising concerns that "tampering with the [DNS] … breaks Internet security and encourages the development of an insecure, offshore pirate DNS".[172] PROTECT IP also encompassed a broad range of intermediaries that a Court could require to undertake preventative measures (including small businesses, universities and non-profit organisations).[173] Other worries included the possibility of the Acts destroying established safe harbours, innovation and free speech.[174]

5.1.1 Security Risks

Analysis of some legal provisions for DNS filtering brings to light the security risk that follows from disrupting a foundational structure of the Internet.[175] The PROTECT IP Act would have mandated ISPs to filter and redirect attempts to access infringing domains.[176] Interrupting the connection between the requested domain and redirecting

---

[170] ibid.
[171] Bradshaw, *supra* n.4, 342
[172] Julie Ahrens, 'Stop Censorship: The Problems With SOPA' (2011) CIS <http://cyberlaw.stanford.edu/blog/2011/11/stop-censorship-problems-sopa>
[173] Mark Lemley et al., 'Don't Break the Internet' (2011) 64 Stan. LR 34
[174] Ahrens, *supra* n.172
[175] Macon Phillips, 'Obama Administration Responds to We the People Petitions on SOPA and Online Piracy' (January 2012) White House Blog
[176] Steve Crocker et al., 'Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill' (May 2011) 5

it to another IP address is fundamentally in conflict with the security measures on the DNS, such as the DNS Security Extensions (DNSSEC).[177] DNSSEC facilitates an authentication process that prevents attackers using DNS queries as a form of distributing malware.[178] Without DNSSEC, attackers can alter the pathway between the user's request and the requested resource, in order to redirect the user to an infected resource, enabling, *inter alia*, the theft of personal information such as credit card data.[179] The PROTECT IP Act's method of DNS filtering would "enshrine and institutionalize the very network manipulation DNSSEC [fights] in order to prevent cyberattacks".[180] Furthermore, evasion techniques likely to be used by motivated users of offending websites affect the stability of the DNS, and will reduce the ability of ISPs to combat evasion, due to, for example, increasing traffic to rogue servers.[181] There is also the risk of non-IANA DNSs being used for circumvention. An alternative DNS could be created by mirroring the IANA DNS and creating new TLDs within that system, putting the infringing material out of reach of law enforcement.[182] Logically, if the creation of alternate DNSs became commonplace, the principle of universal naming could be at risk, as Vixie elucidates; "[countries] who want to block certain new IANA TLD's … could do this in-country and force alignment by mandating the use of that country's DNS system", therefore this leads to "questions like 'which DNS system are you using?' … [meaning] a world without universal naming."[183]

5.1.2 Ineffectiveness

An overarching criticism of DNS seizure and blocking is that it is ineffective.[184] Infringing content remains online, though access to it is curtailed significantly: an Internet user would have to know the IP address of the website to access it. This means that an offending website that publicises its IP address, and encourages its users to save it, will be undeterred by a DNS seizure or block. In addition, it may not sufficiently deter the

---

[177] ibid.
[178] ibid.
[179] ibid.
[180] ibid., 6
[181] ibid., 11
[182] Paul Vixie, 'On Mandated Content Blocking in the Domain Name System' (2011) CircleID <http://www.circleid.com/posts/20110318_on_mandated_content_blocking_in_the_domain_name_system/>
[183] ibid.
[184] CDT 'The Perils of Using the Domain Name System to Address Unlawful Internet Content' (September 2011) <https://www.cdt.org/files/pdfs/Perils-DNS-blocking.pdf>

owner of the site to register a new domain. For example, both these methods of evasion were used by WikiLeaks in 2010, reinstating access to secretive governmental data just hours after it was taken down.[185] In addition, traffic data suggests replacement domains quickly garner comparable traffic to the captured or filtered domain, such as rojadirecta.es that effectively replaced the seized rojadirecta.com site.[186] More comparatively technical methods of evasion also exist, including software that retrieves IP addresses, local DNS resolvers and third-party DNS servers.[187] A user base with above-average technical knowledge could execute these methods of evasion.[188] Due to this, data shows only a relatively short term blockage of traffic on servers before content is moved to another domain or a breakthrough in circumvention occurs, such as the seized TVShack.net domain.[189]

5.1.3 Collateral Damage

In contrast to a more 'traditional copyright' approach to notice and takedown, DNS enforcement does not remove specific material, but will instead indiscriminately remove content under the same Domain Name.[190] Therefore, the risk of striking down legitimate and lawful content online is heightened. For example, 'parent domains' often subsist of numerous, and potentially unrelated, websites under one common second level domain which resolve to different IP addresses.[191] Enforcement action against the parent domain due to infringement on one of its subdomains, such as the Mooo.com case, will capture all its content regardless of legality.[192] US enforcement against Mooo.com resulted in over 84,000[193] innocent domains being filtered and redirected to an announcement of 'seizure by the US government due to child pornography violations'.[194] Given that the content on domain names, such as blogposts, can be the livelihood and primary means of money-making for their owners, the effects of collateral damage must

---

[185] Rob Pegoraro, 'WikiLeaks sinks, resurfaces (repeat as necessary)' (December 2010) The Washington Post Faster Forward Blog
[186] Crocker, *supra* n.176, 7
[187] CDT, *supra* n.184
[188] ibid.
[189] Crocker, *supra* n176, 7
[190] CDT, *supra* n.184
[191] ibid.
[192] ibid.
[193] Crocker, *supra* n.176
[194] CDT, *supra* n.184

not be understated.[195] Further, it is not easy to anticipate when collateral damage may occur, due the intricacy of some site's DNS records and the practice of 'virtual hosting'.[196]

5.2 Response to Criticisms

The above criticisms are well-founded but relate specifically to a sweeping set of US legislation. Generally, whilst DNS enforcement is possible to circumvent, the methods to do so are more technically advanced than the evasion techniques of, for example, geo-blocking. Software that identifies the geolocation of the site user to filter their access is effective only up until the use of a proxy server.[197] Delisting orders tailored to individual ccTLDs, as Google argues for in *Equustek*, are plainly ineffective, as a basic action can circumvent the order.[198] Identifying the infringers and tracking them down for criminal prosecution to prevent re-offending is another challenging task, but is achievable with current technology and cooperation from domain registry services.[199] Side-effects of DNS enforcement are the risks to the infrastructure and collateral damage. However, with cooperation from registrars, registries, and ICANN, a functional technical mandate for DNS enforcement can be construed.[200] This would create an effective means for curtailing IPR breaches; this author emphasises again that for *bona fide* IPR cases, no fundamental rights (such as freedom of speech) are at risk by initiating a global and resolute takedown. The next development therefore would be to ensure DNS enforcement remains strictly for obvious cases of piracy and counterfeiting and creating the means of oversight to impose this criterion; a lack of neutral oversight could lead to the formation of a slippery slope towards censorship.[201]

---

[195] Mike Masnick, 'Why PROTECT IP Breaks The Internet' (2011) Techdirt <https://www.techdirt.com/articles/20110531/13331214491/why-protect-ip-breaks-internet.shtml>
[196] Crocker, *supra* n.176, 13
[197] Koekkoek, *supra* n.126, 20
[198] ibid.
[199] See, however, TF, 'WHOIS Limits Under GDPR Will Make Pirates Harder to Catch, Groups Fear' (2018) <https://torrentfreak.com/whois-limits-under-gdpr-will-make-pirates-harder-to-catch-groups-fear-180413/>
[200] Francesca Musiani et al., *The Turn to Infrastructure in Internet Governance* (Springer 2016) p.96
[201] ibid., p.99

6. DNS Enforcement: Arbitration

6.1 The UDRP

ICANN's regulatory competence extends to trade mark violations in domain names through their Uniform Dispute Resolution Procedure (UDRP). It is important to note the distinction that the UDRP deals with trade mark violations in the domain names themselves, rather than counterfeiting or piracy *per se*.[202] The newfound practice of 'cybersquatting' and complaints from rightsholders, aghast at having to pay off registrants using their own trade mark in bad faith, led to the uneasy application of traditional trade mark law onto the DNS. The UDRP offers a speedy and cost-effective dispute resolution method.[203] Further, given the jurisdictional flexibility of arbitration, it bypasses territorial disputes over the trade mark in question. Instead, the UDRP 'effectively globalised' domestic trade mark rights, extending rightsholders' enforcement powers far beyond traditional borders, albeit confined solely to domain names.[204] Alternative dispute resolution, of UDRP ilk, departs from the traditional reliance on the legislator or judiciary to resolve disputes. Using arbitration as a dispute resolution mechanism over the courts of law is not without controversy: ensuring a 'fair trial' with due process, adequately scrutinising the decision-makers, and ensuring a route of appeal are just some of the issues that arise.

Whilst the UDRP was a success for trade mark rightsholders,[205] and an effective tool against cybersquatting,[206] it is an often-criticised policy. There are strong indicators of bias within the proceedings; panellists are not subject to specific disqualification criteria[207] and are usually experts in the field of trade mark law, which may put defendants at an immediate disadvantage.[208] There is a lack of procedural fairness

---

[202] ICANN, 'Uniform Domain Name Dispute Resolution Policy', Section 4(a) <https://www.icann.org/resources/pages/policy-2012-02-25-en>
[203] Bridy, *supra* n.18, 1356
[204] ibid.
[205] ibid.
[206] Milton Mueller, 'Success By Default: A New Profile of Domain Name Trademark Disputes Under ICANN's UDRP' (2002) Syr.Uni. 15
[207] Juan Dieguez, 'The UDRP reviewed: the need for a "uniform" policy' (2008) CTLR 133, 136
[208] Elizabeth Thornburg, 'Fast, Cheap, and Out of Control: Lessons from the ICANN Dispute Resolution Process' (2002) 7 J S&EBL 191, 221

protections enshrined in the policy,[209] in addition to overly strict time restrictions imposed on respondents.[210] Most worryingly, the UDRP lacks a strong deterrent against reverse domain name hijacking (RDNH), whereby bad faith complaints succeed in obtaining (or closing) a domain name,[211] and there have been examples of questionable decisions made under the UDRP.[212]

6.2 A Model Policy?

Despite its flaws, the UDRP has been mooted as an inspiration for enforcement against counterfeiting and piracy,[213] even in its formative years.[214] Suggested arbitration platforms for counterfeiting and piracy would be strictly for 'straightforward'[215] offences, mirroring the UDRP's admissibility criteria.[216] However, establishing clear-cut cases of copyright infringement, for example, likely presents more difficulties (e.g. defendant's fair use, evidence of 'copying' and the existence of copyright in the work itself) than that of cybersquatting.

Most recently, the Domain Name Association (DNA) and Public Interest Registry (PIR) had floated the idea of a 'Copyright Alternative Dispute Resolution Policy' (CADRP), which would have been a voluntary policy for registries.[217] The CADRP would focus on domains "where the alleged infringement is pervasive or where the primary purpose … is the dissemination of alleged infringing material".[218] A more technical and thorough exposition of the CADRP had been subject to finalisation with Forum, a firm which also plays a significant role in the UDRP.[219] However, the CADRP seems to have been

---

[209] M. Lemley & R. Reese, 'A Quick and Inexpensive System for Resolving Peer-to-Peer Copyright Disputes' (2005) 23 Card. A&ELJ 1
[210] Dieguez, *supra* n.207
[211] ICANN, 'Rules for Uniform Domain Name Dispute Resolution Policy' (2013)
[212] See, for example; *Fiber-Shield Industries, Inc. v Fiber Shield LTD,* NAF No. FA92054 (2000) which conflated a lack of 'superior' rights with 'legitimate' rights
[213] Andrew Christie, 'The ICANN Domain Name Dispute Resolution System as a Model for Resolving other Intellectual Property Dispute on the Internet' (2002)
[214] Laurence Helfer, 'International Dispute Settlement at the Trademark-Domain Name Interface' (2001) Int'l. L WWS 87, 89
[215] Lemley & Reese, *supra* n.209, 2
[216] ICANN, *supra* n.211
[217] Kevin Murphy, 'The Pirate Bay likely to be sunk as .org adopts "UDRP for copyright"' (2017) <http://domainincite.com/21517-the-pirate-bay-likely-to-be-sunk-as-org-adopts-udrp-for-copyright>
[218] Domain Name Association, 'DNA Healthy Domains Initiative: Registry/Registrar Healthy Practices' (2017) at Appendix D, 'Principles' < http://domainincite.com/docs/DNA-Healthy-Practices-2017.pdf>
[219] Murphy, *supra* n.217

scrapped by the PIR.[220] Concerns about abusive applicants attempting to effectively 'censor' parts of the internet were raised,[221] mirroring the criticism of the UDRP for facilitating RDNH. Nevertheless, this author posits that an internationally recognised alternative dispute resolution mechanism would be the most effective and expedient method of tackling online IPR breaches. It is proposed that the UDRP, as an established IPR arbitration system, is used as inspiration for a new internationally recognised policy.

6.2.1 Arbitration and Jurisdiction

The UDRP has been described as a model for "resolving complex jurisdictional issues"[222] and addressing "disputes that cross national borders"[223]. The infrastructure of the UDRP bares resemblance to national legal systems, but crucially, its substantive provisions do not rely on any regime.[224] Fervent supporters of international arbitration see it as a dispute resolution system autonomous from national legal systems; describing arbitration as being "anational" and "delocalised".[225] In effect, the detachment from national law resurrects the spirit of *lex mercatoria* as an overriding stateless and customary law.[226] Upon appealing to the courts, jurisdiction issues can persist,[227] but internationally recognised guidelines exist to aid the recognition of foreign arbitral awards.[228] By forming jurisdiction on the consent of the parties, problems with jurisdiction are limited to creating workable 'choice of law' clauses.[229]

6.2.2 Choice of Law

---

[220] Kevin Murphy, 'PIR slams brakes on "UDRP for copyright"' (2017) < http://domainincite.com/21564-pir-slams-brakes-on-udrp-for-copyright>
[221] See, for example; J. Malcom & M. Stoltz, 'Healthy Domains Initiative Isn't Healthy for the Internet' (EFF, 2017) < https://www.eff.org/deeplinks/2017/02/healthy-domains-initiative-censorship-through-shadow-regulation>
[222] BNA, 'Subcommittee Tackles Jurisdiction Issues on Internet' (2000) 60 PTC J 214, 215
[223] Helfer, *supra* n.214
[224] Laurence Helfer et al., 'Designing Non-National Systems: The Case of the Uniform Domain Name Dispute Resolution Policy' (2001) 43 W&M LR 141, 149
[225] Roy Goode, 'The Role of the *Lex Loci Arbitri* in International Commercial Arbitration' (2001) 17 Arb. Int'l. 19, 21
[226] ibid.
[227] ibid., 22
[228] E.g. Convention on the Recognition and Enforcement of Foreign Arbitral Awards (1958)
[229] See, for example, Daniel Chow, 'The Costly Problem of Poorly Drafted Choice of Law Clauses' (2017) <https://ssrn.com/abstract=3038827>

The UDRP represents a more liberal approach to 'choice of law'. Rule 15(a) of the UDRP stipulates that decisions should be made "in accordance with the Policy, these Rules and *any rules and principles of law that it deems applicable*" (emphasis added). Therefore, the arbitration panel may choose which legal authority it wishes to apply to the dispute.[230] The panel's choice is straightforward with regards to domestic disputes,[231] although problems do arise with the inevitable use of precedent within the UDRP; for example, where the precedent of a domestic dispute using *State X* law is applied to a separate domestic dispute which should clearly be using *State Y* law.[232] Cross-jurisdictional disputes present a greater problem, exacerbated by the lack of guidance from the UDRP.[233] Consulting all legal jurisdictions in interpreting a point of law is a non-starter,[234] therefore, in practice, panellists must apply a "common sense interpretation suitable for the Internet"[235]. As seen in the *tourplan.com* dispute, despite the freedom afforded by the UDRP, the American panel was predominantly influenced by its own background in US law.[236] The lack of strong guidance regarding choice of law in the UDRP makes this area ripe for disputation. Nevertheless, its flexibility has allowed issues of jurisdiction to be tackled in a more pluralistic and cosmopolitan manner, befitting of the Internet.[237]

Note, for example, the stark contrast between the treatment of TLDs in Google's position in *Equustek*, and that of a UDRP panellist in the *sesamesnaps.com* dispute. In *sesamesnaps.com*,[238] a Polish exporter to Canada, who held a Canadian trade mark for 'sesame snaps', prevailed over an American respondent who owned the .com domain, even though 'sesame snaps' *per se* had been denied trade mark registration in the US.[239] It was stated that it is "permissible for panels to ignore gTLDs where they serve no

---

[230] Berkman Center for Internet & Society, 'Using ICANN's UDRP: Analysis' (at 'Choice of Law') <https://cyber.harvard.edu/udrp/analysis.html#choice>
[231] ibid.
[232] ibid.
[233] ibid.
[234] ibid.
[235] ibid.
[236] ibid.
[237] Paul Berman, 'Towards a Cosmopolitan Vision of Conflict of Laws: Redefining Governmental Interests in a Global Era' (2005) 153 UPLR 1819
[238] *Agros Trading Confectionary Spolka Akcyjna v David Michaels* WIPO Case No. D2016-1827 (2016)
[239] ibid.

purpose other than the technical one".[240] A crucial difference, however, is that *Equustek* also involved ccTLDs. A ccTLD nevertheless "gives rise to a global presence"[241] and therefore enables the offering of goods to a global audience; a 'closed domain' approach to a ccTLD dispute enhances the possibility of foreign-trade mark cybersquatting.[242] Additionally, under the UDRP, a single complaint may consist of consolidated claims against ccTLDs and gTLDs, suggesting that there is little credence given to the territoriality of the trade mark rights in question.[243] Further, ccTLDs such as .co (Colombia) and .tv (Tuvalu), have frequently been used for commercial purposes given their attractiveness;[244] enforcing only trade mark rights granted in Colombia and Tuvalu respectively would open a significant loophole for cybersquatters to exploit. Lastly, a WIPO overview of the UDRP states that the registration of a domain name before the acquiring of trade mark rights by the complainant "does not by itself preclude … a panel's finding of identity or confusing similarity".[245]

6.3 Establishing the Policy

As a body created outside the scope of national authorities, the UDRP was inherently vulnerable.[246] Garnering legitimacy was a critical notion to consider during the establishment of the UDRP.[247] Traditionally, 'deliberative construction'[248] is the predominant methodology for creating international dispute resolution systems: it involves comprehensive negotiations between a multitude of possible stakeholders to flesh out 'checking mechanisms'[249] in addition to the substantive and procedural provisions.[250] Deliberative construction is rightly seen as the most successful way of developing legitimacy in a non-national adjudicative body.[251]

---

[240] ibid.
[241] WIPO, 'ccTLD Best Pracitices for the Prevention and Resolution of Intellectual Property Disputes' (2001) <http://www.wipo.int/amc/en/domains/bestpractices/bestpractices.html>
[242] ibid.
[243] WIPO, 'Domain Name Dispute Resolution Service for Country Code Top Level Domains (ccTLDs)' <http://www.wipo.int/amc/en/domains/cctld/>
[244] Doug Isenberg, 'Popular ccTLDs for Domain Name Disputes' (2017) <https://giga.law/blog/2017/10/18/popular-cctlds-disputes>
[245] WIPO, 'WIPO Jurisprudential Overview 3.0' (2017) <http://www.wipo.int/amc/en/domains/search/overview3.0/#item11>
[246] Helfer, *supra* n.224, 244
[247] ibid.
[248] ibid., 145
[249] ibid., 146
[250] ibid., 145
[251] ibid., 146

However, the UDRP was created on an accelerated timescale,[252] befitting of the technological advancement under ICANN's oversight, but not to the liking of many critics. Attacks against the ICANN's competence highlighted the lack of accountability for the interim Board in charge at the time of the UDRP's construction,[253] a lack of time for 'reflection and comment' for stakeholders,[254] and a noticeable lack of participation from groups with freedom of expression interests.[255] Given the pushback against proposed arbitrary bodies in the field of piracy,[256] this author suggests a deliberative methodology should be followed, fully utilising ICANN's large stakeholder portfolio and, optimally, cooperation from the World Trade Organisation (WTO). Crucially, the WTO has established universal minimum standards of IPR protection through the TRIPs[257] agreement, which is applicable to every WTO member.[258] These internationally recognised standards were created due to the importance of achieving a consensus amongst multinational corporations and their governments.[259] Increased global data liquidity, and the back-and-forth between Canadian and American courts over the *Equustek* injunction, has shown that this consensus must be invoked once more.

6.4 Disincentivising Abusive Complaints

The rights to access information and freedom of expression are nobly defended and should not be disregarded even in the face of IPR infringement. However, 'straightforward' cases of IPR infringement do not represent threats to freedom of speech.[260] Any public-facing rhetoric should underline the prospective arbitrary body as a tool to preserve freedom of expression on the Internet: it is a measure to hinder those sovereign nations with extensive domestic censorship regimes from making jurisdictional power-grabs.

---

[252] ibid., 178
[253] ibid., 180
[254] ibid., 181
[255] ibid.
[256] See, *supra*, discussion on CADRP [7.2]
[257] The Agreement on Trade-Related Aspects of Intellectual Property Rights (1995)
[258] J.H. Reichmann, 'Universal Minimum Standards of Intellectual Property Protection under the TRIPS Component of the WTO Agreement' (1995) <https://scholarship.law.duke.edu/cgi/viewcontent.cgi?referer=https://www.google.co.uk/&httpsredir=1&article=1617&context=faculty_scholarship>
[259] Duncan Matthews, *Globalising Intellectual Property Rights: The TRIPs Agreement* (Routledge 2002), 3-4
[260] *Google v Equustek*, *supra* n.61 [48]

Under the UDRP, RDNH is deterred by provisions which enable panellists to 'announce' an attempt to exploit the policy.[261] There is a lack of genuine measures to counter bad faith complaints, with virtually no power of punishment.[262] Instead, a strict adherence to the UDRP theoretically denies any facilitation of RDNH. For any IPR dispute resolution policy, there must exist strict guidelines on the prevention and punishment of abusive complaints. The fears of over-enforcement by bodies such as the MPAA are analogous to RDNH, in this regard the UDRP should not be used as an inspiration.

7. Conclusion

With current technology, the need for an effective, balanced and jurisdiction-neutral means of combating piracy and counterfeiting is strong. A dispute resolution policy can effectively balance the need to properly enforce IPRs with the need to curtail jurisdictional overreach. This is achieved by using the DNS, which is the most effective form of IPR enforcement on the Internet, and taking adjudication out of the domestic courts' hands, using a globally recognised standard for IPR protection. To a certain extent, this balancing act mirrors a consolidation of separatist and realist approaches to Internet jurisdiction. The establishment of such a dispute resolution system would need the cooperation between an internationally recognised body involved with IPR protection (WTO), and a body with a far-reaching technical mandate (ICANN).

[261] David Sorkin, 'Judicial Review of ICANN Domain Name Dispute Decisions' (2002) 18 SCHTLJ 35, 41
[262] ibid.

Bibliography

Case Law

Agros Trading Confectionary Spolka Akcyjna v David Michaels WIPO Case No. D2016-1827 (2016)

Babanaft International Co. SA v Bassante [1989] 1 All ER 433

Cartier International AG v Nominet UK (2013) Claim HC13 B04781

Equustek Solutions Inc. v Jack, 2014 BCSC 1063

Equustek Solutions Inc. v Jack (2018) BCSC 610

Fiber-Shield Industries, Inc. v Fiber Shield LTD, NAF No. FA92054 (2000)

Gloria v. Casa Editorial El Tiempo Colombian Constitutional Court, judgment of 12 May 2015, No. T277

Google Inc. v Equustek Solutions Inc., 2017 SCC 34 [2017] 1 S.C.R 824

Google Inc. v. Mr. M 12th Civil Division of the Tokyo High Court, judgment of 12 July 2016, No. 192

Google Spain SL, Google Inc. v Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez (C-131/12)

L'Oreal v eBay (C-324/09)

Louis Feraud Int'l SARL v Viewfinder Inc. (SDNY 2005) 406 F Supp 2nd 274

Louis Vuitton Malletier, S.A. v Akanoc Solutions, Inc. (2001) 658 F.3d 9th. Circuit

Macquarie Bank Limited & Anor v Berg [1999] NSWSC 526

Niemela v Malamas [2015] BCSC 1024

Religious Tech. v Netcom On-Line (1995) 907 F. Supp. 1361

Universal Music v Key-Systems GmbH [2014] Regional Court Saarbrücken

Books

Currie, J., *Public International Law* (Irwin 2001)

Matthews, D., *Globalising Intellectual Property Rights: The TRIPs Agreement* (Routledge 2002

Mueller, M., *Networks and States: The Global Politics of Internet Governance* (MIT Press, 2010)

Musiani F., et al., *The Turn to Infrastructure in Internet Governance* (Springer 2016)

Ryngaert, C., *Jurisdiction in International Law* (Oxford University Press, 2008)
Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn CUP 2017)

Svantesson, D., *Solving the Internet Jurisdiction Puzzle* (2017)

Journals

Akehurst, M., 'Equity and General Principles of Law' (1976) 25(4) ICLQ 801

Bar-Ziv S., et al., 'Behind the Scenes of Online Copyright Enforcement: Empirical Evidence on Notice & Takedown' (2017) 50 CLR

Benko, B., 'Russia and Allofmp3.com: Why The WTO And WIPO Must Create a New System for Resolving Copyright Disputes in the Digital Age' (2016) 1 AIPJ 299

Berman, P., 'Towards a Cosmopolitan Vision of Conflict of Laws: Redefining Governmental Interests in a Global Era' (2005) 153 UPLR 1819

BNA, 'Subcommittee Tackles Jurisdiction Issues on Internet' (2000) 60 PTC J 214

Bower, M., 'Cyberspace, The Final Frontier: Examining the International Trade Commission's Jurisdiction Over Digital Information' (2018) 27 FCBJ 213

Bradshaw, S., 'The politicization of the Internet's Domain Name System: Implications for Internet security, universality, and freedom' (2018) 20 NM&S 332

Bridy, A., 'Notice and Takedown in the Domain Name System: ICANN's Ambivalent Drift into Online Content Regulation' (2017) 74 W&L L Rev 1345

Cohen-Almagor, R., 'Freedom of Expression, Internet Responsibility, and Business Ethics: The Yahoo! Saga and Its Implications' (2012) 106 J Bus Ethics 353

Corn, G., & Taylor, R., 'Sovereignty in the Age of Cyber' (2017) AJIL 111

Dieguez, J., 'The UDRP reviewed: the need for a "uniform" policy' (2008) CTLR 133

Douglas, M., 'A Global Injunction Against Google' (2018) LQR 183

Etteldorf, C., 'Canadian Supreme Court on Google: Effective Legal Protection Tops Jurisdictional Boundaries' (2017) 3 EDPLR 384

Goode, R., 'The Role of the *Lex Loci Arbitri* in International Commercial Arbitration' (2001) 17 Arb. Int'l. 19

Helfer, L., et al., 'Designing Non-National Systems: The Case of the Uniform Domain Name Dispute Resolution Policy' (2001) 43 W&M LR 141

Helfer, L, 'International Dispute Settlement at the Trademark-Domain Name Interface' (2001) Int'l. L WWS 87

Hildebrandt, M., 'Extraterritorial Jurisdiction to Enforce in Cyberspace? Bodin, Schmitt, Grotius in Cyberspace' (2013) 63 U TLJ 196

Kowalik-Banczyk, K., 'Migration of European Judicial Ideas concerning Jurisdiction over Google on Withdrawal of Information' (2016) 17 German L.J. 315

Larson, W., 'Internet Service Provider Liability: Imposing a Higher Duty of Care' (2014) 37 CJL&A 573

Lemley, M., et al., 'Don't Break the Internet' (2011) 64 Stan. LR 34

Lemley, M., & Reese, R., 'A Quick and Inexpensive System for Resolving Peer-to-Peer Copyright Disputes' (2005) 23 Card. A&ELJ 1

Menthe, D., 'Jurisdiction in Cyberspace: A Theory of International Spaces' (1998) 5 MTTLR 69

Mueller, M., et al., 'Governing Internet Territory: ICANN, Sovereignty Claims, Property Rights, and Country Code Top-Level Domains' (2017) 18 Colum. S&TLR 435

Mueller, M., 'Success By Default: A New Profile of Domain Name Trademark Disputes Under ICANN's UDRP' (2002) Syr.Uni. 15

Papacharissi, Z., 'The virtual sphere' (2002) 4 NM&S 9

Perloff-Giles, A., 'Transnational Cyber Offences: Overcoming Jurisdictional Challenges' (2018) 43 YJIL 191

Reidenberg, J., 'Technology and Internet Jurisdiction' (2005) 153 U.PennLR 1951

Reidenberg, J., 'Yahoo and Democracy on the Internet' (2001) 42 Jurimetrics 261

Schultz, T., 'Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface' (2008) 19 EJIL 799

Seng, D., 'The State of the Discordant Union: An Empirical Analysis of DMCA Takedown Notices' (2014) 18 Uni. Virginia 370

Slaughter, A., 'Judicial Globalization' (2000) 40 VJIL 1103

Sorkin, D., 'Judicial Review of ICANN Domain Name Dispute Decisions' (2002) 18 SCHTLJ 35

Stoyan, S., 'Just a click away? Jurisdiction and virtually carrying on business in Canada' (2017) J. Private Intl. L. 602

Straumann, B., 'Early Modern Sovereignty and Its Limits' (2015) 16 TIL 423

Svantesson, D., 'Lagom Jurisdiction – What Viking Drinking Etiquette Can Teach Us About Internet Jurisdiction and Google France' (2018) 12 Mas. UJL&T 29

Thornburg, E., 'Fast, Cheap, and Out of Control: Lessons from the ICANN Dispute Resolution Process' (2002) 7 J S&EBL 191

Tramwell, A., 'Personal Jurisdiction and the "Interwebs"' (2015) 100 Cornell L. Rev. 1129

Other Sources

Ahrens, J., 'Stop Censorship: The Problems With SOPA' (2011) CIS <http://cyberlaw.stanford.edu/blog/2011/11/stop-censorship-problems-sopa>

Alves, S., 'Internet Governance 2.0.1.4: The Internet Balkanization Fragmentation' (2014) <https://ssrn.com/abstract=2466222>

Arnold, B., 'Equustek Again: BC Supreme Court Upholds Worldwide Injunction Despite US Refusal To Enforce' (2018) < https://gowlingwlg.com/en/insights-resources/articles/2018/equustek-again-bc-supreme-court-upholds-injuction/#_ftn8>

Barlow, J., 'A Declaration of the Independence of Cyberspace' (1996) EFF <https://www.eff.org/cyberspace-independence>

Berkman Center for Internet & Society, 'Using ICANN's UDRP: Analysis' (at 'Choice of Law') <https://cyber.harvard.edu/udrp/analysis.html#choice>

Bridy, A., 'A Response to Paul Vixie's "Notice, Takedown, Borders and Scale"' (2017) <http://cyberlaw.stanford.edu/blog/2017/03/response-paul-vixie%E2%80%99s-notice-takedown-borders-and-scale%E2%80%9D>

Brown-Okruhlik, S., 'The New Frontier of Jurisdiction: Supreme Court of Canada Upholds Worldwide Injunction Against Google' (2017) McMillan <https://mcmillan.ca/Files/199962_The-New-Frontier-of-Jurisdiction.pdf>

CDT 'The Perils of Using the Domain Name System to Address Unlawful Internet Content' (September 2011) <https://www.cdt.org/files/pdfs/Perils-DNS-blocking.pdf>

Chow, D., 8'The Costly Problem of Poorly Drafted Choice of Law Clauses' (2017) <https://ssrn.com/abstract=3038827>

Christie, A., 'The ICANN Domain Name Dispute Resolution System as a Model for Resolving other Intellectual Property Dispute on the Internet' (2002)

Crocker, S., et al., 'Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill' (May 2011) 5

DeNardis, L., 'One Internet: An Evidentiary Basis for Policy Making on Internet Universality and Fragmentation' (2016) CIGI Paper Series No. 38

EFF, 'Shadow Regulation' <https://www.eff.org/issues/shadow-regulation>

Fleischer, P., 'Implementing a European, Not Global, Right to be Forgotten', Google Europe Blog (30 July 2015)

Getman-Pavlova, I., 'The concept of "comity" in Ulrich Huber's conflict doctrine' (2012) National Research University <https://f-origin.hypotheses.org/wp-content/blogs.dir/818/files/2013/04/The-concept-of-%E2%80%9Ccomity%E2%80%9D-in-Ulrich-Huber%E2%80%99s-conflict-doctrine.pdf>

ICANN, 'Beginner's Guide to Participating in ICANN' (2013) <https://www.icann.org/en/system/files/files/participating-08nov13-en.pdf>

ICANN, 'IANA Functions: The Basics' <https://www.icann.org/en/system/files/files/functions-basics-07apr14-en.pdf>

ICANN, 'ICANN Doesn't Take Down Websites' (2010) <https://www.icann.org/news/blog/icann-doesn-t-take-down-websites>

ICANN, 'Rules for Uniform Domain Name Dispute Resolution Policy' (2013)

ICANN, 'There are not 13 root servers' (2007) <https://www.icann.org/news/blog/there-are-not-13-root-servers>

ICANN, 'Uniform Domain Name Dispute Resolution Policy', Section 4(a) <https://www.icann.org/resources/pages/policy-2012-02-25-en>

ICANN, 'What Does ICANN Do?' <https://www.icann.org/resources/pages/what-2012-02-25-en>

Isenberg, D., 'Popular ccTLDs for Domain Name Disputes' (2017) <https://giga.law/blog/2017/10/18/popular-cctlds-disputes>

Koekkoek, M., et al., 'Internet and Jurisdiction After Google Spain: The Extra-territorial Reach of the EU's "Right to be Forgotten"' (2015) KU Leuven Working Paper 152

Kulesza, J., 'Internet Governance and the Jurisdiction of States: Justification of the Need for an International Regulation of Cyberpaces' (2008) GigaNet, Annual Symposium 2008

MacDonald, R., 'The Google Inc. v. Equustek Solutions Inc. Decision' (2017) < https://gowlingwlg.com/en/insights-resources/articles/2017/google-inc-v-equustek-solutions-inc-decision/>

Malcom, J., & Stoltz, M., 'Healthy Domains Initiative Isn't Healthy for the Internet' (EFF, 2017) < https://www.eff.org/deeplinks/2017/02/healthy-domains-initiative-censorship-through-shadow-regulation>

Masnick, M., 'Why PROTECT IP Breaks The Internet' (2011) Techdirt <https://www.techdirt.com/articles/20110531/13331214491/why-protect-ip-breaks-internet.shtml>

Murphy, H., 'The Role of a Domain Name Registrar as an Internet Intermediary' Tilburg Uni., 15 <http://arno.uvt.nl/show.cgi?fid=141685>

Murphy, K., 'PIR slams brakes on "UDRP for copyright"' (2017) < http://domainincite.com/21564-pir-slams-brakes-on-udrp-for-copyright>

National Commission on Informatics and Liberty, 'CNIL Orders Google to Apply Delisting on All Domain Names of the Search Engine' (12 June 2015) <https://www.cnil.fr/en/cnil-orders-google-apply-delisting-all-domain-names-search-engine>

OECD, 'The Economic and Social Role of Internet Intermediaries' (April 2010)

Pegoraro, R., WikiLeaks sinks, resurfaces (repeat as necessary)' (December 2010) The Washington Post Faster Forward Blog

Phillips, M., 'Obama Administration Responds to We the People Petitions on SOPA and Online Piracy' (January 2012) White House Blog
Reichmann, J., 'Universal Minimum Standards of Intellectual Property Protection under the TRIPS Component of the WTO Agreement' (1995) <https://scholarship.law.duke.edu/cgi/viewcontent.cgi?referer=https://www.google.co.uk/&httpsredir=1&article=1617&context=faculty_scholarship>

Reporters Committee for Freedom of the Press, *Statement on Case C-507/17* (29 Nov 2017) 9 <https://www.rcfp.org/sites/default/files/2017-11-29-Googe-v-CNIL.pdf>

Schwemer, S., 'On Domain Registries and Website Content' (2018) CIR <https://ssrn.com/abstract=3107547>

Testart, C., 'Understanding ICANN's complexity in a growing and changing Internet' (2014

TF, 'WHOIS Limits Under GDPR Will Make Pirates Harder to Catch, Groups Fear' (2018) <https://torrentfreak.com/whois-limits-under-gdpr-will-make-pirates-harder-to-catch-groups-fear-180413/>

Trimble, M., 'Geoblocking and "Legitimate Trade"' (2018) (*Intellectual Property and Obstacles to Legitimate Trade*, Wolters Kluwer, forthcoming 2018)

Tusikov, N., 'Internet Firms as Global Regulators' (2018) GigaNet, Annual Symposium 2017

Paul Vixie, 'Notice, Takedown, Borders and Scale' (2017) <http://www.circleid.com/posts/20170301_notice_takedown_borders_and_scale/#add_comment>

Vixie, P., 'On Mandated Content Blocking in the Domain Name System' (2011) CircleID <http://www.circleid.com/posts/20110318_on_mandated_content_blocking_in_the_domain_name_system/>

Weston, M., 'Google v. Equustek: United States Federal Court Declares Canadian Court Order Unenforceable' (2017) < https://jolt.law.harvard.edu/digest/google-v-equustek-united-states-federal-court-declares-canadian-court-order-unenforceable>

WIPO, 'ccTLD Best Pracitices for the Prevention and Resolution of Intellectual Property Disputes' (2001) <http://www.wipo.int/amc/en/domains/bestpractices/bestpractices.html>

WIPO, 'Domain Name Dispute Resolution Service for Country Code Top Level Domains (ccTLDs)' <http://www.wipo.int/amc/en/domains/cctld/>

WIPO, 'WIPO Jurisprudential Overview 3.0' (2017) <http://www.wipo.int/amc/en/domains/search/overview3.0/#item11>

Xue, H., 'Caveats of Intermediary Liability in Domain Name System' (2014) GigaNet, Annual Symposium 2014

Zittrain, J., 'Be Careful What You Ask For: Reconciling a Global Internet and Local Law' (2003) Berkman Center No. 2003-03