Denning Law Journal 2015 Vol 27 pp 204-240

THE MODEL FOR A PATH FORWARD. A PROPOSAL FOR A MODEL LAW DEALING WITH CYBER-SQUATTING AND OTHER ABUSIVE DOMAIN NAME PRACTICES

James Plotkin[*]

1. INTRODUCTION

The internet is without a doubt the most powerful network ever developed. Its connective capacity and speed are peerless. One of the internet's primary applications is and always has been e-commerce. Given the prevalence of online shopping,[1] strong online presence is a commercial necessity, and the preferred means of identifying a business online is by a domain name containing the business' trademark. A single domain name can only be associated with a single website. Domain names are therefore a scarce resource.

Cyber-squatters exploit this resource by registering domain names that are either identical or confusingly similar to well-known trademarks. They then attempt to sell the domain name(s) to the legitimate trademark holder for a profit.

Little is written today about domain name dispute resolution and cyber-squatting. The majority of the literature on the subject was published between 2000 and 2003. This is surprising given the fact that the incidence of cyber-squatting has not abated since the internet's early days and has in fact been on the rise for the past nine years.[2]

[*] James Plotkin, LLB, JD jamesplotkin@gmail.com

[1] In 2010, Canadians placed nearly 114 million orders while shopping online, averaging about 10 orders per person. Orders totalled $15.3 billion, with an average value of $1,362 per person per year. See: 'Online Shopping' (*Statistics Canada*, 20 December 2012) <http://www.statcan.gc.ca/pub/11-402-x/2012000/chap/retail-detail/retail-detail01-eng.htm> accessed 5 October 2014.

[2] The World Intellectual Property Organization (WIPO) has received increasing numbers of complaints since 2005. See: 'WIPO UDRP Domain Name Decisions (gTLD)' (*World Intellectual Property Organization – Arbitration and Mediation Center*) <http://www.wipo.int/amc/en/domains/decisionsx/> accessed 2 October 2014.

The current legal framework surrounding domain names comports two major components: 1) national trademark laws; and 2) the Internet Corporation for Assigned Names and Numbers (ICANN) Uniform Dispute Resolution Policy (UDRP).[3] The United States is the only jurisdiction to enact a purpose-built piece of legislation aimed at abusive domain name registration practices. That law is called the *Anticybersquatting Consumer Protection Act* (ACPA).[4]

Given that cyber-squatting is as prevalent as ever, the current regulatory regime is clearly inadequate to deal with this issue. Both the UDRP and ACPA suffer from significant shortcomings. The proposed solution represents a major change to the current cyber-squatting framework □ a model law dealing with cyber-squatting and other abusive domain name practices. This purpose-built piece of model legislation would create causes of action for cyber-squatting and what is known as reverse-domain name hijacking, the practice of instituting false cyber-squatting claims to have a domain name transferred from a registrant.[5]

First, this paper briefly describes the Domain Name System (DNS), defines cybersquatting, and presents data demonstrating a need for further regulation. Next the paper examines the existing legal regime, namely the UDRP and the ACPA.[6] While both of these instruments are useful, they suffer from certain legal (and, in the case of the UDRP, empirical) shortcomings. Finally, this paper makes the case for a model law dealing with cyber-squatting and other abusive domain name practices and elaborates on several key provisions of the proposed model law.[7]

[3] 'Uniform Domain Name Dispute Resolution Policy' (*Internet Corporation for Assigned Names and Numbers,* 24 October 1999) <https://www.icann.org/resources/pages/policy-2012-02-25-en> accessed 29 September 2014. Note that certain country-code top level domain registries have established their own dispute resolution policies. These policies generally strongly resemble the UDRP. One such example is the Canadian Internet Registration Authority (CIRA): Canadian Dispute Resolution Policy (CDRP).

[4] 15 USC s1125(d) and 15 USC s1114(2)(D)(v).

[5] *Sallen v Corinthians Licenciamentos* [2001] 273 F3d.

[6] While it is beyond the scope of this paper to examine a large number of national trademark laws, Part 4 below briefly explains why domain names do not fit neatly into the trademark context.

[7] The Author recognizes that ICANN's recent initiative allowing private entities to register their own 'Generic Top-Level Domains (gTLDs) is perhaps a more current issue. It falls outside the scope of this paper and has therefore intentionally been excluded. This is because the process for registering these gTLDs is different from that relating to domain names; so too is the dispute resolution framework. ICANN has established a sunrise period for each new

This Edition of the Denning Law Journal has running through it a common thread: Magna Carta. While the proposals set out in this writing fall well short of anything resembling a “Great Charter of the Internet”, it does touch on some of the subject matter such a document would cover, namely property rights and access to swift justice. In that regard, it is fitting that this paper be included in an edition celebrating the 800th anniversary of Magna Carta, for had such a document been written today, it is not unreasonable to think that domain names, as digital property rights, may have garnered the Barons’ attention.

2. THE DNS AND CYBER-SQUATTING PRIMER

Before delving into the current cyber-squatting legal framework, and potential regulatory innovations, it is useful to first briefly define exactly what cyber-squatting is and introduce the Domain Name System (DNS), the vehicle with which cyber-squatters ply their trade. This section also presents data demonstrating that cyber-squatting is still a problem in need of regulation.

a. The DNS

At its core, the internet, like all networks, is little more than a web of connections (albeit a particularly vast and complex one). In the same way that the postal system relies on physical addresses to identify the source and destination of mail, the internet relies upon “internet protocol (IP) addresses” to identify computer systems allowing information to be transferred between them.[8]

IP addresses consist of sets of numbers which themselves break down into binary bits.[9] Early developers of the internet rightly thought that this system would be cumbersome as it is difficult for individuals to remember long sets of integers. The DNS was created to address this problem. A domain name is composed of a hierarchical set of “labels” separated by

gTLD registration allowing trademark holders to submit claims for domains in the new TLD. In contrast, the present paper offers a new model for *ex post* dispute resolution.

[8] David Lindsay, *International Domain Name Law: ICANN and the UDRP* (1st edn, Hart Publishing 2007) 3.

[9] John Postel and A Cooper, ‘The US Domain (RFC 1480)’ (*USC/Information Sciences Institute*, June 1993) <http://tools.ietf.org/html/rfc1480> accessed 2 October 2014.

periods (.).[10] Each domain name consists of a "top-level domain" (TLD) and a "second-level domain". [11]

TLDs are contained in all web addresses and occupy the right-most portion of a domain name. There are several categories of TLDs. Among the most notable ones are "generic top-level domains" (gTLDs) - such as ".com", ".net" and ".edu"- and "country-code top level domains" (ccTLDs) –like ".ca", ".us" and ".eu". Each must be administered by a registry responsible for registering the second-level domains under the TLD.[12]

To the left of the TLD in the domain name lays the second-level domain. This is the part of the domain name that bears the greatest significance to internet users as they are unique and identify a defined address space on the web. It is also the part of the domain name that is susceptible to cyber-squatting and is thus the subject of the present inquiry.[13]

b. Cyber-squatting

Cyber-squatting has come to connote several different activities. "Classic cyber-squatting" could be defined as the act of registering domain names that are either identical or confusingly similar to trademarks, and then attempting to sell the domain name(s) to the legitimate trademark holder for a profit. The U.S. Court of Appeal for the 9th Circuit offered the following definition:

> "Cybersquatting is the internet version of a land grab. Cybersquatters register well-known brand names as internet domain names in order to force the rightful owner of the marks to

[10] Paul Mockapetris, 'Domain Names – Implementation and Specification (RFC 1035)' (*USC/Information Sciences Institute*, 1987) <http://tools.ietf.org/html/rfc1035> accessed 2 October 2014.

[11] Domain names may contain further sub-levels (third level domain, fourth level domain etc.), but for the purposes of this writing, only TLDs and second level domains are relevant.

[12] For example, Verisign Inc is the registry responsible for the '.com' and '.net' gTLDs. The Canadian Internet Registration Authority (CIRA) is responsible for administering the '.ca' ccTLD.

[13] From this point forward, the term domain name will reference second-level domains.

> pay for the right to engage in electronic commerce under their own name."[14]

A related activity known as "typo-squatting" consists of registering a domain name that is nearly identical to an existing website, save that it contains a typo that people commonly make when trying to access that site.[15] This is done to divert traffic from the intended website to the "typo site" for the purposes of generating advertising revenue or gaining exposure for the website's content. Panels constituted under the UDRP have found that the Policy captures typo-squatting.[16] Typo-squatting has also been captured by the ACPA (see Section 3C below).[17]

"Domaining" is another deceitful practice by which the alleged cyber-squatter registers a domain name (usually containing a trademark) that he or she believes will see a high volume of traffic with the goal of generating advertising revenue.[18] Here the cyber-squatter never actually tries to sell the domain name, though he or she is profiting from it all the same.

Cybersquatting is an international problem and has been since the early days of the internet. The World Intellectual Property Organization (WIPO) Arbitration and Mediation Center is the world's busiest domain name dispute resolution provider. Since 2000, it has handled between 1700-2600 disputes annually with a marked uptake in complaints since 2005.[19] In 2013 alone, WIPO administered over 2000 domain name disputes.[20]

[14] *Interstellar Starship Services, Ltd v Epix, Inc*, [2002] 304 F 3d 936, 946. See also *Harrods Ltd v Sixty Internet Domain Names* [2002] 302 F3d 214, 219-20, 238.

[15] For example, instead of 'YouTube', one may erroneously enter 'YouTubr' into the address bar of a web browser (the 'r' key is directly adjacent to the 'e' key on a standard computer keyboard). See Christopher Clark, 'The Truth in Domain Names Act of 2003 and a Preventative Measure to Combat Typosquatting' [2004] 89-6 Cornell L Rev 1476, 1480.

[16] See for example: *Dell Computer Corporation v Clinical Evaluations* [2002] No D2002-0423; *Expedia, Inc v Alvaro Collazo* [2003] No D2003-0716*;* and *Marriott International, Inc v Seocho* [2003] NAF Decision No FA149187.

[17] *Shields v Zuccarini* [2001] 254 F 3d 476, 483.

[18] See for example *Teva Pharmaceutical Industries Ltd v Apex Domain Pty Ltd* [2014] No DAU2014-0001.

[19] 'WIPO UDRP Domain Name Decisions (gTLD)' (*World Intellectual Property Organization – Arbitration and Mediation Center*) <http://www.wipo.int/amc/en/domains/decisionsx/> accessed 12 October 2014.

[20] Ibid.

The vast majority of disputes involve only a single domain name, though there is no limit to the number of domain names that may be the subject of a single UDRP proceeding.[21] For example, in *Hermes International v. Brian E. Nielson*[22], the sole panellist granted the transfer of 184 domain names to the Complainant. Multiple domain names have also been adjudicated in the same action under the ACPA.[23]

Despite the fact that there are legal implements in place giving trademark holders the tools to combat cyber-squatting, the issue is still pervasive. The current regulatory framework surrounding domain names therefore merits closer inspection to determine if and where it comes up short.

3. THE CURRENT SYSTEM – THE ICANN UDRP AND THE ACPA

Domain names are currently regulated by means of a few (sometimes conflicting) legal regimes. Operating on a transnational level, the ICANN UDRP is the most important piece of the domain name regulation. This is because every ICANN accredited domain name registrar has incorporated the UDRP into the terms of its domain name registration agreements. This means that virtually every domain name registrant has agreed to be bound by the UDRP.

The ACPA is the only purpose-built piece of national cyber-squatting legislation enacted as of this writing. Its broad scope of application, which as demonstrated below stretches far beyond the U.S., is relevant to any discussion on global domain name policy. This is particularly true here given that this paper advocates a model law approach. The opportunity to examine a piece of national legislation with a fifteen-year history is essential to plotting a path forward.

Finally, domain names have received some protection via national trademark laws. As discussed more fully in Part 4 below, trademark law is ill-equipped to deal decisively with cyber-squatting because domain names are conceptually different from (though related to) trademarks rendering the application of certain key trademark law concepts difficult.

[21] Jean-Francois Poussard, ‘Keep Alert White Paper: Domain Name Cybersquatting in 2013’ (*Keep Alert*, May 2014) <http://sys.to/cyb13en> accessed 10 October 2014.

[22] [2013] No D2013-1407.

[23] *Harrods* (n 14).

a. The UDRP

In December of 1999, ICANN set afoot its UDRP in an effort to combat cyber-squatting. The UDRP was intended to provide a streamlined arbitration-style procedure by which a complainant, upon meeting the criteria set out in the Policy, could have a domain name containing its trademark transferred or cancelled.

To be successful in a UDRP complaint, a complainant must show that:

> (i) The impugned domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights;
> (ii) The registrant has no rights or legitimate interests in respect of the domain name; and
> (iii) The registrant registered and is using the domain name in bad faith.[24]
> Section 4(c)(i)-(iii) sets out a non-exhaustive list of affirmative defences to counter a complaint under Section 4(a):
> (i) before any notice to the registrant of the dispute, its use of, or demonstrable preparations to use, the domain name or a name corresponding to the domain name in connection with a bona fide offering of goods or services;
> (ii) the registrant (as an individual, business, or other organization) have been commonly known by the domain name, even if the registrant has acquired no trademark or service mark rights; or
> (iii) the registrant is making a legitimate non-commercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark at issue.

The UDRP was originally intended to deal with “easy cases” of blatantly abusive domain name registrations.[25] Since the UDRP is agreed to by default by every domain name registrant, and given the relatively low cost of proceeding under the Policy as compared with any form of litigation, the UDRP has seen steady, and at times growing, application since its inception.[26]

[24] Uniform Dispute Resolution Policy (UDRP), s 4(a)(i)-(iii).

[25] See Greame B Dinwoodie, ‘(National) Trademark Laws and the (Non-National) Domain Name System’ [2000] 21 U Pa J Int’l Econ L 495, 511; Bernadette Dino, ‘Passive Warehousing Under ICANN’s Uniform Dispute Resolution Policy: A Utilitarian Perspective’ [2002-2003] 10 Comm Law Cons 301, 301-302.

[26] ‘WIPO UDRP Domain Name Decisions (gTLD)’ (n 2).

b. Shortcomings of the UDRP

This subsection examines the shortcomings of the UDRP. These have been divided into "legal shortcomings" and "empirical shortcomings".

c. Legal Shortcomings

The UDRP suffers from a number of legal shortcomings. Some of these, like the fact that the UDRP fails to stipulate an applicable body of law, are general; others are specific to certain countries- for example that the UDRP conflicts with certain consumer protection laws.

- No Set Body of Law

Beyond the requirements to prove a claim and the listed affirmative defences in Section 4, the UDRP does not prescribe any legal rules to be applied by UDRP panels. UDRP Rules 15a states that: "A Panel shall decide a complaint on the basis of the statements and documents submitted and in accordance with the Policy, these Rules and any rules *and principles of law that it deems applicable*."[27] (Emphasis added).

Reference to national laws may be required to establish whether a complainant has a legitimate trademark rights. Section 4(a)(i) of the UDRP says "trademark or service mark in which the complainant has rights". There is no requirement that the trademark be registered which opens the door to allowing complainants to oppose a domain name registration on the basis of a common law trademark. Some countries such as France and China do not have unregistered trademarks.[28] For these reasons, it would be appropriate for a UDRP panel to refer to a given jurisdiction's law.

National laws should not, however, be used as a basis for determining confusion or bad faith. The legal tests associated with confusing use of a trademark or trademark infringement may vary from jurisdiction to jurisdiction. As panels are free to apply whichever legal principles they

[27] 'Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules")' (*Internet Corporation for Assigned Names and Numbers*, 30 October 2009), <https://www.icann.org/resources/pages/rules-be-2012-02-25-en> accessed 2 November 2014.

[28] France is one such example, less an exception for protection of unregistered 'well-known' marks pursuant to art 6*bis* of the *Paris Convention for the Protection of Industrial Property*. See: David I Greenbaum, 'No Registration, No Problem' [2013] 40 World Trademark Magazine 90.

consider appropriate, it is difficult for parties to a UDRP proceeding to know exactly what legal standard they have to meet.

Likewise, the notion of bad faith is not a rigid concept.[29] There is a fair degree of variation in how different UDRP panels have interpreted the bad faith requirement. Some have even transferred domain names that were registered before the UDRP took effect and when there was no attempt to sell the domain name to the complainant.[30]

How does a panel choose to apply one country's laws over another? Should the law be that of the complainant's jurisdiction, respondent's jurisdiction or the law of the dispute panel's seat? At least one author held out hope that UDRP panels could develop a rich corpus of conflict of law rules.[31] This does not seem to have materialized.

- UDRP is not Binding on Courts

Section 4(k) of the UDRP says that: "The mandatory administrative proceeding requirements set forth in Paragraph 4 shall not prevent either you or the complainant from submitting the dispute to a court of competent jurisdiction for independent resolution before such mandatory administrative proceeding is commenced or after such proceeding is concluded." Several U.S. Courts have noted the non-binding nature of UDRP proceedings.[32]

The fact that parties to a UDRP proceeding may commence a court action at any time clearly undermines the value and finality of a UDRP panel decision (and arguably the process as a whole). One of the more attractive features of arbitration generally is that it allows for final resolution of an issue in a forum that is (often) less costly and time consuming than court.[33] This cost efficiency is challenged by the fact that

[29] See generally Emily Houh, 'The Doctrine of Good Faith in Contract Law: A (Nearly) Empty Vessel?' [2005] 1 Utah L Rev 1.

[30] *Hearst Communications Inc and Hearst Magazines Property Inc v David Spencer d/b/a/ Spencer Associates, and Mail.com, Inc,* [2000] NAF Case No. FA0093763.

[31] See Laurence R Helfer, 'Whither the UDRP: Autonomous, Americanized, or Cosmopolitan?' [2004] Cardozo J Int'l & Comp L 493, 504.

[32] *Sallen* (n 5); *Weber-Stephen Products Co. v. Armitage Hardware* [2000] Case No. D2000-0187 and *Building Supply* Inc, [2000] 54 USPQ 2d 1766; *Parisi v Netlearning, Inc,* [2001] 139 F Supp 2d 745.

[33] Thomas J Stipanowich, 'Arbitration: The "New Litigation"' [2010] 1 U Ill L Rev 1, 4.

UDRP panel decisions are not binding. So too is the time efficiency in the event that one of the parties chooses to re-litigate the issue before a court.

- Complainant Driven Selection Process

One of the most biting criticisms of the UDRP is the fact that the complainant driven provider selection process provides a major incentive for dispute resolution providers and panellists to be "complainant friendly."[34] One author noted that there is "statistical evidence that selection of dispute resolution service providers by challengers leads to forum shopping that biases the results."[35] While this is discussed in greater depth in part ii (Empirical Shortcomings) below, consider the following.

WIPO is the largest UDRP dispute resolution provider; NAF is the second largest. In 2000, WIPO and NAF together accounted for about 90% of UDRP disputes decided annually.[36] A third provider, eResolutions (based in Quebec) accounted for about 7% of UDRP disputes. eResolutions ceased offering UDRP arbitration services in 2001.[37] Its President, Professor Karim Benyekhlef, spoke out in a press release in which he condemned the whole UDRP framework as being biased in favour of complainants and blamed WIPO in specific for perpetuating the problem.[38] Whether or not Professor Benyekhlef was correct, eResolutions was the only UDRP provider that demonstrated a more balanced record of decisions.[39]

- Panellists Tend to be Pro-Intellectual Property by Nature

Unlike courts which tend to be made up of judges with various practice or academic backgrounds, the overwhelming majority of UDRP

[34] Laurence R Helfer and Graeme B Dinwoodie, 'Designing Non-National Systems: The Case of the Uniform Domain Name Dispute Resolution Policy' [2001] 43 WM & Mary L Rev 144, 210.

[35] Milton Meuller, 'Rough Justice, An Analysis of ICANN's Uniform Dispute Resolution Policy (v2.1)' <http://www.acm.org/usacm/IG/roughjustice.pdf>, 2.

[36] Ibid.

[37] Kieren McCarthy, 'eResolution Quits Domain Arbitration: Blames WIPO' (*The Register*, 4 December 2001) <http://www.theregister.co.uk/2001/12/04/eresolution_quits_domain_arbitration/> accessed 12 November 2014.

[38] Ibid.

[39] Meuller (n 35) 11.

panellists are practicing or retired intellectual property lawyers. These individuals (understandably) tend to favour strong intellectual property rights enforcement. In any case in which a respondent's defense is not based on intellectual property rights, the argument could be made that the average panellist would be less receptive to that line of argumentation.

One common example is when respondents raise freedom of expression defenses. In 2013, three WIPO UDRP panels assessed complaints in which the respondent mounted a freedom of expression defense.[40] The domain names were transferred in two of those cases. The complaint was denied in the third, but on the grounds that the complainant did not meet the standard set out in Section 4(a) of the UDRP.

Wal-Mart Stores, Inc. v. Walsucks and Walmarket Puerto Rico is a well-known WIPO panel decision dealing with a group of domain names which were variations on the theme "Wal-MartSucks.com".[41] That decision seems to all but ignore the respondent's freedom of expression argument altogether: "For purposes of deciding this proceeding, the Panel need not explore the content of Respondent's website, nor the relevance of the quantum of expression on his website."[42] One would think that in order to determine whether a registrant is making legitimate use of a domain name, it would be germane to in fact view the website's content, especially when a freedom of expression defense has been mounted.

None of this conclusively proves systemic bias or pre-judgment by UDRP panellists. However, some UDRP decisions, like *Wal-Mart*, demonstrate a marked disinclination towards freedom of speech defenses to UDRP complaints.

- Little Protection Against Reverse-Domain Name Hijacking

Rule 15(e) of the UDRP Rules defines reverse-domain name hijacking as "*using the Policy in bad faith to attempt to deprive a registered domain-name holder of a domain name*." As noted, the UDRP was originally conceived to deal with the most blatant and uncontroversial instances of cyber-squatting.[43] ICANN recognized this by adding the

[40] *The Priory in New Zealand of the Most Venerable Order of the Hospital of St John of Jerusalem v 24-7 Ltd / Domains By Proxy, LLC,* [2012] Case No D2012-2301; *Deskan S/A v PRQ Inet KB / Internet.bs Corp. / Fundación Private Whois* [2013] Case No D2013-1112; and *Yellowstone Mountain Club LLC v Offshore Limited D and PCI* [2013] Case No D2013-0097.

[41] [2000] Case No D2000-0477.

[42] Ibid.

[43] Dinwoodie (n 25) 511.

affirmative defences at Section 4(c)(i)-(iii). This has proven to be inadequate in that the UDRP does not provide any meaningful sanctions for frivolous or abusive process as is the case in civil litigation.[44] The low cost of a UDRP proceeding makes it an attractive avenue for a complainant who, despite not having a strong chance of success, is willing to launch a complaint in the hopes that it will go unopposed.

- UDRP Does Not Protect Against "Passive Warehousing"

Passive warehousing refers to the practice of registering potentially sought after domain names without intent to use them or actively market them as would a classic cyber-squatter. Instead, the passive warehouser relies on instances in which a trademark holder seeks to register a domain name, finds out that it is already registered to someone else, and then offers that individual (the warehouser) a sum of money for the domain name.[45]

This activity is objectionable under the spirit of the UDRP and would be captured by a broad definition of cyber-squatting. Since Section 4(a)(ii) requires that a complainant show not only registration, but *use* in bad faith, a passive warehouser should not be caught by the UDRP.[46]

This seems to make a distinction where none should exist. There are perfectly obvious instances of passive-warehousing which by all accounts would be objectionable under the UDRP but for the "use in bad faith" requirement. This wording therefore obfuscates the UDRP's purpose by allowing an entire sub-category of genuine cyber-squatting to go unaddressed.

- UDRP Does Not Protect Personal Names That Are Not Registered as Trademarks

[44] Catherine A Shutz and Courtney A Hofflander, 'Reverse-Domain Name Hijacking and the Uniform Dispute Resolution Policy: Systematic Weaknesses, Strategies for the Respondent, and Proposed Policy Reforms' [2013] Cybaris IP L Rev 218, 233-234.

[45] See Dino (n 25) 301.

[46] This is consistent with the findings of ICANN's second staff report. See 'Second Staff Report on Implementation Documents for the Uniform Dispute Resolution Policy' (Internet Corporation for Assigned Names and Numbers, 25 October 1999) <http://www.icann.org/udrp/udrp-second-staff-report-24oct99.htm> para 4.1(c).

Strictly speaking, the UDRP is only supposed to apply to existing "trademarks of service marks".[47] This excludes personal names of famous individuals who have not obtained trademark rights therein. Despite the fact that the UDRP should properly exclude complaints of this kind, several have been made and some have resulted in the impugned domain name(s) being transferred or cancelled. Both Bruce Springsteen and Julia Roberts were successful in front of WIPO UDRP panels.[48] Sting was less fortunate.[49]

Apart from the unfortunate Section 4(a)(1)'s wording, there is no reason why the definition of cyber-squatting should exclude instances in which alleged cyber-squatter's buy up domain names containing famous individuals' names. These domain names are valuable to (and have been targeted by) cyber-squatters in the same way as those containing well-known trademarks. That said, given that the Policy currently excludes these rights, the fact that UDRP panels have found in favour of complainants in these scenarios is disconcerting.

- Conflict With Consumer Protection Laws

Some authors have voiced concern about potential conflicts between the UDRP and national consumer protection laws.[50] Under both French and German law, it would appear that at least some domain name registrants would be considered consumers under the relevant consumer protection statutes.[51] These laws prohibit clauses in consumer contracts which require mandatory submission to arbitration. In cases where the respondent in a UDRP proceeding fits under the definitions of consumer set out in these laws, the UDRP clauses found in domain name registration agreements would be invalidated.

In Canada, consumer protection laws would not appear to prohibit incorporating the UDRP into domain name registration agreements. The only two provinces whose consumer protection legislation addresses the

[47] UDRP s 4(a)(i).

[48] *Bruce Springsteen v Jeff Burgar and Bruce Springsteen Club* [2000] Case No D2000-1532; and *Julia Fiowna Roberts v Russel Boyd* [2000] Case No D2000-0210.

[49] *Gordon Sumner, p/k/a Sting v Michael Urvan* [2000] Case No D2000-0596.

[50] For an in depth discussion on how the incorporation of the UDRP into internet registrar/registrant contracts may be counter to the consumer protection laws in France and Germany, see: Holger P Hestermeyer, 'The Invalidity of ICANN's UDRP Under National Law' [2002] 3 Minn Intell Prop Rev 1, 32.

[51] Hestermeyer (n 50) 36-37.

binding nature of arbitration agreements in consumer contracts are Quebec and Ontario.[52] The relevant provisions of those laws only prevent the clauses from prohibiting a consumer from suing in court. As discussed above, the UDRP expressly allows for court proceedings concurrent with or consecutive to UDRP proceedings. These provisions therefore should not apply.

- Conflict With Language Laws

The UDRP was only officially drafted in English.[53] To this day, ICANN has not released an official version of the UDRP in any other language.[54] This appears to be a serious oversight on ICANNs part given the international application of the Policy. More than being an inconvenience to non-English speakers, the unilingual nature of the UDRP may in fact invalidate its application in certain countries.

French law and its "legendary contempt" for the use of other languages on its territory require that consumer contracts be in French.[55] Incorporating the UDRP by reference therefore appears to offend that law. German law requires that the contract be in a language understandable to the parties.[56] In a contract between a German registrant and registrar, that language would likely be German. The UDRP clause would therefore fall under those laws as well.

d. Empirical Shortcomings

The UDRP is often criticized as being substantively one-sided. While this may or may not be the case, the fact that it is applied by dispute resolution providers in a one-sided manner is empirically verifiable.[57] In 2000, complainants won 67.5% of WIPO UDRP proceedings and 71.5%

[52] Art 11.1 of the Quebec *Consumer Protection Act*, c P-40.1; and s 6(2) of the Ontario *Consumer Protection Act, 2002*, SO 2002 ch 30 sch A.

[53] Hestermeyer (n 50) 38.

[54] See 'Uniform Domain-Name Dispute-Resolution Policy' (*Internet Corporation for Assigned Names and Numbers*) <https://www.icann.org/resources/pages/udrp-2012-02-25-en> accessed on 13 November 2014. Even though the page linking to the UDRP may be viewed in English, French, Spanish, Arabic, Russian (Cyrillic) and Chinese, as of 13 November 2014, the Policy itself is still only accessible in English.

[55] Hestermeyer (n 50) 42.

[56] Hestermeyer (n 50) 41.

[57] Meuller (n 35) 34.

of NAF proceedings.[58] eResolution decided only 44.5% of disputes in favour of complainants; it filed for bankruptcy in 2001.[59]

Thirteen years later, the numbers are even more skewed in favour of complainants. In 2013 WIPO decided in favour of complainants 91% of the time.[60] NAF edged WIPO out at 92%.[61] The fact that panel decisions are decided overwhelmingly in favour of complainants is not itself sufficient proof of bias, though it does raise questions.

Forum shopping has been labelled as an endemic issue the UDRP's application.[62] While complainant bias is the most obvious factor in selecting a UDRP dispute resolution provider, given that complainant bias is nearly uniform across all providers, it cannot be the sole factor. One exhaustive empirical study of UDRP proceedings conducted in 2005 showed an unequivocal bias by providers towards nationals from their own countries.[63]

The same study found that the panellist selection process itself favours complainants. In the event that the complainant opts for a single panellist (and the respondent does not request a three-member panel), the provider chooses the panellist.[64] When the provider chooses the sole panellist, complainants win 80% of the time whereas in the case of three-member panels –where each party chooses one panellist– complainants only win 63% of the time.[65]

If one is of the opinion that the UDRP itself is skewed towards complainants, this data is not very revelatory. It would simply show that UDRP dispute resolution providers are faithfully applying a complainant-centric Policy. However, if it is in fact true that the UDRP is balanced from a policy perspective, then this data shows conclusively that UDRP dispute resolution providers and panellists are biased towards complainants.

[58] Ibid 11.

[59] Ibid and McCarthy (n 37).

[60] Poussard (n 21) 8.

[61] Ibid 21.

[62] Meuller (n 35) 2.

[63] Jay P Kesan and Andres A Gallo, 'The Market For Private Dispute Resolution Services - An Empirical Re-Assessment Of ICANN-UDRP Performance' 11 Mich. Telecomm Tech L Rev 285, 296.

[64] UDRP Rules, r 6(b).

[65] Kesan (n 63) 300. See also Michael Geist, 'Fair.com? An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP' (2002) 27 Brook J Int'l L 903, 926.

e. The ACPA and its Case Law

The ACPA was enacted by the U.S. Congress in 1999 to explicitly deal with cyber-squatting. The law (an amendment to the Lanham Act) gives trademark holders a new cause of action against cyber-squatters and also allows for a plaintiff to bring an action *in rem* against a domain name itself. The law also comports a provision offering relief for litigants who believe they are the victim of reverse-domain name hijacking.[66]

In determining the optimal path forward, it is relevant to examine the ACPA and some of its case law for at least two reasons: 1) The ACPA is, as of this writing, the only national law in force that directly addresses cyber-squatting; and 2) Given U.S. federal courts' position on jurisdiction over cyber-squatting claims (discussed more fully below), the ACPA has significant extra-territorial effect and relevance.

f. The ACPA

The ACPA is found at 15 U.S.C. §1125(d) and 15 U.S.C §1114(2)(D). The provisions under § 1125(d) create a cause of action for trademark holders against cyber-squatters. §1114(2)(D)(i)-(iv) deal with limiting domain name registrars, registries, or other domain name registration authorities' liability when they comply with court and panel orders. §1114(2)(D)(v) is a novel provision allowing a registrant believing that his or her domain name was transferred by a UDRP panel in error to have a court declare that it is the rightful owner and restore its registration.

- *Bad faith registration of a domain name - §1125(d)(1)(A)*

§1125(d)(1)(A) makes it actionable to register a domain name that is identical or confusingly similar to a trademark with a "bad faith intent to profit from that mark".[67] §1125(d)(1)(B) sets out nine factors to be considered in determining whether the bad faith requirement is met. Some of the factors mirror those found in the UDRP such as "the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person"[68] or "the person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services"[69]. Others are unique to the ACPA.

[66] 15 USC s 1125 (3)(C) for definition of reverse-domain name hijacking.

[67] 15 USC s 1125(d)(1)(A)(i).

[68] Ibid s 1125(d)(1)(B)(i)(II).

[69] Ibid s 1125(d)(1)(B)(i)(III).

Unlike the UDRP, the factors set out in this section are non-exhaustive and need not all be considered in every instance.

One of the main advantages of an action under §1125(d)(1)(A) of the ACPA over a UDRP proceeding is the availability of the full suite of common law and equitable remedies including damages, accounting of profits and injunctions.

- *In rem action against domain name* - §1125(d)(2)(A).

In certain cases, the ACPA also allows a plaintiff to undertake an action *in rem* against the domain name itself.[70] This is permitted when: 1) The plaintiff is unable to obtain *in personam* jurisdiction over the registrant; or 2) The plaintiff, having exercised due diligence, cannot locate the registrant.

The ACPA therefore favours actions *in personam* but allows an individual to sue a domain name directly if necessary. This is in recognition of the fact that people who register domain names that affect the holders of U.S. trademark rights are situated around the world and that registrants often provide false information to domain name registrars during registration.[71] Unlike an action under §1125(d)(1)(A), proceeding under this provision limits the available remedies to the cancellation or transfer of the domain name.

- *Preventing reverse-domain name hijacking - §1114(2)(D)(v)*

Reverse-domain name hijacking occurs when a trademark holder uses the UDRP mechanism to bully a registrant out of a validly registered domain name.[72] §1114(2)(D)(v) addresses this abusive practice by empowering individuals who believe that their domain names should not have been cancelled or transferred to have that domain returned. §1114(2)(D)(v) reads as follows:

[70] 15 USC s 1125(d)(2)(A).

[71] See Kieren McCarthy, '77% of Domain Name Registrations Stuffed with Rubbish' (*The Register,* 17 February 2010) <http://www.theregister.co.uk/2010/02/17/domain_name_problems/> accessed 9 December 2014.

[72] Ryan R Owens, 'Domain-Name Dispute-Resolution after *Sallen v Corinthians Licenciamentos & Barcelona.com, Inc v Excelentisimo Ayuntameiento De* Barcelona' 18:1 Berkeley Tech LJ 257, 262.

> A domain name registrant whose domain name has been suspended, disabled, or transferred under a policy [UDRP] described under clause (ii)(II) may, upon notice to the mark owner, file a civil action to establish that the registration or use of the domain name by such registrant is not unlawful under this chapter. The court may grant injunctive relief to the domain name registrant, including the reactivation of the domain name or transfer of the domain name to the domain name registrant.

The provision gives the court the power to grant injunctive relief requiring the domain name to be returned to its rightful owner. The provision does not, however, expressly give courts permission to award damages.

g. Case law under the ACPA

The following is a brief look as three key decisions under the ACPA. They demonstrate how American courts have given the ACPA a broad reading, extending far beyond the U.S. border.

- *Sallen v Corinthians Licenciamentos*[73]

In 1998, Jay Sallen, a resident of Massachusetts, registered "corinthians.com" with Network Solutions Inc. (NSI). Corinthians Licenciamentos ("Corinthians") was a Brazilian soccer team with trademark rights in the word "corintheoa" (the Portuguese equivalent to Corinthian). Sallen contacted Corinthians offering to sell the domain name to the team. Corinthians responded with a cease and desist letter demanding that he turn the domain name over to it. Sallen did not comply.

In May 2000, Corinthians undertook a UDRP preceding before a WIPO arbitration panel to have the domain name transferred.[74] The panel found that the domain name was confusingly similar to Corinthians' trademark and that Sallen had registered and used it in bad faith. The Panel ordered that the domain name be transferred to Corinthians.

Sallen filed an action under the ACPA in the U.S. District Court for the District of Massachusetts to have the WIPO panel decision reviewed. His action was based on §1114(2)(D)(v) (the provision that addresses the practice of reverse-domain name hijacking).

[73] *Sallen* (n 5).

[74] *Corinthians Licenciamentos LTDA v Sallen* [2000] No D2000-0461.

The District Court refused Sallen's claim on the grounds that no actual controversy existed between the parties at the time the action was brought.[75] On appeal, the US Court of Appeal for the First Circuit found that it had jurisdiction as Sallen's claim was based on a federal statute.

Corinthians argued that the Court lacked subject-matter jurisdiction because the "corintheao" trademark was registered in Brazil, not in the U.S. The Court found this argument unpersuasive. It based its reasoning on the language in §1114(2)(D)(v) which uses the term "mark owner". The *Lanham Act*[76] comports separate definitions for the terms "mark" and "registered trademark". "Mark" is defined broadly and does not that require the trademark be registered in the U.S. In fact, the definition of "mark" (which itself refers to the definition "trademark") does not appear to set any territorial limitations.[77] In other words, the definition applies to trademarks that are used as such anywhere in the world. The Court made reference to the fact that in drafting the ACPA, Congress intended to signal its awareness of the "international nature of trademark disputes".[78]

While the Court actually agreed with the WIPO Panel on the merits, it made a rather grand statement when it said: "A [federal] court's §1114(2)(D)(v) decision that a party is not a cybersquatter under the ACPA, and that a party has a right to use a domain name, necessarily negates a WIPO decision that a party is a cybersquatter under the UDRP."[79] Keep in mind that the trademark at issue was not registered in the U.S. This case stands for the proposition that if a foreign complainant obtains an award from a UDRP panel based on non-U.S. trademark rights, an American court will still assert jurisdiction over a complaint brought under the ACPA. The sole basis for this is that the ACPA is a federal statute enabling parties to bring causes of action relating to domain names, and that Congress' legislative intent was clear.

One author calls *Sallen* a "startling precedent endorsing the view that a federal statute in the U.S. can trump an international convention."[80] This

[75] art III, s 2, Clause 1 of the United States Constitution limits the jurisdiction of U.S. federal courts to actual cases and controversies dealing with (among other things) federal law.

[76] 15 USC s 1051 et seq.

[77] *Sallen* (n 5) 24.

[78] The Court obviously misspoke here and should have at least said 'internet related trademark disputes' or 'cyber-squatting related disputes'.

[79] *Sallen* (n 5) 28.

[80] Aaron J Horowitz, 'U.S. Jurisdictional Monopolization of International Cybersquatting Disputes: A review of Current Inequities and Future Consequences' [2006] 11 J. Tech L & Pol'y 191, 203.

seems to be a slight overreaction in that the UDRP is not an international convention; it is a policy created by a private entity. While it is true that, in effect, the UDRP may have a broader and more pervasive application than many international treaties, it is still incorrect to call it an international legal instrument. While strictly speaking incorrect, the author's point is well taken. The *Corinthians* decision demonstrates at least one U.S. court's disregard for international norms that touch on extra-territorial IP rights.

From a practical perspective, a ruling of this nature under the ACPA will only have effect if the registrar that registered the impugned domain is located either in the U.S. or a jurisdiction in which a U.S. court decision will be recognized and enforced. NSI is a U.S. based registrar. Any order made by a U.S. federal court would therefore be binding upon it. Had the domain name been registered with a Chinese registrar, things may have been different.

- *Harrods Ltd. v Sixty Internet Domain Names*[81]

Harrods UK ("Harrods") operates a high end department store in London, England. Harrods Buenos Aires (HBA) was once a wholly-owned subsidiary of Harrods but had since begun operating independently. HBA registered 60 domain names containing the "Harrods" trademark. Both companies owned registered trademarks in "Harrods" in different countries (Harrods being the owner of the U.S. trademark). After a breakdown in negotiations and an unsuccessful law suit for, among other things, passing-off in England, Harrods filed an action in the Eastern District of Virginia against HBA citing breaches of the ACPA.[82] Unable to show that the Court had personal jurisdiction over HBA, Harrods brought an action *in rem* against the domain names themselves.

The District Court held in favour of Harrods with reference to 54 of the domain names but granted summary judgement in favour of HBA for six. On appeal, the U.S. Court of Appeal for the Fourth Circuit upheld the Trial Judge's ruling as to the 54 domains to be transferred to the Plaintiff but overturned the summary judgement ruling finding that it was inappropriate given the Plaintiff's lack of opportunity to conduct discoveries. Citing the United States Supreme Court, the Fourth Circuit based its decision on an old Common Law doctrine dealing with damage

[81] *Harrods* (n 14).

[82] Note that NSI, the registrar with which the 60 domains were registered was located in Virginia.

caused by an absentee owner's land "suits for injury suffered on the land of an absentee owner, where the defendant's ownership of the property is conceded but the cause of action is otherwise related to rights and duties growing out of that ownership."[83] The Court ruled that HBA was tantamount to an absentee owner of the domain names which were causing the Plaintiff damage.

The *Harrods* Court's reasoning is dubious. The equivocation between a domain name registrant and an absentee land owner is not seamless. For one thing, the decision is unclear as to whether the domain names were actually in use or if they were simply parked. In the second case, the analogy makes a little more sense. However, if the domain names were being used in connection with a *bona fide* offering of goods or services, it is hard to see how the analogy finds application. Another problem with this decision is the assertion that a domain name is situated at the seat of the registrar that registered it. While NSI is located in Virginia, the servers containing the information and files that made up the website were not. If the website is "situated" anywhere, would it not be in the jurisdiction in which those servers are located?

The *Harrods* case further extends the ACPA's reach to allow transfers of domain names in instances where there is legitimate concurrent use of the same trademark by two entities. Unlike *Corinthians*, the Plaintiff in *Harrods* actually did have a U.S. trademark registration. At the same time, while *Corinthians* dealt with a more classic example of cyber-squatting, the Court in *Harrods* transferred the domain names in spite of the fact that HBA had legitimate trademark rights therein, an outcome that should never be reached by a UDRP panel.[84] While not expressly saying so, the Court in this case essentially said that a foreign trademark can "infringe" a U.S. trademark for the purposes of a domain name dispute under the ACPA.

- *NBC Universal, Inc. v NBCUniversal.com*[85]

No decision rendered under the ACPA is as expansionist as the District Court for the Eastern District of Virginia in *NBC Universal*. Junak Kwon registered "NBCUniversal.com" in Korea with a Korean registrar. NBC undertook a WIPO UDRP proceeding in which Kwon failed to appear. Kwon brought an action in a Korean court causing the UDRP

[83] *Harrods* (n 14) 225.

[84] This is likely why Harrods UK never bothered undertaking a UDRP proceeding and instead chose to challenge HBA in the courts of England and then the US.

[85] [2005] 78 F Supp 2d 715, 717-18.

panel to abstain from ordering the transfer of the domain name pending the Korean Court's decision. NBC Universal concurrently started an i*n rem* action under the ACPA. In spite of the fact that the Korean action was already pending, the District Court refused to stay proceedings on the grounds that the action in Korea was *in personam* whereas the action before it was *in rem*. The Court seemingly ignored the fact that despite this legal technicality, the subject-matter of the disputes was identical.

As to jurisdiction, the Court found that because Verisign Inc., the registry that administers the ".com" gTLD registry is located in Virginia, it had jurisdiction over the claim. This reasoning is based on § 1225(d)(2)(A) of the ACPA:

> The owner of a mark may file an in rem civil action against a domain name in the judicial district in which the domain name registrar, <u>domain name registry</u>, or other domain name authority that registered or assigned the domain name is located if—
> (i) the domain name violates any right of the owner of a mark registered in the Patent and Trademark Office, or protected under subsection (a) or (c) of this section; (Emphasis added).

This means that the U.S. District Court for the Eastern District of Virginia has jurisdiction over any ".com", ".net" or ".gov" domain name (it manages the registries for those TLDs as well as the ccTLDs ".cc" and ".tv"), even if the it is registered by a non-U.S. citizen with a registrar in a foreign jurisdiction, as was the case in *NBC Universal.*

The foregoing three cases show that U.S. courts are ready to accept jurisdiction over ACPA claims in a broad range of circumstances in which a court would traditionally decline jurisdiction. This is largely facilitated by the *in rem* jurisdiction conferred by §1225(d)(2)(A) of the ACPA.

Sallen allows a litigant to pursue a reverse-domain name hijacking claim against a party whose trademarks are registered outside the U.S. *Harrods* endorses the idea that a foreign trademark can "infringe" a U.S. trademark for the purposes of determining rightful ownership over a domain name. Under *NBC Universal,* the U.S. District Court for the Eastern District of Virginia has jurisdiction over any second-level domain under the ".com", ".net" or ".gov" gTLDs registered worldwide. *NBC Universal* also shows at least one American Court's unwillingness to decline jurisdiction even when another seemingly competent court is addressing substantively the same issue.

h. Shortcomings of the ACPA

Being the only national law to deal directly with the problem of cybersquatting, any proposal for a model law should examine the ACPA's shortcomings to avoiding potential pitfalls.

On the positive side, the ACPA is a powerful vehicle for trademark holders. It also provides a certain degree of balance by allowing a registrant to fight what it thinks is a bad UDRP panel decision. The case law outlined above, however, shows what may arguably be called an unjustifiable overreaching by American courts.

The Court in *Sallen* showed a total disregard for the Respondent's foreign trademark rights. The internet is a global network whereas trademark rights are necessarily territorial. The *Sallen* Court's assertion that Congress' use of the term "domain name" in the ACPA gives it jurisdiction to hear any case relating to a domain name regardless of other jurisdictional factors is problematic. This approach would be unsustainable if other countries enacted similar laws and their national courts began taking the same view. Forum shopping would likely become an issue.

Harrods shows even greater disregard for foreign trademark rights. As noted, the global nature of the internet sometimes conflicts with the territorial nature of trademarks. The UDRP deals with this by adopting a "first to register" system. In other words, in a competition between two or more trademark holders, the first to register the domain name should get it and the others should have no recourse so long as the registrant has a "legitimate interest" in the domain name. The Respondent in *Harrods* did have a legitimate interest in the domain names in question; it was a registered trademark holder (though not of U.S. trademarks). The idea that a foreign trademark could be treated as "infringing" a U.S. trademark for the purposes of determining domain name rights shows a wanton disregard for non-U.S. jurisdictions, also known as the rest of the world.

Finally, If the Court in *NBC Universal*'s reasoning is to stand, the fact that Verisign Inc. is located in Virginia has the effect of granting a single U.S. District Court jurisdiction over the whole .com TLD which is currently comports more than 100 million domain names and growing.[86] The Court's indifference to the pending litigation in Korea over the same issue is also troubling. In addition to being an affront to judicial economy,

[86] Sean Michael Kerner, 'Dot Com Domains Top 105 Million Names' (*Enterprise Networking Planet,* 2 January 2013) <http://www.enterprisenetworkingplanet.com/netsp/dot-com-domains-top-105-million-names.html> accessed 2 November 2014.

conflicting judgements from two different national courts may cause enforcement issues, particularly when the domain name registry is not located in one of the states in which a court action has been brought.

Some authors have pointed to the growing unease in certain countries vis-à-vis the current state of internet governance.[87] Not everyone is comfortable with the U.S. Government's significant influence over ICANN. In fact, at a 2005 UN summit, more than 170 countries pressured the U.S. Government to relinquish its unilateral oversight over ICANN; it refused.[88]

There has even been talk of private companies in other countries starting their own intranets which would be excluded from ICANN's control.[89] Users of these intranets would not be excluded from the greater internet, but they would be excluded from the UDRP. Given the ruling in *Sallen*, however, it is debatable as to whether even these drastic measures would be enough to prevent a U.S. court from accepting jurisdiction under the ACPA.

4. A POTENTIAL PATH FORWARD – A MODEL LAW ON CYBER-SQUATTING AND OTHER ABUSIVE DOMAIN NAME PRACTICES

Having established that the current domain name regulatory framework can be improved upon, this paper proposes a model law dealing with cyber-squatting and other abusive domain name practices made to work in place of or in tandem with the UDRP. Before addressing the substantive provisions of the model law as well as its benefits and shortcomings, we must first establish that regulation is in fact the best form of action, and that a model law is the most rational regulatory avenue.

a. Is Regulation the Best Form of Action?

Most countries, with the notable exception of the U.S., have not enacted national legislation dealing with cyber-squatting, relying instead upon trademark laws and the UDRP to address the issue. Based on the shortcomings of the UDRP and national trademark laws, and given the

[87] Horowitz (n 80). See also Christopher Rhoads, 'In Threat to Internet's Clout, Some are Starting Alternatives' (*Yale Global*, 31 January 2006) <http://yaleglobal.yale.edu/display.article?id=6906> accessed 2 November 2014.
[88] Horowitz (n 80) 212.
[89] Rhodes (n 87).

established fact that cyber-squatting is a problem that shows no sign of stopping or slowing down under the current regulatory framework, further regulatory efforts are warranted.

Since cyber-squatting only directly affects a relatively small subset of the population (i.e. trademark holders and domain name registrants) market-based solutions are inapplicable.[90] Unlike perpetrators of online copyright infringement, cyber-squatters are relatively few in number compared with the total number of internet users. A broad-based educational regime would therefore have little effect. Further, most cyber-squatters likely know that what they are doing is objectionable, or at least that it contravenes the UDRP; this does not seem to stop them.

a. What Form Should the Regulation Take?

A Model Law is the Best Regulatory Approach

As set out in Section 5 below, this paper espouses the idea of a model law on cyber-squatting and other abusive domain name practices. There are potential alternatives, for example, a convention to amend national trademark laws to include specific causes of action for cyber-squatting. Another route would be advocating for a re-vamped UDRP that takes into consideration the legal and empirical shortcomings referenced above.

A model law approach would be superior to a convention in that it would create actual legal provisions outlining new causes of action and legal procedures that an adopting country could implement with minimal legislative effort. Since uniform interpretation is a goal, having experts in the area draft purposeful provisions (and potentially provide explanatory notes) would maximize that objective. A convention on this subject-matter would, by contrast, create obligations for signatories without providing any concrete guidance on how to fulfil them.

The model law approach is also superior to advocating for a re-vamped UDRP. Even if ICANN could be persuaded to retool the UDRP to the point where all of the above mentioned concerns would be addressed, the fact remains that it is a policy created by a U.S. non-profit with the U.S. government backing. ICANN itself has been accused of operating in a less than democratic manner.[91] The Model law would achieve the result of a reworked UDRP while respecting national

[90] While it can be argued that cyber-squatting indirectly affects society as a whole, the average individual may be entirely unaware of these practices.

[91] See: A Michael Froomkin, ‘Wrong Turn In Cyberspace: Using ICANN To Route Around The APA And The Constitution’ [2000] 50 Duke LJ 17.

sovereignty and the fact that the internet is a truly international (or more accurately supra-national) space. The model law would also be capable of working in tandem with the UDRP offering disputants the choice to proceed under that Policy if they so choose.

In addition to the above approaches, there is also the option of allowing individual countries to figure cyber-squatting out themselves (or not). The Author does not believe that an uncoordinated, de-centralized effort is appropriate given the global nature of the problem and that the structure of the internet makes compartmentalized regulation a challenge. Be it a model law or some other instrument, the chosen approach should seek to promote a harmonized regime.

b. Is There a Legal Basis for a Model Law Framework?

There is a legal basis for a model law dealing with cyber-squatting and other abusive domain name practices. The model law approach's flexibility allows the adopting country to adjust the model law to fit seamlessly into the country's existing legal regime. This assures respect for the rule of law. Since there is no existing international instrument dealing directly with cyber-squatting, the model law would not conflict with adopting countries' existing treaty obligations.

c. Which is the Appropriate Level (or Levels) of Government to Implement the Model Law?

The appropriate level of government to deal with the adoption and implementation of the model law depends on the constitutional framework of the country in question. In Canada, the model law would almost certainly have to be adopted at the provincial level in accordance with Article 92(13) of the *Constitution Act (1867)*[92] (Property and Civil Rights in the Province). The model law will also include certain procedural provisions (discussed in more detail below) which would engage Article 92(14) (The Administration of Justice in the Province) as well.

d. Do the Benefits of a Model Law Outweigh its Costs?

The model law is a particularly economic approach for at least two reasons:

[92] 30 & 31 Victoria, c 3 (UK).

1) Since it is already drafted, the adoption process is much smoother and less time-consuming for legislators and legislative drafters. This makes it less demanding on the public purse.
2) It uses each adopting country's existing legal system. The law's procedural provisions will reference the adopting jurisdiction's existing procedural rules rather than create new procedures.

While the subset of the population that will benefit directly from the model law is relatively small, adopting it does not pose any obvious social cost given that: 1) it is "complain-driven"; and 2) it poses no budgetary cost (i.e. need to create a regulatory body or bureaucracy).

e. The Model Law's Provisions Must be Clear, Consistent, Comprehensible, and Accessible to Users

In order to maximize the model law's utility, an effort should be made to both employ a plain language drafting style and, wherever appropriate, define terms exhaustively. This approach maximizes both transparency and certainty for potential litigants.

One example of how this will be implemented in the model law is the reverse-domain name hijacking provision. As discussed more fully below, that provision will begin by exhaustively defining reverse-domain name hijacking. This is not the case under the UDRP. UDRP Rule 15(e) defines reverse-domain name hijacking as: "the filing of a complaint in bad faith, resulting in the abuse of the UDRP administrative process." This definition is vague. First, the provision does not tell us what constitutes abuse of the UDRP process. Second, the provision fails to define bad faith. The UDRP offers examples of bad faith registration at Section 4(b), but that provision clearly does not apply to the term bad faith as used in Rule 15(e). The model law provision will list factors for courts to apply when considering whether to grant a plaintiff's cause of action.

Creating a freely available database and digest of decisions dealing with the model law will also achieve the ends of consistency, accessibility and transparency. The United Nations Commission on International Trade Law (UNCITRAL) has implemented this strategy in the creation of its "Case Law on UNCITRAL Texts" (CLOUT) database. The UNCITRAL Commission on International Trade Law has noted the positive effects the CLOUT database has had on promoting uniform application of UNCITRAL texts.[93]

[93] *Report of the United Nations Commission on International Trade Law, Forty-seventh session (7-18 July 2014),* (United Nations, New York, 2014), 32.

f. All Interested Stakeholders Should be Consulted

The three major stakeholders implicated by cyber-squatting regulation are: trademark owners, domain name registrants who are not trademark owners and the general public.[94] Adopting countries should consult representatives of these groups before implementing the model law. Since the model law will encourage a balanced approach, all three of these groups should (in principle) be in favour of it. Representatives of these groups will, however, lobby for amendments to the law favourable to their respective priorities, which will often collide.

g. How Will Compliance with the Model Law be Achieved?

One of the weaknesses of the model law approach (discussed more fully below) as with any international instrument is that a sovereign state cannot be forced to adopt it. The hope is that governments will see the merits in the model law and wish to adopt it. However, once the model law is adopted, compliance will be achieved through the adopting country's judicial system.

Once implemented, the model law will be enforceable like any other law. Compliance would be encouraged by the fact that the law is backed by the executory force of the judicial system. This may be contrasted with a model law favouring arbitration where a successful party would, after succeeding before the arbitral tribunal, still have to commence proceedings before the court in the enforcement jurisdiction (this is known as single exequatur or homologation).[95]

Benefits and Shortcomings of a Model Law Approach

As with any regulatory approach, a model law comports both benefits and shortcomings. The Author is naturally of the opinion that the former outweigh the latter in the present context.

[94] See Warren B Chick, 'Lord of your Domain but Master of None: The Need to Harmonize and Recalibrate the Domain Name Regime of Ownership and Control' [2008] 16 Int'l JL & Info Tech 8, 32.

[95] See A Redfern and M Hunter, *Law and Practice of International Commercial Arbitration* (4th edn, Sweet & Maxwell, 2004), 516; and Antonin I Pribetic, '"Winning is Only Half the Battle": Procedural Issues Relating to the Recognition and Enforcement of Foreign Arbitral Awards' [2009] 8 ICFAI University Journal of Alternative Dispute Resolution 11, 13.

h. Benefits

As noted in brief above, the model law offers the best of both worlds: certainty of content and flexibility of implementation. Different countries have varying judicial procedures and systems of adjudication. The most obvious distinction is between Common Law and Civil Law jurisdictions. The model law's drafting will be juridically neutral. This means that the provisions of the law will either make use of only neutral terms (i.e. terms that do not derive specifically from Common Law or Civil Law) or will include the terms applicable in both legal traditions.[96]

Another benefit is the creation of binding precedent within a given jurisdiction and persuasive jurisprudence vis-à-vis other model law countries. Like all arbitral awards, the decisions of UDRP panels are not binding on future panels.[97] This has led to inconsistent and often conflicting decisions.[98] In contrast, courts in Common Law jurisdictions operate under the principle of *stare decisis*, the rule that courts are bound by prior decisions dealing with the same subject-matter. While this is not the case in civil law jurisdictions, there is the notion of *jurisprudence courante*. This doctrine stands for the proposition that, without being binding, a steady current of consistent decisions on a legal point (especially by a country's high court) is highly persuasive on other courts.[99] These doctrines serve the important objective of providing legal certainty to litigants (and potential litigants) which is currently lacking under the UDRP.

To amplify the benefit of this new body of case law, the entity responsible for drafting the model law should keep and update a searchable database which should be freely accessible. As noted above, this has already been implemented by UNCITRAL to positive effect.

[96] An example of the latter technique may be found at s 75 of the Canadian *Bankruptcy and Insolvency Act*, RSC, 1985, c B-3: 'Despite anything in this Act, a deed, transfer, agreement for sale, mortgage, charge or hypothec…'

[97] Yun Zhao, 'Reflection on the Finality of Panel's Decisions in Domain Name Dispute Resolution Process, With Reference to China's Practice' [2008-2009] 26 J Marshall J Comp & Info L 395, 399-400.

[98] Ibid, 408.

[99] See Jean-Louis Baudoin, 'The Impact of the Common Law on the Civilian Systems of Louisiana and Quebec', in Joseph Dainow, *The Role of Judicial Decisions And Doctrine In Civil Law And In Mixed Jurisdictions* (Louisiana State University Press 1974) 13; and Jean Boulanger, 'Notations sur le Pouvoir Créateur de la Jurisprudence Civile' [1961] 59 Revue Trimestrielle de Droit Civil 417.

The models law's treatment of cyber-squatting and reverse-domain name hijacking as legislatively and conceptually separate from trademark law is another key benefit. While related, domain names and trademarks are not the same. The legal principles surrounding trademark law can be ill-fitting in the cyber-squatting context. For example, a key concepts in trademark law is consumer confusion. In Canada (like many other jurisdictions), in order to demonstrate trademark infringement, a plaintiff must show a likelihood that the average Canadian consumer would be confused by the defendant's mark into thinking that the latter's goods or services were actually being offered by the plaintiff.[100] In many cases, the average consumer would not be confused by a cyber-squatter's use of a trademark in a domain name.[101]

Some jurisdictions including Canada and the U.S. require that a defendant "use" a trademark for there to be trademark infringement.[102] Cyber-squatters often do not post any content (or relevant content) to the domain.[103] In these cases, even though the defendant is clearly engaging in cyber-squatting, a plaintiff in a trademark infringement action would be unsuccessful due to its inability to meet the threshold use requirement.[104]

Other trademark related causes of action such as trademark dilution under American trademark law have been applied to the domain name context as well.[105] Some trademark holders have found success with dilution arguments.[106] There are still gaps in protection, however. First, the dilution provisions only apply to "famous trademarks".[107] This short-changes trademark owners who have not achieved "fame" status, but are

[100] *Mattel, Inc v 3894207 Canada Inc* [2006] SCC 22, 56.

[101] Keith Blackman, 'The Uniform Domain Name Dispute Resolution Policy: A Cheaper Way To Hijack Domain Names And Suppress Critics' [2001] 15:1 Harv JL & Tech 212, 217.

[102] *Clairol International Corp v Thomas Supply & Equipment Co* [1968] 55 CPR 176, 3.

[103] Blackman (n 101) 218.

[104] There must also be a commercial component to the use by the cyber-squatter. S 4 of the Canadian *Trade-marks Act*, RSC, 1985, c T-13 requires use "in the normal course of trade". The relevant provisions of the *Lanham Act* require "use in commerce".

[105] *Federal Trademark Dilution Act*, codified at 15 USC s 1125(c).

[106] See *Intermatic Inc v Toeppen* [1996] 947 F Supp 1227.

[107] The provision reads: "Subject to the principles of equity, *the owner of a famous mark* that is distinctive, inherently or through acquired distinctiveness, shall be entitled to an injunction against another person who, at any time *after the owner's mark has become famous,* commences use of a mark or trade name…"(Emphasis added).

well-known enough to attract a cyber-squatter. Second, the provision is only meant to apply to instances in which there is "blurring" or "tarnishment" of the plaintiff's trademark.[108] In some instances a cyber-squatter registers a domain name and immediately contacts the trademark owner to offer it for sale without populating it with content. In these cases, no blurring or tarnishment could have occurred.

i. Shortcomings

Like any international instrument, a model law is only useful if it is implemented. Some model laws have been very well received. Two examples of these are the *UNCITRAL Model Law on International Commercial Arbitration* and the *UNCITRAL Model Law on Electronic Commerce* which have been adopted in 67 countries (totalling 97 jurisdictions) and 61 countries (totalling 126 jurisdictions) respectively.[109] Others have been made available for adoption for several years without implementation by a single jurisdiction.[110]

Since the U.S. already has the ACPA, it would likely not sign onto the model law. Given that U.S. courts have demonstrated a willingness to exercise extra-territorial jurisdiction when it comes to domain names, the effect of the model law may be attenuated. That said, U.S. courts are predisposed to exercise extra-territorial jurisdiction as it is under the ACPA. There is no reason why implementing the model law would exacerbate that fact.

Though improving the corpus of international domain name law, the model law will not have the effect of creating internationally binding precedents. The court decisions in one sovereign country will never have binding effect on courts in other sovereign countries; there is thus still room for contradictory jurisprudence.

[108] Blackman (n 101) 219. See also *Toppen* (n 106) and *Hasbro Inc v Internet Entm't Group, Ltd,* [1996] 40 US P Q 2d 1479.

[109] See 'UNCITRAL Texts and Status' (*United Nations Commission on International Trade Law*) <http://www.uncitral.org/uncitral/en/uncitral_texts.html> accessed 14 November 2014.

[110] For example, the UNCITRAL Model Law on International Credit Transfers (1992) has not been ratified anywhere, although a directive of the European Parliament and of the Council of the European Union based on the principles of the model law was issued on 27 January 1997. Another example is the UNCITRAL Model Law on Public Procurement (2011) which has yet to be adopted.

In spite of the shortcomings to the model law approach, the Author is still of the opinion that they are far outweighed by the benefits.

j. Key Provisions of the Model Law

The model law's two most important provisions are the cyber-squatting and the reverse-domain name hijacking causes of action. This section will also outline a few other key provisions to be drafted into the model law.

k. Cause of Action for Cyber-Squatting

This provision seeks to improve upon Section 4 of the UDRP. The UDRP requires the complainant to prove that the respondent has "no rights" in the disputed domain name. This asks the complainant to prove a negative. Instead, the model law provision will require the plaintiff to show that, after exercising reasonable diligence, it is unable to identify any legitimate rights in the domain name. The provision will set out a non-exhaustive list of what constitutes legitimate rights; this list will include express recognition of free expression rights.[111] Once this threshold is met, the burden will shift to the defendant to show that it does in fact have a legitimate right.

The ACPA's wording seems to be a good starting point. Like the ACPA, the provision will expressly include protection for personal names. The provision will also favour the ACPA's "bad faith intent to profit" language over the UDRP's "registration and use in bad faith" language. This will capture passive domain name warehousing so long as it can be shown that the warehouse's only reasonable goal was to lure the trademark owner into making an offer to purchase the domain name. The bad faith considerations listed in the ACPA will also be incorporated, with certain exceptions. For example § 1125(d)(1)(B)(VIII) reads:

[T]he person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties.

[111] The ACPA references 'bona fide [sic] non-commercial or fair use' at s 1125(d)(1)(B)(IV). Since fair use is a doctrine found exclusively in US law, the model law will us more neutral 'freedom of expression style' language.

This factor would be excluded. The intention here was to allow the court to consider whether the defendant has demonstrated a pattern of cyber-squatting. This is not relevant. The cause of action is against cyber-squatting, not the identification and elimination of *cyber-squatters*. The action is between the plaintiff and defendant. The only relevance is whether the defendant has infringed the plaintiff's rights. We do not consider a defendants prior conduct when determining infringement in the patent, copyright and trademark contexts; why should it be considered here?

The model law will also allow *in rem* actions against websites. Unlike the ACPA, this will only be allowed when, after exercising due diligence, the plaintiff was unable to locate the defendant. The ACPA also allows for an *in rem* action when the plaintiff is "unable to obtain *in personam* jurisdiction" over a would-be defendant.[112] This was applied in *NBC Universal* to allow the U.S. District Court to assume jurisdiction even though NBC was able to locate the registrant. Limiting *in rem* actions to instances in which the registrant legitimately cannot be found would limit the potential for jurisdictional encroachments like the one in *NBC Universal*.

Cause of Action for Reverse-Domain Name Hijacking

This provision will provide an individual who feels they have been wronged by a domain name dispute panel with a means of retaining their domain name and obtaining damages for frivolous or vexatious proceedings undertaken by a complainant. The model law's reverse-domain name hijacking provision will exhaustively define the term. One possible definition could be the following: "Reverse-domain name hijacking" refers to the act of instituting frivolous, vexatious or baseless proceedings under the UDRP or another domain name dispute policy.

The provision would then set out a test for determining whether to grant a reverse-domain name hijacking claim. Some of the factors to be considered would include the following:

- Assuming the facts alleged by the complainant are true, does complainant meet the legal standard required to succeed under the relevant policy?
- Did complainant make an attempt to settle the matter amicably with respondent before instituting proceedings?
- Did complainant undertake any due diligence to determine the existence and extent of respondent's rights in the disputed domain name?

[112] s 1125(d)(2)(A)(ii)(I).

- Did respondent attempt to communicate to complainant that it had rights in the disputed domain name?
- Does respondent's domain name registration predate complainant's trademark rights?

Note that none of these factors directly refers to the correctness of the panel's decision. This is because the reverse-domain name hijacking provision is not an "appeal" or "review" of the panel's decision so much as it is a cause of action against the complainant in that process. This approach is necessary due to the inconsistency with which UDRP panels apply legal concepts. If the model law allowed for a judicial review of panel decisions, courts in each adopting jurisdiction would likely look at the case as a function of whether the decision conforms to that jurisdiction's trademark law. This would thwart the model law's harmonization objective.

l. Other Key Provisions

A few other key provisions to be included in the model law include:

- Jurisdictional Provision

The model law will maximize jurisdictional certainty to minimize forum shopping. Every jurisdiction has its own body of private international law. However, the model law may offer guidance on whether the court should accept jurisdiction over a cause of action thereunder. Some potential factors for determining jurisdiction could be:

- Residence of parties
- Location of trademark registration
- Location of the domain name registry
- Country in which one of the parties has significant assets or business dealings.

The Author does not advocate for any of these in particular. Further study should be given to the question of what constitutes the best indicator of appropriate jurisdiction. The location of the domain name registry (applied in *NBC Universal*) appears to be a weak factor because it would grant exclusive jurisdiction to a single court for each TLD. It is, however, a potential factor and should therefore be left on the table until decided otherwise by the drafters of the model law.

- Default Should be Summary or Abridged Proceeding

One of the UDRP’s benefits is its speed and cost-effectiveness. No court process will be as cheap as a UDRP proceeding. However, the model law could favour quick and cost-effective resolution by including a provision which presumes a summary or simplified procedure wherever such an option exists in the adopting country’s procedural rules.

The model law would employ neutral language so as not to refer to a specific type of procedure. For example, the provision would not expressly use the term “summary proceeding” or “simplified procedure” as those terms refer to procedural rules that may not exist everywhere. Adopting jurisdictions would then be free to modify the text of this provision to refer to their own procedural mechanisms. For example, in Ontario, the model law could refer to the simplified procedure rules (Rule 76) in the *Rules of Civil Procedure*.[113]

- Burden of Proof

The model law should have a provision expressly setting out which party has the burden of proof in a given context. This will almost always be the plaintiff, though certain provisions -such as the requirement for a defendant in a cybersquatting action to show that it does have rights in the domain name after the plaintiff demonstrates reasonable diligence in trying to ascertain the existence of those rights- may reverse that presumption.

- Stay Provisions

The Model law should comport a stay provision allowing: 1) a party to have the court order that a domain name dispute resolution panel stay its proceedings pending final resolution by the court; and 2) a party to have a proceeding taken under the model law stayed if there is a pending proceeding in another model law jurisdiction dealing with the same subject-matter.

5. CONCLUSION

[113] RRO 1990, reg 194.

The current domain name dispute resolution framework is inadequate as the UDRP, ACPA and national trademark laws are only partially effective. The model law presents a novel solution.

The model law is superior to the UDRP because: it creates an exhaustive legal regime under which no reference need be made to trademark law; decisions invoking the model law are final; it eliminates the propensity for bias inherent in the complainant/provider-driven UDRP panel selection process; the greater variety in legal background of judges eliminates the pro-intellectual property slant some UDRP panellists may carry; it provides robust protection against reverse-domain name hijacking; it captures passive warehousing; it protects personal names; and it will not conflict with national consumer protection and language laws.

The model law's key cyber-squatting provision will bear a stark resemblance to § 1125(d) of the ACPA. However, the jurisdictional provisions in the model law will do a much better job of circumscribing the jurisdiction of the national courts in adopting countries.

Trademark law has never fully addressed cyber-squatting. The fact that the model law would be treated as conceptually separate from trademark law would allow for the case law developing around the new causes of action to be uninhibited by those ill-fitting concepts.

Since there are currently no international treaties on cyber-squatting, there is a legal basis for a model law dealing with cyber-squatting and other abusive domain name practices. The appropriate level of government to deal with the adoption and implementation of the model law depends on the constitutional framework of the country in question.

The benefits of the model law justify its minimal implementation cost because: 1) the model law comes essentially ready for implementation cutting the time and cost associated with enacting legislation from the ground up; and 2) Since litigants would go before the courts, there would be no need to create any additional administrative body for oversight or adjudication.

The law's provisions will be clear, consistent and accessible. This will be achieved primarily through plain language drafting and properly defined terms. All interested stakeholders, namely trademark owners, domain name registrants who are not trademark owners and the general public, should be consulted before the model law is implemented in each adopting country. Compliance with the model law, once enacted, will be achieved through the adopting country's established judicial system and will enjoy the benefit of the executory force attached thereto.

While it represents a significant undertaking, this paper shows that drafting and implementing a model law dealing with cyber-squatting and other abusive domain name practices would be the most effective regulatory approach to curbing cyber-squatting and reverse-domain name hijacking. The UDRP and ACPA are fifteen years old. Both are laudable efforts, but neither has ever adequately measured up to the task of eliminating (or greatly diminishing) cyber-squatting. Perhaps, in 2014, it is time to revisit the domain name regulatory framework and create a complete, harmonizing document in the hopes of addressing the issue once and for all.