LET GO OF MY DOT-CA: USING THE CDRP IN THE FIGHT AGAINST CYBERSQUATTING

Melissa Beaumont*

INTRODUCTION[1]

IT GOES WITHOUT SAYING that the Internet has transformed the way in which the world does business. With its speed, accessibility, and ease of use, the opportunities for using the Internet as a business tool seem endless. The Internet has drastically reduced the time and expense needed to get around the many geographical barriers associated with doing business. Consumers today have come to rely on the Internet to research and purchase goods and services available from all corners of the globe. At the same time, businesses have come to rely on the Internet to convey their brands around the world and access new markets.

That being said, it must be kept in mind that the Internet, like any new technology that creates business opportunities, undoubtedly creates threats as well. It is therefore imperative that businesses not be blinded by the initial dazzle of the Internet and stay abreast of the new types of threats that arise as a result of its growing and evolving nature.

Domain name abuse, or "cybersquatting," is one such threat that all Internet users have likely experienced. For example, an Internet user might have once typed into an Internet address bar <www.blackanddecker.ca>, expecting to be taken to the website of a well-known manufacturer of power tools and appliances, but was instead directed to a webpage providing links to what appeared to be Black & Decker's competitors.[2] A similar result may have once occurred when an Internet user searching for the Canada Post website mistakenly omitted the second "a" in "Canada" and typed in <www.candapost.ca>.[3] It was neither a coincidence nor an accident that those Internet users were redirected to unexpected webpages. Rather, these domain names were strategically chosen and registered by those known as cybersquatters.

This paper identifies some of the legal issues surrounding cybersquatting and the different forums available for formal redress

* B.Comm. (Hons.) (UM); LL.B. (UM, 2008)

[1] The author would like to acknowledge her classmates and Dr. Bryan Schwartz for their comments and any other influence they might have otherwise had on this paper. Any errors or omissions remain the sole responsibility of the author.

[2] Based on *The Black & Decker Corporation v. J. Chapnik Trust—(100%),* CIRA Decision No. 00069 (15 November 2006).

[3] Based on *Canada Post Corporation v. Marco Ferro,* CIRA Decision No. 00042 (22 October 2005).

against cybersquatters. Although the legal issues underlying cases of cybersquatting might resemble traditional trade-mark infringement principles and be actionable *via* the courts, several arbitration systems have now been put in place to deal uniquely with this issue.

This paper explores the scope and procedures of two such arbitration systems: the *Uniform Domain Name Dispute Resolution Policy* ("*UDRP*") system and the *Canadian Internet Registration Authority Domain Name Dispute Resolution Policy* ("*CDRP*") system; with a predominant focus on the latter. The *UDRP* system was the first established domain name dispute resolution system and is used to resolve disputes involving generic domain spaces (for example, the dot-com). The *CDRP* system is used to resolve disputes involving the dot-ca domain space. As the *CDRP* was established subsequent to the *UDRP,* this paper will highlight some of the differences between the two systems.

The purpose of this paper is four-fold. First, this paper serves to identify and analyze some of the specific criticisms against the *CDRP.* Second, this paper will identify both how the *CDRP* has improved on some aspects of the *UDRP* and what it can still learn from the *UDRP.* Third, this paper serves to recommend improvements that the *CDRP* uniquely might benefit from. Finally, this paper will touch on some of the deficiencies inherent in both the *CDRP* and *UDRP* systems and will discuss potential future improvements that might be beneficial to either system.

A QUICK BUSINESS LESSON: THE INTERNET'S IMPACT ON BRANDING

Any person or entity seeking to do business should be aware of the importance of establishing and securing a brand. A key tool for brand maintenance is the focus on the brand's "marketing mix," or what is generally known in the marketing world as the "4Ps": product, price, place, and promotion.[4] It goes without saying that the emergence of the Internet has had a significant influence on the way those 4Ps interact, thus creating the need to re-consider business plans and branding strategies. For example, the "place" variable has been significantly expanded as the Internet has improved the convenience with which a consumer can access a greater selection of products and services.[5] Similarly, the "promotion" variable has also increased in complexity as the Internet has created a new medium by which information can be

---

[4] Philip Kotler, Gary Armstrong & Peggy H. Cunningham, *Principles of Marketing*, 6th Can. ed., (Toronto: Pearson Education Canada Inc., 2005) at 67.
[5] *Ibid.* at 89.

communicated to businesses with their customers in highly useful and interactive forms.[6]

Considering the above examples, it is no wonder that businesses are seeking to establish themselves on the Internet. Major advantages of setting up online include enhancing a business's ability to build customer relationships, improving the efficiency of business operations, and increasing the speed at which business can be conducted.[7] In today's business world, establishing a presence on the Internet is not only important, it is imperative. Gone are the days where an Internet presence is a unique strategic advantage; rather, an Internet presence has become a necessary business requirement which consumers have come to expect.

Despite the many business opportunities that the Internet creates, however, major caveats exist. For instance, it must be remembered that setting up online means competing in a global market.[8] On one hand, global competition may seem lucrative, as brands gain exposure to global marketplaces, ultimately resulting in a substantially larger consumer base. On the other hand, global competition also requires brands to contend with competitors from around the globe. This presents a significant risk of brand dilution, as the Internet "[c]reates an environment in which a company's brands are subject to extensive use by competitors, affiliates, partners, resellers and consumers."[9] The Internet not only presents the threat of brand dilution, but is also a magnet for many other forms of brand abuse, such as competitive trade-mark confusion, false brand affiliation, website traffic diversion, and domain name abuse.[10] Trade-mark infringement often lies at the heart of these forms of abuse.

Domain name abuse, also known as cybersquatting, is the underlying issue of this paper. As a business's website is often the first point of brand recognition for the e-consumer, a well-recognized domain name becomes a prime target for brand infringement. One's domain name is certainly a critical element of a website, forming both the "real estate" and brand image of the business.[11] In other words, a domain name is both a key business identifier and valuable intellectual property.[12]

---

[6] *Ibid.* at 89-90.
[7] *Ibid.* at 90-91.
[8] *Ibid.*
[9] Mark McGuire, "Comprehensive Internet brand protection strategy is a must in today's world" *The Lawyer's Weekly*, 22:29 (29 November 2002) (QL).
[10] *Ibid.*
[11] Richard Fletcher, Jim Bell & Rod McNaughton, *International e-Business Marketing* (England: Thomson Learning, 2004) at 155-6.
[12] May M. Cheng & Ziad J. Katul, "Assessing the Merits of your Alternative to Litigation" 16 I.P.J. 485 at 486 (WL).

A QUICK INTERNET LESSON: WHAT IS A DOMAIN NAME?

The Nuts and Bolts of Domain Names

A domain name, more commonly known as a website address or a Uniform Resource Locator ("URL"), is the registered alpha-numeric designation which refers to an Internet Protocol ("IP") address.[13] An IP address specifies the location of a website's host computer,[14] and is comprised of four sets of numbers separated by periods.[15] Domain names are used to locate websites more commonly than IP addresses, as they are easier to remember. Domain names have been compared to telephone numbers in that they must be unique, must be registered by one person only, and are registered on a first-come, first-served basis.[16]

The element of the domain name which appears after the last "dot" is the top-level domain ("TLD");[17] for example, the ".com" or ".ca" portion of a domain name. There are two main types of TLDs. The first is the generic TLD ("gTLD"), which encompasses the most common domain spaces (such as dot-com, dot-net, and dot-org).[18] The second type is the country code TLD ("ccTLD"), which encompasses country-specific domain spaces (such as dot-ca for Canada or dot-uk for the United Kingdom).[19] For all domain names with gTLDs and for certain ccTLDs, registration and governance is managed by the Internet Corporation for Assigned Names and Numbers ("ICANN"), an international organization responsible for managing and coordinating the domain name system.[20] However, many countries have taken the management of their respective ccTLDs into their own hands. Canada is one such country. For all domain names with the dot-ca ccTLD, registration and governance is managed by the Canadian Internet Registration Authority ("CIRA"), as opposed to ICANN.

---

[13] Sheldon Burshtein, *Domain Names and Internet Trade-Mark Issues: Canadian Law and Practice* (Toronto: Thomson Canada Limited, 2005) at 2-1.

[14] *Network Solutions, Inc. v. Umbro International, Inc.*, 529 S.E. 2d 80 (E.D. Va., 2000) cited in Burshtein, *ibid.*

[15] *Name.Space, Inc. v. Umbro International Inc.,* 202 F.3d 573 (C.A. 2, 2000), cited in Burshtein, *ibid.* Also see Bradley J. Freedman & Robert J.C. Deane, "Trade-Marks and the Internet: A Canadian Perspective" (2001) 34 U.B.C.L. Rev. 345-414 at paras. 40-41 (QL).

[16] Burshtein, *supra* note 13 at 2-2. Also see Freedman & Deane, *ibid.* at paras. 45-46; Luke Walker, "Dispute Resolution: ICANN's Uniform Domain Name Dispute Resolution Policy" (2000) 15 Berkeley Tech. L.J. 289 at 291-295; and Ida Madieha Azmi, "Domain Names and Cyberspace: the Application of Old Norms to New Problems" (2000) 8 I.J.L. & I.T. 193 at 194.

[17] Burshtein, *ibid.*

[18] *Ibid.*

[19] *Ibid.*

[20] "Fact Sheet", online: ICANN <http://www.icann.org/general/fact-sheet.html>.

Registering a Domain Name

Registering a domain name is not a complex process. For example, the process under CIRA for registering a dot-ca domain name requires just a few simple steps. First, the applicant must satisfy what is known as the "Canadian Presence Requirements"[21] which ensure that the applicant has a connection to Canada (for example, is a Canadian citizen, permanent resident, corporation, association, etc.). Next, the applicant must conduct a "Whois" search to see if the domain name is available for registration.[22] "Whois," an online directory of domain name information, allows people to view the availability of a potential domain name and to look up contact or technical information about an existing domain name.[23]

If the domain name is available for registration, the applicant selects a certified registrar to whom it will send its registration application.[24] The registrar then acts on behalf of the applicant in submitting the registration to CIRA.[25] In other words, the registrar is the "middle man" who acts between the individual applicant and CIRA. Applicants should choose the registrar most suitable to their needs, as each registrar may have different contractual provisions, may offer different services, may have different geographical focuses, may function in different languages, and may have different terms and conditions regarding payment.[26] Once the registrar is chosen and the applicant has submitted the relevant information, the registrar prepares and submits the domain name registration request to CIRA.[27]

It should be noted that the CIRA General Registration Rules provide that it is the applicant's responsibility to ensure the legality of the domain name being registered:

> It is the Applicant's responsibility to ensure that the Applicant has the right to use the Domain Name which is the subject of the Registration Request and that the registration or use of the Domain Name to which the Registration Request relates does not violate any third party intellectual property rights or other rights, does not

---

21 CIRA Polices, Rules and Procedures, "General Registration Rules," Version 3.9, online: CIRA <http://www.cira.ca/en/cat_Registrar.html> at para. 2.1 [CIRA General Registration Rules].

22 *Ibid.* at para. 2.2.

23 "Whois Frequently Asked Questions", online: CIRA <http://www.cira.ca/en/Whois/whois-faq.html>.

24 CIRA General Registration Rules, *supra* note 21 at para. 2.3.

25 *Ibid.*

26 *Ibid.*

27 *Ibid.* at para. 2.4.

> defame any person and does not contravene any applicable laws including Canadian federal, provincial and territorial human rights legislation and the laws of the *Criminal Code* (Canada), R.S.C. 1985, c. C-46 as amended from time to time.[28]

The process for registering a dot-com is also fairly straight forward, requiring steps similar to the dot-ca registration. Applicants must select an ICANN-accredited registrar, select a domain name to be registered, perform a search to see if the domain name is available, and then provide the registrar with the information necessary for the registrar to effectuate the registration.[29]

Domain Names versus Trade-marks

The issues underlying domain name abuse and trade-mark infringement are closely related. Trade-marks often look like domain names, and domain names often look like trade-marks. However, a domain name, although registered, is not itself considered a trade-mark unless it is used as such.[30] A trade-mark under Canadian legislation can be defined as:

> (a) a mark that is used by a person for the purpose of distinguishing or so as to distinguish wares or services manufactured, sold, leased, hired or performed by him from those manufactured, sold, leased, hired or performed by others,
> (b) a certification mark,
> (c) a distinguishing guise, or
> (d) a proposed trade-mark.[31]

Domain names differ from trade-marks in that slightly different and confusingly similar domain names can be registered.[32] Trade-marks are generally registrable only if they are not confusing with an already registered mark.[33] The registrability requirements of domain names, however, are less stringent. Apart from character and length requirements,[34] the restrictions to registering a domain name under

---

[28] *Ibid.* at para. 2.8.
[29] Ryan Sewchuk, "The UDRP and the ACPA: What Are They, and Which Should be Used?" (2002) 2 Asper Rev. Int'l Bus. & Trade L. 85 at paras. 3 & 4 (QL).
[30] Burshtein, *supra* note 13 at 3-56.
[31] *Trade-Marks Act,* R.S.C. 1985, c. T-13, s. 2.
[32] Freedman & Deane, *supra* note 15 at para. 51.
[33] *Trade-Marks Act, supra* note 31, s. 12(1)(d).
[34] See CIRA General Registration Rules, *supra* note 21 at paras. 3.1 & 3.2.

CIRA are that it not be a reserved name[35] and that it not be a "conflicting name."[36] A conflicting name is one that is an *exact* match in all aspects of a domain name that has already been registered by CIRA.[37] However, it should also be noted that the CIRA does ultimately maintain, in its sole discretion, the right to refuse to register any domain name.[38]

Further, domain names, unlike trade-marks, need not be distinctive of a good, service, or business and need not even be used once registered.[39] A trade-mark on the other hand, referring back to the definition above, has "the purpose of distinguishing or so as to distinguish wares or services" of the trade-mark holder. Thus, a trade-mark in relation to wares must actually be marked on the wares or packaging of the wares themselves[40] and a trade-mark in relation to services must be used or displayed in the performance or advertising of the services themselves.[41]

Although a domain name is not necessarily in and of itself a trade-mark, a trade-mark may, and often does, form all or part of a domain name.[42] This is where there problem of domain name abuse arises.

THE PROBLEM OF CYBERSQUATTING

GENERALLY, CYBERSQUATTING OCCURS when a person registers a domain name that incorporates a well-known trade-mark and then offers it for sale to the "highest bidder"[43]; usually the trade-mark holder. Cybersquatting has thus been characterized as "hijacking for ransom," whereby cybersquatters intentionally register domain names comprised of trade-marks belonging to others.[44] Trade-mark owners are then forced to pay money for access to these domain names.[45] The

---

[35] *Ibid.* at para. 3.3, which provides examples of "reserved" domain names such as "village.ca," "town.ca," "city.ca," "ville.ca," names and abbreviations of Canada, its provinces and territories, etc.
[36] *Ibid.* at para. 3.4.
[37] *Ibid.*
[38] *Ibid.* at para. 3.5.
[39] Freedman & Deane, *supra* note 15 at para. 51.
[40] *Trade-Marks Act, supra* note 31, s. 4(1).
[41] *Ibid.*, s. 4(2).
[42] Hasan A. Deveci, "Domain Names: Has Trade Mark Law Strayed From Its Path?" (2003) 11 I.J.L. & I.T. 203 at 205-206.
[43] Freedman & Deane, *supra* note 15 at para. 53.
[44] Burshtein, *supra* note 13 at 4-81.
[45] *Ibid.* at 4-81.

problem stems from the first-come, first-served nature of the domain name registration system.[46]

In addition to collecting "ransom," a cybersquatter might want to register a well-known trade-mark as a domain name in order to affect Internet traffic. For example, using a well-known domain name might help improve search results for the registrant's own website or might help the cybersquatter attract Internet users initially seeking a legitimate brand to his or her site.[47] An increasingly popular practice among cybersquatters has been to "park" domain names at websites "that offer revenue programs whereby domain name holders who redirect Internet traffic to these websites become eligible for a referral fee."[48] These "parking" websites usually contain links to other websites on a "pay-per-click" basis, and both the parking service and the registrant share in the revenue.[49]

The threats that cybersquatters pose are significant and impact businesses in numerous ways. First, *cybersquatters interfere with consumer behaviour.* Cybersquatters have the effect of diverting the consumer's attention away from the intended brand. Thus, in the course of an electronic transaction, the potential consumer might either end up making an alternative purchase with a competitor or might forgo making a purchase altogether in frustration.[50] Second, *cybersquatters may create ongoing battles for businesses.* For some companies, the problem may not readily go away. For example, Mattel is often in battles against cybersquatters (amongst other types of brand abusers) who use its "Barbie" brand in relation to pornography and escort service websites.[51] Third, *cybersquatters cause loss of revenue.* Not only is revenue lost as a result of consumers changing their buying behaviour, but also when the ability of a business to engage in online transactions is compromised.

For example, consider the experience that the Organisation of Economic Co-operation and Development ("OECD") had with domain name abuse. The OECD became victim to a cybersquatter when they accidentally allowed the registration of one of their domain names to lapse. A cybersquatter had taken advantage of this lapse in registration

---

[46] Cheng & Katul, *supra* note 12 at 488.
[47] Brian H. Murray, *Defending the Brand: aggressive strategies for protecting your brand in the online arena* (New York: AMACOM, 2004) at 45.
[48] *Alberta Alcohol and Drug Abuse Commission v. Akshay Khanna*, CIRA Decision No. 00065 (12 October 2006) at para. 60.
[49] "Cybersquatting Remains on the Rise With Further Risk to Trademarks From New Registration Practices" WIPO/PR/2007/479, online: WIPO <http://www.wipo.int/edocs/prdocs/en/2007/wipo_pr_2007_479.html>.
[50] Murray, *supra* note 47 at 70.
[51] *Ibid.* at 10-11. Also Sewchuk, *supra* note 29 at para. 33.

and took over the domain name for over a month.[52] Although the OECD case was not about a loss of revenue, imagine the impact on revenue if this were to happen to a major online business!

Given that cybersquatting is a problem for business that is unlikely to resolve itself, businesses must have a way to judicially or administratively seek an enforceable remedy against cybersquatters.

RESOLVING A DOMAIN NAME DISPUTE

Traditional Litigation

Businesses that fall victim to dot-ca cybersquatters may be able to take the matter to court. In the litigation context, the issue will likely be resolved according to Canadian trade-mark law.[53] If successful, a variety of remedies are available from the courts, such as an injunction, the transfer of the domain name, damages (including punitive), accounting, and costs.[54] Similarly, businesses that fall victim to dot-com cybersquatters also have the option of taking their case to court, where the matter will be resolved under American trade-mark law. In fact, the United States passed an amendment to their federal trade-mark legislation, under the *Anti Cybersquatting Consumer Protection Act* ("*ACPA*"),[55] that deals specifically with the bad faith taking of domain names. The *ACPA* is not limited to cases involving American trade-marks[56] and it provides for remedies such as cancellation or transfer of the domain name to the plaintiff, injunctions, and damages.[57] Uniquely, the *ACPA* also provides for *in rem* proceedings against the domain name if the registrant cannot be located,[58] giving the complainant the option of suing the domain name itself, as opposed to the domain owner.[59] This is

---

[52] "Cybersquatting: The OECD's Experience and the Problem it Illustrates With Registrar Practices and the Whois System", online: OECD <http://www.oecd.org/dataoecd/46/53/2074621.pdf> [OECD Report].

[53] For example, under the *Trade-marks Act* for registered marks, or under common law passing-off principles for unregistered marks.

[54] Burshtein, *supra* note 13 at 5-48 – 5-99.

[55] 15 U.S.C. § 1125(d).

[56] Cheng & Katul, *supra* note 12 at 519.

[57] J.M. Osborn, "Effective And Complimentary Solutions to Domain Name Disputes: ICANN's Uniform Domain Name Dispute Resolution Process and the Federal Anticybersquatting Consumer Protection Act of 1999" (2000) 76 Notre Dame L.R. 209 at 236 cited in Sewchuk, *supra* note 29 at para. 44. Also see the related discussion in Burshtein, *supra* note 13 at 6-28 – 6-30.

[58] Sewchuk, *supra* note 29 at para. 45.

[59] Freedman & Deane, *supra* note 15 at para. 126. However, note that under an *in rem* action, the only remedies available are cancellation or transfer of the

an important remedy, as the anonymity of the Internet can make it difficult, if not impossible, to track down the offending registrant. A limitation of the *ACPA*, however, is that it only seems to protect famous or distinctive trade-marks.[60]

An analysis of domain name dispute resolution via the courts is beyond the scope of this paper. However, it can be said generally that litigating this issue has its disadvantages. These include delay, high costs, and jurisdictional issues[61]; the latter being of great concern given the unregulated, global nature of the Internet. Time is also of the essence in cybersquatting disputes, as many complainants are businesses in need of resolving the dispute as quickly as possible in order to avoid large losses in revenue. One author suggests that this need to quickly restrain the use of domain names is a reason why few Canadian domain name cases have been resolved in court.[62]

As a response to the pitfalls of litigating domain name disputes, arbitration mechanisms have been put in place to more efficiently and cost-effectively resolve cybersquatting disputes.[63]

Arbitration of a dot-com dispute: the UDRP

As previously noted, ICANN manages and governs the gTLDs; a role taken over from what was initially the responsibility of the United States government.[64] On recommendation from the World Intellectual Property Organization ("WIPO"), ICANN implemented its *Uniform Domain-Name Dispute-Resolution Policy* ("*UDRP*") on 1 December 1999.[65] The *UDRP* is carried out by ICANN-appointed service providers, as ICANN itself does not participate in the *UDRP* proceedings.[66] WIPO was the first service provider appointed to carry out the *UDRP*,[67] and currently remains appointed along with the National Arbitration Forum ("NAF")

---

domain name. See Sewchuk, *supra* note 29 at para. 45, citing (d)(2)(D)(I) of the *ACPA*.

60 Burshtein, *supra* note 13 at 6-14 and Freedman & Deane, *supra* note 15 at para. 132

61 Sewchuk, *supra* note 29 at para. 50.

62 R. Lynn Campbell, "Judicial Involvements in Domain Name Disputes in Canada" (2003-2004) 34 R.D.U.S. 373-421 at para. 3 (QL).

63 "ICANN Information", online: ICANN <http://www.icann.org/general>.

64 *Ibid.*

65 "Frequently Asked Questions: Internet Domain Names", online: WIPO <http://www.wipo.int/amc/en/center/faq/domains.html>.

66 "Uniform Domain Name Dispute Resolution Policy", online: ICANN <http://icann.org/dndr/udrp/policy.htm> at paras. 4(h) & 6 [*UDRP* Policy].

67 "Timeline for the Formulation and Implementation of the Uniform Domain-Name Dispute-Resolution Policy", online: ICANN <http://www.icann.org/udrp/udrp-schedule.htm>.

and the Asian Domain Name Dispute Resolution Center.[68] On receipt of a domain name complaint, the service provider appoints a panel from a publicly available list of panelists to ultimately decide the particular dispute.[69] It is up to the panel to decide the proceeding in a manner in accordance with the *UDRP* Policy and Rules so as to ensure that all parties are treated fairly and given equal opportunity to present their cases, to ensure the expediency of the proceedings, and to determine the admissibility, relevance, materiality, and weight of evidence.[70]

Procedure under the *UDRP*

A *UDRP* complaint is initiated when a complainant selects a service provider and submits a complaint in accordance with the *UDRP* Policy and Rules.[71] Paragraph 3(b) of the *UDRP* Rules provides for the details which must be submitted by the complainant. Some of these details include the complainant's preference towards a one- or three-person panel,[72] the domain names which are the subject of the complaint,[73] the registrars who registered the domain names,[74] and the trade-marks or service marks upon which the complaint is based.[75] The complainant must also describe the grounds on which the complaint is based[76] and the remedy sought.[77]

The service provider then reviews the complaint for administrative compliance, and if it is in compliance, forwards the complaint to the respondent,[78] who then has the opportunity to file a response. The service provider then appoints a panel to decide the case[79] and submit its final decision back to the service provider.[80]

Panels decide a case under the *UDRP* on the basis of the statements and documents submitted.[81] Generally, *UDRP* disputes are not held in person nor by teleconference, videoconference, or web

---

[68] "Approved Providers for Uniform Domain-Name Dispute-Resolution Policy", online: ICANN <http://www.icann.org/dndr/udrp/approved-providers.htm>.
[69] "Rules for Uniform Domain Name Dispute Resolution Policy", online: ICANN <http://www.icann.org/dndr/udrp/uniform-rules.htm> at para. 6 [*UDRP* Rules].
[70] *Ibid.* see paras. 10(a) through (d).
[71] *Ibid.* at para. 3(a).
[72] *Ibid.* at para. 3(b)(iv).
[73] *Ibid.* at para. 3(b)(vi).
[74] *Ibid.* at para. 3(b)(vii).
[75] *Ibid.* at para. 3(b)(viii).
[76] *Ibid.* at para. 3(b)(ix).
[77] *Ibid.* at para. 3(b)(x).
[78] *Ibid.* at para. 4(a).
[79] *Ibid.* at para. 6.
[80] *Ibid.* at para. 15(b).
[81] *Ibid.* at para. 15(a).

conference, unless the panel decides in its sole discretion that the dispute involves an exceptional matter and such a hearing is deemed necessary.[82]

The Claim under the *UDRP*

To be successful in a *UDRP* dispute, a complainant must prove three grounds on a balance of probabilities:

> i. [the registrant's] domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and
> ii. [the registrant has] no rights or legitimate interests in respect of the domain name; and
> iii. [the registrant's] domain name has been registered and is being used in bad faith. [83]

The *UDRP* provides guidance in terms of finding whether or not the above grounds have been established. For example, the *UDRP* provides that the panel deciding the case may look at, but is not limited to, the following factors when determining whether or not there has been bad faith on the part of the registrant:

> i. circumstances indicating that [the registrant has] registered or [has] acquired the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark or to a competitor of that complainant, for valuable consideration in excess of [the registrant's] documented out-of-pocket costs directly related to the domain name; or
> ii. [whether the registrant has] registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that [the registrant has] engaged in a pattern of such conduct; or
> iii. [whether the registrant has] registered the domain name primarily for the purpose of disrupting the business of a competitor; or

---

[82] *Ibid.* at para. 13.
[83] *UDRP* Policy, *supra* note 66 at para. 4(a).

> iv. by using the domain name, [whether the registrant has] intentionally attempted to attract, for commercial gain, Internet users to [the registrant's] web site or other on-line location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of [the registrant's] web site or location or of a product or service on [the registrant's] web site or location. [84]

The *UDRP* also provides guidelines as to whether or not the registrant had a legitimate interest in the domain name. In order to determine whether the registrant had a legitimate interest in the domain name, the *UDRP* provides that the panelists may consider, but are not limited to, a variety of factors, including whether:

> i. before any notice to [the registrant] of the dispute, [the registrant's] 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; or
> ii. [the registrant] (as an individual, business, or other organization) [has] 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 noncommercial 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. [85]

Remedies under the *UDRP*

Remedies available to the complainant under the *UDRP* are either the cancellation of the domain name or the transfer of the domain name to the complainant.[86] A "cancellation" results in the domain name registration being cancelled altogether, denying both the registrant and the complainant of the domain name. A "transfer" shifts the access of the domain name away from the registrant to the complainant. However, should either party wish to initiate further proceedings after a panel hands down its decision, it should be noted that *UDRP* decisions are not binding on the courts.[87]

---

[84] *Ibid.* at para. 4(b).
[85] *Ibid.* at para. 4(c).
[86] *Ibid.* at para. 4(i).
[87] Sewchuk, *supra* note 29 at para. 47.

The *UDRP* can potentially resolve a claim within 45 days.[88] Advantages of the *UDRP* system are that it is relatively fast, efficient, and cost effective, it does not impose a high evidentiary burden on parties, and it bypasses questions of jurisdiction.[89] Further, a remedy awarded to a complainant can also be completely carried out by the registrar without the need to further involve the registrant.[90]

The main limit of the *UDRP* is its inability to award certain remedies. *UDRP* complainants cannot recover costs or damages from bad-faith registrants.[91] This is especially detrimental where the complainants' goodwill has been compromised as a result of the domain name abuse.[92]

Arbitration of a dot-ca dispute: the CDRP

As previously noted, Canada has assumed the governance of the dot-ca domain space by establishing CIRA, a not-for-profit, non-governmental organization that sets policy for, manages, and operates the dot-ca domain database.[93] CIRA became the official dot-ca registry as of 1 December 2000,[94] and subsequently developed the *CIRA Dispute Resolution Policy* ("*CDRP*") to decide claims of bad-faith registration of dot-ca TLDs.[95] CIRA, which does not participate directly in *CDRP* proceedings,[96] appointed two service providers in June 2002[97] to administer the *CDRP*: the British Columbia International Commercial Arbitration Centre ("BCICAC") and Resolution Canada Inc.[98] Each provider provides a list of qualified and available candidates who may serve as the panelists in deciding *CDRP* claims.[99]

---

88 *Ibid.* at para. 43.
89 Cheng & Katul, *supra* note 12 at 511-512.
90 *Ibid.*
91 *Ibid.*
92 *Ibid.*
93 "CIRA FAQ", online: CIRA <http://www.cira.ca/en/faq-menu7.html>.
94 *Ibid.*
95 CIRA Polices, Rules and Procedures, "CIRA Domain Name Dispute Resolution Policy," version 1.1, online: CIRA <http://www.cira.ca/en/documents/q4/CDRP_Policy_2003-12-04_en_final.pdf> at para. 1.1 [*CDRP* Policy].
96 *Ibid.* at para. 1.6.
97 Cheng & Katul, *supra* note 12 at 487.
98 "Dispute Resolution Service Providers", online: CIRA <http://cira.ca/en/cat_dpr_providers.html>.
99 "CIRA Domain Name Dispute Resolution Rules," version 1.2, online: CIRA <http://www.cira.ca/en/documents/q4/CDRP_Rules_2003-12-04_en_final.pdf> at para. 6.1 [*CDRP* Rules].

Procedure under the *CDRP*

A complaint is initiated by a complainant first selecting a service provider and submitting the necessary information to establish a complaint under the *CDRP*.[100] For example, the details that complainants must specify or identify include: each domain name registration which is the subject of the complaint,[101] the basis on which the complainant satisfies the CPR,[102] the registrar of the domain name(s),[103] the marks on which the complaint is based,[104] and the particulars of the basis of the complaint.[105] The complainant must also specify the remedy sought,[106] and provide a summary and references to any relevant Canadian law,[107] CIRA, or other dispute resolution proceedings.[108]

The service provider then reviews the complaint,[109] and once satisfied that the complaint complies with *CDRP* Policy and Rules, sends notice to the registrant.[110] The registrant then has an opportunity to respond to the complaint.[111] The requirements of what must be included in the response are similar to the requirements of what must be included in the complaint[112]; however, the registrant does have the option of claiming up to $5,000 in costs.[113] Again, the service provider will review the response[114] and promptly send notice to the complainant once satisfied that the response complies with the *CDRP* policy and rules.[115] The panel is then appointed to decide the case and forward its ultimate decision to the service provider.[116]

A decision under the *CDRP* is based purely on submission; no in-person hearing, teleconference, videoconference, or web-conference is

---

100 *Ibid.* at para. 3.1 and *CDRP* Policy, *supra* note 95 at para. 2.1.
101 *CDRP* Rules, *ibid.* at para. 3.2(e).
102 *Ibid.* at para. 3.2(f).
103 *Ibid.* at para. 3.2(g).
104 *Ibid.* at para. 3.2(h).
105 *Ibid.* at para. 3.2(i).
106 *Ibid.* at para. 3.2(j).
107 *Ibid.* at para. 3.2(l).
108 *Ibid.* at para. 3.2(m).
109 *Ibid.* at para. 4.1.
110 *Ibid.* at para. 4.3.
111 *Ibid.* at para. 5.1.
112 *Ibid.* at para. 5.2 generally.
113 *Ibid.* at para. 5.2(h).
114 *Ibid.* at para. 5.5.
115 *Ibid.* at para. 5.7.
116 *Ibid.* at para. 12.2.

used.[117] It is estimated that it takes a *CDRP* panel 60 to 90 days to decide a dispute.[118]

The Claim under the *CDRP*

Bringing a cybersquatting claim under the *CDRP* is similar to bringing a claim under the *UDRP*; however, differences do exist. A key difference in initiating a claim under the *CDRP* is the complainant's first step of satisfying the Canadian Presence Requirements ("CPR"). Like the CPR that an applicant must satisfy in order to register a domain name, a complainant must also first satisfy the CPR to bring a claim under the *CDRP*.[119] The CPRs require that the complainant be a Canadian citizen, permanent resident, or corporation.[120] Provisions are also made for Canadian trusts, partnerships, associations, government, and Aboriginal persons.[121] A claimant not meeting the CPR but who has registered a trade-mark in Canada will also be eligible.[122]

A claimant satisfying the CPRs must then be able to establish the three main grounds which form the basis of a *CDRP* complaint:

> a) the Registrant's dot-ca domain name is Confusingly Similar to a Mark in which the Complainant had Rights prior to the date of registration of the domain name and continues to have such Rights;
> b) the Registrant has no legitimate interest in the domain name as described in paragraph 3.6 [of the *CDRP* Policy]; and
> c) the Registrant has registered the domain name in bad faith as described in paragraph 3.7 [of the *CDRP* policy].[123]

The burden lies on the complainant to prove the "confusingly similar" and the "bad faith" requirements on a balance of probabilities. However, the complainant need only present *some* evidence of "no

---

117 Unless the panel in its sole discretion and as an exceptional matter determines otherwise. *CDRP* Rules, *ibid.* at para. 11.3.

118 "CIRA Dispute Resolution Policy (CDRP) FAQ", online: CIRA <http://www.cira.ca/en/cat_dpr_faq.html#q103> [*CDRP* FAQ].

119 *CDRP* Policy, *supra* note 95 at para. 1.4.

120 CIRA Policies, Rules and Procedures, "Canadian Presence Requirements for Registrants," version 1.3, online: CIRA <http://www.cira.ca/en/documents/q3/CanadianPresenceRequirementsForRegistrants-EffectiveDateJune52003.pdf> at para. 2 [CPR].

121 *Ibid.*

122 *Ibid.* at para. 2(q).

123 *CDRP* Policy, *supra* note 95 at para. 3.1.

legitimate interest." The onus then shifts to the registrant to prove that he or she has a legitimate interest in the domain name on a balance of probabilities.[124]

The *CDRP*, like the *UDRP*, sets out what factors the panel must consider in determining whether or not the three required grounds have been proven. The *CDRP* has gone one step further than the *UDRP*, as it provides more than "guidelines" for the deciding panel. Rather, the *CDRP* provides *exhaustive* lists of grounds which limit the factors a panel can consider. First, the *CDRP* Policy provides six exhaustive factors for which a registrant's legitimate interest in the domain name in question can be found. To prove a legitimate interest in the domain name, para. 3.6 of the *CDRP* Policy holds that the registrant has a legitimate interest in the domain name if and only if:

> a) the domain name was a Mark, the Registrant used the Mark in good faith and the Registrant had Rights in the Mark;
> b) the Registrant used the domain name in Canada in good faith in association with any wares, services or business and the domain name was clearly descriptive in Canada in the French or English language of: (i) the character or quality of the wares, services or business; (ii) the conditions of, or the persons employed in, production of the wares, performance of the services or operation of the business; or (iii) the place of origin of the wares, services or business;
> c) the Registrant used the domain name in Canada in good faith in association with any wares, services or business and the domain name was understood in Canada to be the generic name thereof in any language;
> d) the Registrant used the domain name in Canada in good faith in association with a non-commercial activity including, without limitation, criticism, review or news reporting;
> e) the domain name comprised the legal name of the Registrant or was a name, surname or other reference by which the Registrant was commonly identified; or
> f) the domain name was the geographical name of the location of the Registrant's non-commercial activity or place of business.

Secondly, panels are also limited to considering the following grounds when considering whether the registrant has acted in bad faith.

---

[124] *Ibid.* at para. 4.1.

Looking to para. 3.7 of the *CDRP* Policy, bad faith can be found if and only if:

a) the Registrant registered the domain name, or acquired the Registration, primarily for the purpose of selling, renting, licensing or otherwise transferring the Registration to the Complainant, or the Complainant's licensor or licensee of the Mark, or to a competitor of the Complainant or the licensee or licensor for valuable consideration in excess of the Registrant's actual costs in registering the domain name, or acquiring the Registration;
b) the Registrant registered the domain name or acquired the Registration in order to prevent the Complainant, or the Complainant's licensor or licensee of the Mark, from registering the Mark as a domain name, provided that the Registrant, alone or in concert with one or more additional persons has engaged in a pattern of registering domain names in order to prevent persons who have Rights in Marks from registering the Marks as domain names; or
c) the Registrant registered the domain name or acquired the Registration primarily for the purpose of disrupting the business of the Complainant, or the Complainant's licensor or licensee of the Mark, who is a competitor of the Registrant.

Remedies under the *CDRP*

Like the *UDRP*, the remedies available to a successful complainant under the *CDRP* are cancellation of a domain name or transfer of the domain name to the complainant.[125] Also as under the *UDRP*, the panel's decision under the *CDRP* is neither final nor binding on the courts.[126] The advantages and disadvantages of the *CDRP* system are similar to those noted for the *UDRP* system above. However, a more detailed discussion of the efficiencies and deficiencies of the *CDRP* is to follow.

[125] *Ibid.* at para. 4.3.
[126] Campbell, *supra* note 62 at para. 51.

Differences between the CDRP and the UDRP

Although the *CDRP* and *UDRP* policies are similar, many differences are apparent. For example:

- **The *CDRP* is a "closed" system.** *CDRP* complainants must satisfy the Canadian Presence Requirements ("CPR"), while *UDRP* complainants do not have a comparable obligation.[127] Seemingly, anyone can initiate a claim under the *UDRP*, regardless of geographical ties.
- **The *CDRP* defines key terms.[128]** The *CDRP* Policy defines terms such as "mark," "rights," and "use," while the *UDRP* Policy leaves interpretation completely up to panelists.[129]
- **The *CDRP* gives less deference to arbiters.** The interpretation and scope of the *CDRP* Policy is less flexible, as its grounds for finding bad faith and legitimate interest are exhaustive. The *UDRP* does not seem to impose such limits on the number of grounds on which bad faith or legitimate interest can be proved.[130]
- **The *CDRP* is harsh on bad complainants.** Unlike the *UDRP*, a key departure of the *CDRP* is that it provides for a $5,000 fine for complainants who initiate proceedings in bad faith.[131] A bad faith complainant is one who unfairly and without colour of right attempts to cancel or transfer a registration.[132]
- **The *CDRP* requires the complainant to have prior rights to the mark.** The *CDRP* requires that the complainant had rights to its mark *prior* to the registration of the offending domain name.[133] The *UDRP* does not specifically provide for this.
- **The *CDRP* uses mandatory three-adjudicator panels.** The *CDRP* imposes mandatory three-person panelists to decide the complainant's case, unless there is no response from the registrant.[134] The *UDRP* on the other hand gives the complainant the choice of proceeding with either one or three panelists.[135]

---

127 *CDRP* FAQ, *supra* note 118. Also see Burshtein, *supra* note 13 at 7-126.
128 *Ibid.*
129 Burshtein, *supra* note 13 at 7-126.
130 *CDRP* FAQ, *supra* note 118.
131 Cheng & Katul, *supra* note 12 at 517.
132 *CDRP* Policy, supra note 95 at para. 4.6.
133 *Ibid.* at para. 3.1(a).
134 If the Registrant does not respond to the case, the Complainant may elect to have its case heard by a single panelist. See *CDRP* Rules, *supra* note 99 at para. 5.8.
135 *UDRP* Rules, *supra* note 69 at para. 3(b)(iv).

- **The *CDRP* allows more time for appeal.** Under the *CDRP*, the decision of the panel is implemented by CIRA after 60 days.[136] Under the *UDRP*, the panel's decision is implemented by ICANN after 10 days.[137]
- **The *CDRP* does not allow for supplemental rules.** *CDRP* service providers are not entitled to implement their own supplemental rules,[138] whereas *UDRP* service providers are.[139] The term "Supplemental Rules," as defined by the *UDRP* Rules, "means the rules adopted by the provider administering the proceeding to supplement these [*UDRP*] Rules," and includes topics such as fees, word and page limits, and means of communication.[140]

Trends in the CDRP decisions[141]

As of 1 August 2007, 80 cases have been decided under the *CDRP*.[142] The majority have been decided by the BCICAC (57 cases) as opposed to Resolution Canada Inc. (21 cases).[143] The complainants were successful in 63 (approximately 78.75%) of those cases. Transfers of the disputed domain names were granted in 62 of the successful cases, while only one case resulted in the cancellation of the domain name.[144] It is also interesting to note that in 47 cases (approximately 58.75%), the registrant failed to file a response to the claim. However, even where the registrant did not file a response, the panel was nevertheless charged with the duty of assessing the integrity and credibility of the evidence as

---

136 *CDRP* Policy, *supra* note 95 at para. 4.5.
137 *UDRP* Policy, *supra* note 66 at para. 4(k).
138 *CDRP* Rules, *supra* note 99 at para. 1.7.
139 *UDRP* Rules, *supra* note 69, preamble.
140 *Ibid.* at para. 1, "Definitions."
141 The figures presented are updated statistics from the study conducted in Antonio Turco, "Domain Name Dispute Resolution Under the CDRP—the First Five Years" (11 November 2006), online: Blakes, Cassels & Graydon LLP <http://www.blakes.com/english/view_disc.asp?ID=194>.
142 As posted on the CIRA website on 1 August 2007. Decisions are numbered 00001 through 00080. Note that decision 00050 seems to be missing. All CIRA decisions referred to were found at "Dispute Resolution Decisions", online: CIRA <http://www.cira.ca/en/cat_dpr_decisions.html>.
143 Note that in the case of *Air Products Canada Ltd./Prodair Canada Ltée v. Index Quebec Inc.*, CIRA Decision No. 00007 (15 April 2003), it was not specified with which service provider the claim was filed.
144 *The Toronto-Dominion Bank v. TM WatchDog*, CIRA Decision No. 00048 (15 December 2005). Cancellation, as opposed to a transfer of the domain name to the complainant, was ordered because the domain name in question was comprised of two marks, one of which, the panel found, the complainant itself did not have rights in. Also see the discussion in Turco, *supra* note 141.

disclosed by the complainant.[145] To date, the panels have yet to find a "bad faith" complainant.

CRITICISMS OF THE *CDRP*

Certain critics have argued that the *CDRP* is "stacked against"[146] trade-mark holders and therefore is "frequently not helpful from a brand owner's perspective."[147] Their claims might be based on the following grounds:

- **Inconsistency:** panels do not apply a consistent test to determine whether a domain name is "confusingly similar" to the complainant's mark, as some panels employ a traditional trade-marks "confusion" test, others adopt a "resemblance" test, and some panels consider both.[148]
- **High thresholds:** the test for bad faith under the *CDRP* is harder to satisfy than the test employed in traditional trade-mark cases, as the *CDRP* requires bad faith intention of the registrant to be proved, while trade-mark law looks not to intention, but only to the effect of the registration.[149]
- **Exhaustiveness:** for example, the grounds for finding bad faith grounds on which the complainant can prove its claim are limited.[150]
- **Lack of availability:** the Canadian Presence Requirements are restrictive, as they do not allow foreigners who have Canadian trade-mark rights, but who otherwise do not fulfill the requirements, to commence a proceeding.[151] For example, this might include a foreigner who has not registered a trade-mark in Canada but who has trade-mark rights at common law.[152]
- **Legitimate interest override:** if a panel finds that the registrant had a legitimate interest in the disputed domain name, a complainant

---

[145] *Browne & Co. Ltd./Ltée v. Bluebird Industries*, CIRA Decision No. 00002 (22 October 2002) at 7.
[146] Robert H. Barrigar & Irene M. Waller, "COMMENTARY: litigation may work better than ADR for trade-mark owners" *The Lawyer's Weekly* 25:12 (22 July 2005) (QL).
[147] John McKeown, "Cases demonstrate importance of quickly securing domain names" *The Lawyer's Weekly* 25:37 (10 February 2006) (QL).
[148] See Turco, *supra* note 141. Also see the related discussion in Burshtein, *supra* note 13 at 7-37 – 7-38.
[149] Barrigar & Waller, *supra* note 146.
[150] Burshtein, *supra* note 13 at 7-127.
[151] *Ibid.* at 7-10.
[152] *Ibid.*

> cannot succeed, despite the fact that it can prove confusing similarity and bad faith.[153]

While the above examples do indeed present hurdles to the functioning of the *CDRP*, recent decisions suggest that these problems are more theoretical than practical. Perhaps these criticisms are not quite the problems they are made out to be and thus, the *CDRP* may not be as stacked against the brand owner as sometimes alleged.

Inconsistency

It is true that panels do not apply a consistent test in determining whether a domain name is "confusingly similar" to the complainant's mark. Although "confusingly similar" is defined in the *CDRP* Policy,[154] it is ultimately up to the panels themselves to decide the standard by which confusing similarity should be found. For example, in *Musician's Friend, Inc. v. Robert Piperni*,[155] the panel decided the correct approach would be to apply all the factors used for determining "confusion" under s. 6(5) of the *Trade-marks Act*.[156] This includes looking at:

> (a) the inherent distinctiveness of the trade-marks or trade-names and the extent to which they have become known;
> (b) the length of time the trade-marks or trade-names have been in use;
> (c) the nature of the wares, services or business;
> (d) the nature of the trade; and
> (e) the degree of resemblance between the trade-marks or trade-names in appearance or sound or in the ideas suggested by them.

However, the most consistently applied test is the "resemblance" test articulated in *Government of Canada, on behalf of Her Majesty the Queen in Right of Canada v. Bedford in his own name and doing business*

---

153 Turco, *supra* note 141. Also see Burshtein, *supra* note 13 at 7-127.
154 "A domain name is 'Confusingly Similar' to a Mark if the domain name so nearly resembles the Mark in appearance, sound or the ideas suggested by the Mark as to be likely to be mistaken for the Mark." *CDRP* Policy, *supra* note 95 at para. 3.4.
155 CIRA Decision No. 00075 (February 2007).
156 *Ibid.* at 3. The s. 6(5) test was also adopted in *The Hartz Mountain Corporation v. Robert Harwin*, Decision No. 00078 (June 2007) and *Enterprise Rent-A-Car Company v. Ebenezer Thevasagayam,* CIRA Decision No. 00043 (22 August 2005).

as Abundance Computer Consulting,[157] which considers whether a person knowing of the complainant's mark but having an imperfect recollection of it would, on a first impression, likely mistake the domain name for the complainant's mark based on the appearance, sound, or idea suggested by the mark.[158] Although panels are not bound to use this test, there is a prominent trend in panels applying it. Over the course of the CIRA decisions rendered, numerous panels have cited *Government of Canada*, or have otherwise set out the above test. Even early on in the line of *CDRP* decisions, the panel in *Canadian Thermos Products Inc. v. Michael Fagundes*[159] noted that the resemblance test had been the test adopted in a clear majority of cases.[160] To date, at least 22 *CDRP* cases have adopted the resemblance test.[161] Therefore, in the future of *CDRP* decisions, it appears that the inconsistency in tests used to determine

---

[157] CIRA Decision No. 00011 (27 May 2003).
[158] *Ibid.* at para. 66.
[159] CIRA Decision No. 00049 (18 January 2006).
[160] *Ibid.* at para. 26.
[161] For example, see *McKee Homes Ltd. v. Gerlinde Honsek*, CIRA Decision No. 00079 (25 June 2007); *GoDaddy.com, Inc. v. Jan Ladwig*, CIRA Decision No. 00077 (12 April 2007); *Yellow Pages Group Co. v. Coolfred Co.*, CIRA Decision No. 00076 (13 March 2007); *Musician's Friend, Inc. v. L.A. Music*, CIRA Decision No. 00074 (16 February 2007); *Trailwest Online Inc. v. Talltech Systems Inc.*, CIRA Decision No. 00073 (9 February 2007); *Craiglist, Inc. v. Daniel Cox*, CIRA Decision No. 00072 (23 January 2007); *The Black & Decker Corporation v. J. Chapnik Trust—(100%)*, CIRA Decision No. 00069 (15 November 2006); *Sam Ash Music Corporation v. LAMUSIC*, CIRA Decision No. 00067 (15 October 2006); *Alberta Alcohol and Drug Abuse Commission v. Akshay Khanna*, CIRA Decision No. 00065 (12 October 2006); *Choice Hotels International, Inc. and Choice Hotels Canada Inc. v. Daniel Cox*, CIRA Decision No. 00061 (18 September 2006); *911979 Alberta Inc. v. Hank Morin*, CIRA Decision No. 00060 (25 August 2006); *The Co-operators Group Ltd. v. Artbravo Inc.*, CIRA Decision No. 00055 (6 April 2006); *Canadian Thermos Products Inc. v. Michael Fagundes*, CIRA Decision No. 00049 (18 January 2006); *Bell Canada v. Archer Enreprises*, CIRA Decision No. 00038 (30 August 2005); *Fresh Intellectual Properties Inc. v. Sweets and Treats*, CIRA Decision No. 00033 (9 June 2006); *DRN Commerce Inc. v. REPO DEMO (TM), Park and Sell of Canada Limited*, CIRA Decision No. 00030 (29 April 2005); *Glaxo Group Limited v. Defining Presence Marketing Group Inc. (Manitoba)*, CIRA Decision No. 00020 (26 August 2004); *Amazon.com Inc. v. David Abraham*, CIRA Decision No. 00018 (28 July 2004); *Coca-Cola Ltd. v. Amos B. Hennan*, CIRA Decision No. 00014 (28 October 2003); *Acrobat Construction/Entreprise Management Inc. v. 1550507 Ontario Inc.*, CIRA Decision No. 00013; *Government of Canada, on behalf of Her Majesty the Queen in Right of Canada v. David Bedford in his own name and doing business as Abundance Computer Consulting*, CIRA Decision No. 00011 (27 May 2003); *Canadian Broadcasting Corporation/Société Radio-Canada v. William Quon*, CIRA Decision No. 00006 (8 April 2003). Also see the related discussion in Burshtein, *supra* note 13 at 7-41 – 7-45.

"confusing similarity" does not represent a significant hurdle, as the application of the resemblance test has proved to be the popular choice.

Although it has been stated that the narrower, "confusion" tests will favor respondents and the more liberal "resemblance" test will favour complainants,[162] in many disputes, the outcome of the decision will be unaffected regardless of the test applied. The reasons for this are two-fold. First, a good number of domain name disputes involve domain names that are *identical* to the complainant's mark. For example, in *Viacom International Inc. v. Harvey Ross Enterprises, Ltd.*,[163] the domain name in question was <mtv.ca>, which was *identical* to the complainant's "MTV" trade-mark. In such cases where the domain name is identical to the complaint's mark, "confusing similarity" will automatically be found. As put by one panel, "[a] registrant cannot avoid confusion by appropriating another party's entire mark in a domain name."[164]

Secondly, many disputes involve domain names containing merely a *slight difference* from the complainant's mark. In those cases, "confusing similarity" is automatically found as well. For example, in *Choice Hotels International Inc. v. Mr. Daniel Montanbault*,[165] the complainant had rights in the mark "COMFORT INN" and the domain name in dispute was <comfort-inn.ca>. The panel in that case held that "[t]he presence or absence of a 'dash' is not such a difference as to differentiate the domain name from the marks in the mind of the average Internet user with imperfect recollection."[166] This principle was in fact established early on in the *CDRP* line of decisions in *Canadian Broadcasting Corporation/Société Radio-Canada v. William Quon*.[167] The complainant in that case had rights to the mark "RADIO-CANADA" and the domain name in question was <radiocanada.ca>. The panel established that "the absence of punctuation marks, such as hyphens, does not alter the fact that a domain name is identical to a mark[.]"[168] Other cases have also held that the absence of an apostrophe or addition of an "s" to a domain name is insufficient to distinguish the domain name from the mark.[169]

In sum, inconsistency may not be that big of a problem, both due to the popular adoption of the "resemblance" test and given that in a

---

[162] *Franchizit Corporation v. 984308 Ontario Inc.*, CIRA Decision No. 00021 (5 August 2004) at para. 19.
[163] CIRA Decision No. 00015 (15 October 2003).
[164] *Alberta Alcohol and Drug Abuse Commission v. Akshay Khanna*, CIRA Decision No. 00065 (12 October 2006) at para. 37.
[165] CIRA Decision No. 00062 (20 September 2006).
[166] *Ibid.* at para. 23.
[167] CIRA Decision No. 00006 (8 April 2003).
[168] *Ibid.* at 11.
[169] For example, see *Musician's Friend, Inc. v. L.A. Music*, *supra* note 161 at 7.

significant number of cases the selection of a test will be irrelevant, as confusing similarity will be found under any test.

High Thresholds

As for the test of bad faith, it may be that the test under the *CDRP* may be harder to satisfy than under traditional trade-mark law, and cases have indeed been dismissed for failing to fulfill the bad faith requirement.[170] This high threshold was highlighted in *Caseware International Inc., c/o Mr. Alan Charlton v. Mr. John Lee*,[171] where the panel expressly pointed out that the *CDRP* requires not just that the *effect* of the registrant's registration and use of the domain name disrupt the business of its competitor, but that the *primary purpose* of the registration is to disrupt the business of its competitor.[172]

Although the test is stringent, one must keep in mind the purpose of the *CDRP*, which is not to remedy *every* domain name dispute, but rather is to provide for a speedy, low-cost way to remedy cases of blatant cybersquatting.[173] Where more complicated issues concerning domain names are in dispute, the court remains the appropriate vehicle in which to settle the dispute.[174]

Exhaustiveness

Bad faith may indeed be a hurdle for complainants to overcome, especially if it cannot be proven on one of the pre-determined grounds

---

[170] See for example *American Multi-Cinema Inc. v. Dan J. Kapuscinski*, CIRA Decision No. 00025 (8 February 2005) at para. 35.

[171] CIRA Decision No. 00057 (20 August 2006).

[172] *Ibid.* at para. 24.

[173] See for example *Cheap Tickets & Travel Inc. v. Emall.ca Inc.*, CIRA Decision No. 00004 (31 January 2003) at para. 16, where the panel noted that the scope of the policy is narrow and applies only to cases of cybersquatting and not to other kinds of disputes between trade-mark owners and domain name registrants.

[174] For example, in *Clover Gifts, Inc. v. George Morrision, G M Consulting Services*, CIRA Decision No. 00041 (4 October 2005), the panel noted that the *CDRP* was not the appropriate forum under which to examine issues of infringement or historical rights in a trade-mark [at para. 25]. It noted that it was not the appropriate forum to resolve what seemed to be an "ongoing dispute with many layers between the parties" [at para. 29]. However, note the recent decision of *Vessel Assist Association of America, Inc. v. Michael MacKenzie*, CIRA Decision No. 00080 (31 July 2007) at 9 & 10, in which the majority members entertain the possibility that in a narrow class of cases, such as cases where it is fairly obvious that CIPO may have erred in registering a trade-mark, the panel might have to consider the validity of a registered trade-mark in order to decide whether or not it will transfer or cancel a domain name. The decision in that case, however, did not turn on this discussion.

set out in the Policy. In *Independent Order of Foresters v. Noredu Enterprises Canada Inc., operating as Forester College of Technology*,[175] the panel highlighted that the clear limiting language "if and only if" in the definition of bad faith makes it clear that the scope of the necessary bad faith is intended to be strictly construed.[176]

However, we may see that panels might be beginning to move away from such a strict application. Recently, in the decision of *Alberta Alcohol and Drug Abuse Commission v. Akshay Khanna*,[177] the panel held that "paragraph 3.7(b) of the Policy should be given an expansive interpretation that is consistent with the intention of the Policy to provide redress from abusive domain name registrations."[178] In that case, it was speculated that a narrow interpretation of the *CDRP* Policy would not provide for redress from "typosquatting" (where cybersquatters register intentional misspellings of a mark) or where registrants register a domain name which would otherwise not appeal to the mark owner.[179] The panel held that not providing for redress from the above could not have been the intention of the Policy.[180]

Therefore, although it cannot be denied that strict, exhaustive grounds are required by the policy, it seems possible that future panels might take the scope of bad faith into their own hands, especially in cases where not finding bad faith would seem to defeat the intention of the *CDRP* Policy.

Lack of availability

The purpose of the Canadian Presence Requirements is to ensure that the dot-ca domain space "be developed as a key public resource for the social and economic development of all Canadians."[181] To ensure this purpose, the *CDRP* does restrict who can initiate a claim under the system. However, a finding that a complainant does not satisfy the CPR might not be fatal to the case, as para. 4.3 of the *CDRP* Policy holds that where the complainant is successful but does not satisfy the CPR, the domain name may be transferred to a nominee of the complainant. In *Best Western International, Inc. v. Daniel Montanbault,* this more flexible application of the CPR was applied, as the panel deemed that the complainant was entitled to name a nominee to CIRA who did satisfy the requirements.[182]

---

175 CIRA Decision No. 00017 (25 May 2004).
176 *Ibid.* at para. 37.
177 CIRA Decision No. 00065 (12 October 2006).
178 *Ibid.* at para. 49.
179 *Ibid.* at para. 50.
180 *Ibid.* at para. 53.
181 CPR, *supra* note 120 at para.1.
182 CIRA Decision No. 00070 (23 January 2007) at 20.

While the application of para. 4.3 of the *CDRP* Policy does not by any means do away with the CPR, it does show some degree of leniency in terms of who may proceed under the *CDRP*.

One panel has taken an even more flexible interpretation of the CPR. In *PPL Legal Care of Canada Corporation v. Curtis Patey*,[183] the mark in dispute was a trade name. The complainant was not the owner of the trade name; rather, it was the complainant's parent corporation that owned the name. The panel held that this was not fatal to the claim, as the wording of the CPR provisions does not require that the mark be used in Canada by the complainant *specifically*, but just generally "by a person." The use of the trade name in Canada by the parent corporation was thus sufficient to fulfill the CPR in that panel's determination.

Legitimate Interest Override

As currently defined in the *CDRP* Policy, a finding that a registrant had a legitimate interest in registering a domain name will trump findings of confusing similarity and bad faith. However, the danger may be more theoretical than practical. One author has noted that as of November 2006, no *CDRP* panel yet has had to use a finding of legitimate interest to justify denying the claims of a complainant.[184] Since this time, no panel has used a finding of legitimate interest to trump a finding of bad faith resulting in the dismissal of the claim. In fact, some panels, after having found that no bad faith could be established, did not even go on to consider whether or not the registrant had a legitimate interest in the domain name.[185]

DOT-CA PROTECTION: HOW DOES THE *CDRP* MEASURE UP?

THE CONCLUSIONS ABOVE are responses to some of the familiar criticisms of the *CDRP*. However, although these criticisms are not necessarily fatal to the operation of the *CDRP*, this by no means

---

183 CIRA Decision No. 00056 (24 April 2006).

184 Turco, *supra* note 141.

185 For example, see *Canadian Thermos Products Inc. v. Michael Fagundes*, CIRA Decision No. 00049 (18 January 2006); *The Toro Company, Bloomington MN, USA v. Pierre Hannon, Laval QC, Canada*, CIRA Decision No. 00039 (25 August 2005); *American Multi-Cinema Inc. v. Dan J. Kapuscinski*, CIRA Decision No. 00025 (8 February 2005); *Independent Order of Foresters v. Noredu Enterprises Canada Inc., operating as Forester College of Technology*, CIRA Decision No. 00017 (25 May 2004); *Trans Union LLC v. 1491070 Ontario Inc.*, CIRA Decision No. 00008 (23 April 2003).

eliminates the concerns raised above. Further, the conclusions above were drawn strictly from looking to the posted CIRA decisions; this paper does not attempt to analyze what types of parties are choosing to file, or not to file, a *CDRP* complaint. While from a practical standpoint the above concerns do not necessarily pose significant threats to brand holders, from a theoretical perspective, as long as *CDRP* decisions are not binding, many of the above criticisms will perpetually exist. The *CDRP*, as will be shown below, may have improved on the *UDRP* model in some respects, but could still stand to benefit from further improvements.

How the CDRP has improved the UDRP model

CIRA had the benefit of almost a year's worth of *UDRP* experience before implementing the *CDRP*.[186] It therefore had the ability to improve the *UDRP* model in numerous ways.

First, the *UDRP* has been criticized in that it allows complainants the choice of having their case decided by either a one-person or a three-person panel. One author conducted a study and found that the number of panelists affects the outcome of the case; in particular, that single-person panels are more complainant friendly.[187] This may therefore cause complainants to choose single-person panels in order to increase their chances of success. Critics have therefore suggested that the *UDRP* make a three-person panel the mandatory default in order to increase the parties' perception of fairness of the system.[188] The *CDRP* seems to have addressed this concern by requiring that three-person panels decide all cases where the registrant files a response.[189]

It has also been suggested that a concern of "forum shopping" arises under the *UDRP* as the various ICANN-appointed service providers are allowed to implement their own set of supplemental rules.[190] As mentioned previously, the *CDRP* does not allow its service providers to implement their own supplemental rules thereby mitigating the temptation for complainants to shop around.

Secondly, another author has suggested that to make the *UDRP* system complete, measures to forcibly combat reverse hijacking—or bad-faith complainants—should be employed.[191] The *CDRP* also seems to have taken this deficiency into account by providing a major safeguard against complainants who initiate claims in bad faith. Under the *CDRP*, a

---

[186] *CDRP* FAQ, *supra* note 118.
[187] Michael Geist, "Fair.com?: An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP" 27 Brook. J. Int'l. L. 903 at 922.
[188] Patrick D. Kelley, "Emerging patterns in Arbitration Under the Uniform Domain-Name Dispute-Resolution Policy" 17 Berkeley Tech. L.J. 181 at 203-204.
[189] *CDRP* FAQ, *supra* note 118.
[190] Geist, *supra* note 187 at 905-910.
[191] Walker, *supra* note 16 at 310.

finding of bad faith on the part of the complainant may result in a $5,000 fine and an inability to bring further proceedings until the fine is paid.[192] This ensures that the *CDRP* itself is not used as a vehicle for fraud.

What the CDRP can still learn from the UDRP model

One concern is that CIRA does not implement orders for transfer or cancellation of domain names until 60 days after decisions are handed out, while ICANN implements its orders after 10 days. Although the 60 days provides a party with time to appeal a decision,[193] a 60-day waiting period could be disastrous in certain situations. For example, consider the scenario previously alluded to, where loss of a domain name could result in a significant loss of revenue. One author, however, does suggest that the *UDRP*'s 10-day implementation period might be one of the reasons limiting the usefulness of appealing panel decisions to the courts.[194] Therefore, CIRA might want to strike some middle ground between the 10- and 60-day implementation periods. This is perhaps what the authority that governs the dot-eu space has considered by allowing a 30-day implementation period.[195]

An additional concern is that the *CDRP* might not be as facilitative as the *UDRP* to corporate growth. Unlike the *CDRP*, the *UDRP* does not specifically require a complainant to have rights in its mark *prior* to the offending domain name registration. Although it may be difficult to find bad faith when a complainant has no prior rights, this may be a significant factor to consider in a case where a cybersquatter registers a domain name that is confusingly similar to an anticipated future trade-mark.[196] This often occurs, for example, following the merger of two companies.[197] The *CDRP* may thus be deficient in safeguarding the rights of highly anticipated marks.

How the CDRP can further stand to improve

Further improvements need to be made to the *CDRP* as the dot-ca continues to grow strong. Dot-ca's may soon surpass the one million

---

192 Cheng & Katul, *supra* note 12 at 517.
193 *CDRP* FAQ, *supra* note 118.
194 Kelley, *supra* note 188 at 191.
195 ".eu Alternative Dispute Resolution Rules", online: ADR.eu <http://www.adreu.eurid.eu/html/en/adr/adr_rules/eu%20adr%20rules.pdf> at para. 12(d).
196 "WIPO Overview of WIPO Panel Views on Selected UDRP Questions", online: WIPO <http://www.wipo.int/amc/en/domains/search/overview/index.html> at 1.4.
197 *Ibid.* at 3.1.

mark, as there are currently over 800,000 dot-ca domain names registered with CIRA.[198] Increasing the certainty and consistency of the *CDRP* should therefore be a priority. CIRA might thus consider defining more terms in the *CDRP* Policy in order to put some of the criticisms to rest. Although already defined in the *CDRP*, a prime candidate for reconsideration would be the definition of "confusingly similar." Although a popular test has been adopted in determining the standard to which "confusing similarity" must be met, the test still has somewhat inconsistent application. Defining a test or standard, or establishing exhaustive grounds within the *CDRP* Policy itself, for which confusing similarity can be found, would help to inject more certainty and consistency into the system.

Another term that could stand to be defined is the term "competitor," as the interpretation of the term is essential to a finding of bad faith under para. 3.7(c) of the *CDRP* Policy. Under that paragraph, the registrant must be a competitor of the complainant in order for bad faith to be found where the domain name was registered primarily for the purpose of disrupting the business of the complainant. The cases show that "competitor" can either be interpreted narrowly (i.e. the registrant is a business competitor of the complainant) or more liberally (i.e. the registrant is merely someone who acts in opposition to the complainant).[199] Some decisions have highlighted that a consistent interpretation of "competitor" has yet to be adopted,[200] while others have specifically suggested that the narrow interpretation should be adopted. For example, in *Trans Union LLC v. 1491070 Ontario Inc.*,[201] the panel held that the term "competitor" should be given a narrow interpretation because otherwise registrants would be found to have disrupted the business of the complainant in too many cases.[202] Other panels have held that "disrupting the business of a competitor" is simply satisfied where the domain name creates a likelihood of confusion for end users as to affiliation or sponsorship.[203] As the interpretation selected could

---

198 As at 10 July 2007, online: CIRA <http://www.cira.ca/en/home.html>.

199 *Sam Ash Music Corporation v. LAMUSIC*, CIRA Decision No. 00067 (15 October 2006). Also see the related discussion in Burshtein, *supra* note 13 at 7-64 – 7-69.

200 See *Canadian Thermos Products Inc. v. Michael Fagundes*, CIRA Decision No. 00049 (18 January 2006), where the panel highlights the distinction between the narrow and liberal interpretations and the rationales for supporting one over the other. The case did not reach a decisive opinion on which is the appropriate interpretation to be used, as either way the complainant could not prove the ground, although the majority did prefer the more narrow interpretation. Also see the related discussion in Burshtein, *supra* note 13 at 7-67 – 7-69.

201 CIRA Decision No. 00008 (23 April 2003).

202 *Ibid.* at 6.

203 See *911979 Alberta Inc. v. Hank Morin*, CIRA Decision No. 00060 (25 August 2006); *Internet Movie Database. Inc v. 384128 Canada Inc*, CIRA Decision No.

have a significant impact on the outcome of the panel's decision, CIRA should define the term in the *CDRP*. This would be consistent with the *CDRP*'s theme of giving less deference to the individual arbiters.

How both models generally could stand to improve

Although both the *CDRP* and the *UDRP* work to resolve cybersquatting disputes, they by no means seem to be preventing them. Although the *UDRP* has been in place since December 1999, WIPO decided its 25,000th case in 2006.[204] WIPO also saw a 25% increase in claims filed from 2005 to 2006.[205] Canadians also seem to be getting more involved in cybersquatting. According to WIPO's statistics, Canada formed the fourth highest domicile of registrants against whom complaints were filed with WIPO.[206]

A major concern that plagues the *UDRP* was identified by the OECD: in a domain name dispute, the entire loss falls on the victim, including both the cost of the proceeding and any other loss incurred until the domain name is recovered.[207] This concern equally applies to the *CDRP*. To address this concern, ICANN and CIRA could perhaps impose an increase on the cost of registering a domain name. For example, a small price increase would not likely hamper the development of the dot-ca system (which currently charges only $8.50 per year to register a dot-ca name[208]). The additional funds could be used, for example, to subsidize the complainant's costs associated with commencing a procedure, for example, the cost of hiring the panelists. From a business perspective, it is undesirable to hamper the growth of the Internet, "[f]or as consumer use on the Internet expands, retailers receive greater commercial value for their websites both online and

---

00047 (2 December 2005); *Great Pacific Industries Inc. v. Ghalib Dhalla*, CIRA Decision No. 00009 (21 April 2003).

[204] "WIPO Handles its 25,000th Domain Name Case," WIPO/PR/2006/464, online: WIPO <http://www.wipo.int/edocs/prdocs/en/2006/wipo_pr_2006_464.html>.

[205] "Cybersquatting Remains on the Rise With Further Risk to Trademarks From New Registration Practices," *supra* note 49.

[206] "Respondent Country Filing (Ranking)", online: WIPO <http://www.wipo.int/amc/en/domains/statistics/countries.jsp?party=R>. WIPO published statistics breaking down the geographical distribution of parties. In 541 cases, Canada was the domicile of the respondent. Only the United States, the United Kingdom, and China had more respondent representation, with 4753, 963, and 570 cases respectively (as of 17 July 2007).

[207] OECD Report, *supra* note 52 at para. 23.

[208] CIRA Policies, Rules and Procedures, "Fees Policy and Rules," version 1.6 at 3, online: CIRA <http://www.cira.ca/en/documents/2005/q2/FeesPolicyAndRules-1.6.pdf>.

offline."[209] However, it does not seem that the commercial value of websites increases as cybersquatting expands. Thus, higher registration fees might be beneficial by making it less attractive and more expensive for cybersquatters to register domain names in bulk. Higher fees might help to attract registrants who truly do have a legitimate interest in a domain name while discouraging those who do not.

The OECD also pointed out:

> [t]here seems to be no risk to the cybersquatter in continuing to operate this scheme and no incentive to stop. If one victim doesn't take the bait, the cybersquatter can simply stop actively supporting the name, ignore the *UDRP* proceeding and move on to the next victim for a very low filing fee.[210]

Therefore, similar to the $5,000 fine for bad faith complainants, ICANN and CIRA might think of introducing similar fines to cybersquatters for each offending domain name they register. This may help to discourage cybersquatters, as the authorities currently provide little more than a slap on the wrist.

Finally, it may be necessary to put some degree of accountability on the registrars themselves. Perhaps the registrar should bear some burden in checking to see if someone else has rights in a mark when a domain name application is received.[211] While it is not desirable to hamper registrar operations, as more competitiveness between registrars means more choices available to those seeking to register domain names, registrar accountability could be beneficial in obvious cases and disputes could be avoided in cases where suspicions should clearly be aroused. For example, in the above-mentioned *Government of Canada* case, the registrant had registered the following names: <governmentofcanada.ca>, <gouvernementducanada.ca>, <statscanada.ca>, <theweatheroffice.ca>, and <transportcanada.ca>. The applications for registration of the above names should have clearly signaled to the registrar that the names were being registered in bad faith, and the registrar should not be allowed to turn a blind eye. The OECD, in its report to WIPO, noted that its experience with a cybersquatter, as described above, demonstrated how the registrar in effect protects cybersquatters from civil and criminal processes by sponsoring registrations which it knows, or should know, are a sham.[212] The OECD report also pointed out how there is no incentive for a registrar to exercise any degree of due diligence; rather, it

---

[209] Walker, *supra* note 16 at 304.
[210] OECD Report, *supra* note 52 at para. 24.
[211] Sewchuk, *supra* note 29 at para. 54.
[212] OECD Report, *supra* note 52 at para. 24.

is in the registrar's interest to keep cybersquatters as clients due to the large number of domain names they register![213]

A further lesson from the UK?

Nominet, the authority that regulates the dot-uk domain space, provides some significant departures from the *UDRP* and *CDRP* systems in its domain name dispute resolution system. Two key departures involve: (1) a preliminary mediation session between the complainant and the registrant; and (2) an appeal system from panel decisions.

Mediation

A key difference found in the Nominet system is mandatory informal mediation. After both parties to a domain name dispute have filed their submissions, Nominet requires both parties to participate in mandatory informal mediation before their case will be decided by the "experts" (i.e. the equivalent of panels under the *UDRP* or *CDRP*).[214] Mediation is commenced within three days of the last submission.[215] The case will only be sent to an expert should the parties fail to reach a solution within 10 days.[216] Perhaps the most important aspect of the mediation intervention is that Nominet does *not* charge for mediation services.[217]

During the mediation, confidential negotiations are conducted between the parties to help them achieve settlement.[218] A trained staff member communicates with both parties by telephone in order to discuss the possibility of settlement.[219] As at 1 May 2007, Nominet estimates that 1468 cases had entered mediation and 809 of those cases were able to be settled during the mediation.[220]

---

213 *Ibid.* at para. 25.

214 Nominet, "Dispute Resolution Service Policy", online: Nominet <http://www.nominet.org.uk/digitalAssets/10496_DRS_Policy_v2.pdf> at para. 5a [Nominet Policy]. Note that informal mediation can only take place if the respondent files a reply. See Nominet Procedure, *infra* note 215.

215 Nominet, "Dispute Resolution Service Procedure", online: Nominet <http://www.nominet.org.uk/digitalAssets/10495_DRS_Procedure_-_Version_2.pdf> at para. 7a [Nominet Procedure].

216 *Ibid.* at para. 7e.

217 *Ibid.* at para. 21a.

218 *Ibid.* at para. 7b.

219 Nominet, "The Dispute Resolution Service," Booklet, online: Nominet <www.nominet.org.uk/digitalAssets/6296_A5_DRS_Booklet.pdf> at 4.

220 "Nominet DRS Statistics", online: Nominet <http://www.nominet.org.uk/intelligence/statistics/drs/> [Nominet Statistics].

A free mediation system could be an effective way for the *UDRP* and *CDRP* to help relieve some of the costs that complainants must bear.

Appeal process

An important criticism of both the *UDRP* and *CDRP* systems is that its decisions are not binding, either on subsequent panels or on the courts. Critics argue that the system is deficient in that it does not provide a mechanism by which to reconcile divergent decisions or give precedential value to prior decisions.[221] A number of authors have recommended that an appellate process (for example, a review board) be put into place.[222]

An appellate process presents the following advantages: first, it creates an entity to reconcile divergent bodies of precedent; second, it also allows panelists a means of relying on prior decisions; and finally, an appellate process can serve to correct incorrect rulings, and, as compared with the courts, may be a more accessible forum to parties who feel their case was decided incorrectly.[223] If the case ultimately winds up in the courts, "[c]lear and concise panel decisions based on consistent applications of the UDRP will make things easier for courts reviewing panel decisions."[224]

This is precisely what Nominet seems to have done. The Nominet Dispute Resolution Service Policy holds that "either party will have the right to appeal a decision" and that the appeal panel, consisting of three experts,[225] "will consider appeals on the basis of a full review of the matter and may review procedural matters."[226] As at 1 May 2007, Nominet had heard 17 appeals and had overturned nine of the initial expert decisions.[227]

The Nominet appellate process is a good start, but does not reconcile the problem of divergent precedents from non-binding cases.[228] Author Patrick D. Kelley has suggested that a successful appeal process should provide, among others recommendations, the following:

---

221 Freedman & Deane, *supra* note 15 at para. 160.
222 See *ibid.* at para. 160 and Kelley, *supra* note 188 at 204.
223 Kelley, *ibid.* at 195.
224 *Ibid.*
225 Nominet Procedure, *supra* note 215 at para. 18g.
226 Nominet Policy, *supra* note 214 at para. 10a.
227 Nominet Statistics, *supra* note 220.
228 Kelley, *supra* note 188 at 198.

- A system for challenging decisions;
- A system for harmonizing inconsistent precedent;
- An appeal board that would be controlled by the Internet authority (e.g. ICANN or CIRA) as opposed to a service provider.[229]

CONCLUSION

CHANGES IN THE *CDRP* can be anticipated for the future, as the *CDRP* was reported to have undergone a review of its policies in June 2006.[230] Similarly, governmental intervention might not be far off, as domain abuse came to the attention of Parliament when cybersquatters registered domain names using the names of Members of Parliament in 2005.[231] However, while we await changes to the *CDRP*, businesses should be aware of the necessity to implement safeguards against cybersquatters. One author proposes the following risk management techniques:

- conduct trade-mark searches before registering and using domain names;
- register and use domain names as trade-marks. Note that trade-marks in Canada must be used as "source identifiers" and should therefore be marked directly on wares and services; and
- register and use trade-marks as domain names in all important gTLDs and ccTLDs. [232]

Another author has also suggested that parties with competing interests in a domain name work together to provide cross-linking sites.[233] To illustrate what this entails, that author gives the example of the website <www.playtex.com>. Both Playtex Products and Playtex Apparel are two separate companies who undeniably have interest in the domain name. When consumers access the above website, they are given the option of entering either the site of Playtex Products *or* of Playtex Apparel. The page even explicitly states that both companies are two

---

[229] *Ibid.* at 199-202.
[230] Turco, *supra* note 141.
[231] Michael Geist, "Domain Name Dispute Puts Dot-Ca In The Spotlight" *Toronto Star* (13 June 2005), online: TheStar.com <http://www.michaelgeist.ca/resc/html_bkup/june132005.html>.
[232] Freedman & Deane, *supra* note 15 at para. 162.
[233] Deveci, *supra* note 42 at 224-225.

separate companies even though they share the same name.[234] This cross-linking technique serves to "alley fears of confusion" of parties each having a legitimate interest in the name.[235]

The above are useful tips for safeguarding against domain name disputes, but they will not in themselves put cybersquatting at bay. Businesses must therefore be keenly aware of their rights when it comes to domain names. They must also be aware of the different forums available to resolve domain name disputes. While at first glance the *CDRP* may seem restrictive and "stacked against" trade-mark owners in theory, in practice, trade-mark owners should feel comfortable knowing that their dot-ca is protected from blatant attempts of cybersquatting. However, as long as domain name arbitration systems exist, Canadian or otherwise, further improvements will always be warranted as the Internet and accordingly, instances of cybersquatting, continue to grow.

---

[234] As at 10 July 2007.
[235] Deveci, *supra* note 42 at 225.