Digital Companion

Windsor Review of Legal and Social Issues
Revue des Affaires Juridiques et Sociales de Windsor

Volume 2, (Winter 2016) Article 6

DOMAIN NAME SEIZURE IN ACTION: A CANADIAN-AMERICAN COMPARISON

Josh Marcus

Citation Information
Josh Marcus, "Domain Name Seizure in Action: A Canadian-American Comparison" (2016) 2 Windsor Rev Legal Soc Issues—Digital Companion 93.

DOMAIN NAME SEIZURE IN ACTION: A CANADIAN-AMERICAN COMPARISON

Josh Marcus*

I. INTRODUCTION

The evolution of the Internet has challenged courts and governments to apply existing legislation to the previously neglected digital domain. In many cases, courts must apply centuries-old principles of contract or property law to the virtual world. Issues about squatting, trademark infringement, and piracy have taken on a new form, placing a burden on legislators to ensure that the law evolves alongside technology. While the Internet undoubtedly provides immense benefits to society, it has also given rise to a new vehicle for crime and trademark infringement. Many websites allow for downloading or viewing copyrighted, obscene, or otherwise illegal material. In response, the United States Federal Bureau of Investigation (FBI) has seized many domain names that link to these sites. This paper is an in-depth discussion of Canada's ability to do the same through a comparative analysis of the legal framework in these two countries. It will conclude that through the courts, the Canadian government can seize domain names ending in ".CA" provided that the alleged offences allow for the seizure of property through legislation.

This paper will begin with a brief outline of the components of a domain name and the Internet. It will also discuss two organizations: the Internet Corporation for Assigned Names and Numbers (ICANN) and the Canadian Internet Registration Authority (CIRA). These bodies are responsible for the technical aspects and dispute resolution processes with respect to most domain names in the United States and Canada. Their organizational frameworks also raise jurisdictional issues with respect to domain names. Next, through an inquiry into Canadian and American jurisprudence, this paper characterizes domain names as containing proprietary rights, though alternate models are considered. As a form of intangible personal property, an analysis of the legislative context of the two countries will indicate that domain names are subject to existing property seizure legislation. However, conflicting domestic legislation between states has resulted in confusion in the international system. Lastly, the present paper will address domain name seizure in the context of online gaming websites and conclude that in certain scenarios, the Canadian government is capable of seizing certain domain names.

II. DOMAIN NAMES, ICANN, AND CIRA

(a) DOMAIN NAMES

The Internet is a "worldwide network of computers that enables various individuals and organizations to share information."[1] Essentially, it is a way of connecting a user's computer to a

* Josh Marcus is a third-year J.D. candidate at the University of Windsor, Faculty of Law. He holds an Honours Bachelor of Arts degree from Western University where he specialized in International Relations.

[1] Neil Batavia, "That Which We Call a Domain by Any Other Name Would Smell as Sweet: The Overbroad Protection of Trademark Law as it Applies to Domain Names on the Internet" (2002) 53:2 SCL Rev 461 at 462 [Batavia], citing *Panavison Int'l, LP v Toeppen*, 141 F (3d) 1316 at 1318 (9th Cir 1998).

host computer in order to convey information, media, or data. The most well known category of Internet communication is the World Wide Web (WWW). The WWW consists of data files written in programming language, which contain information, text, media, and links to other websites.[2] Each website is associated with a computer that is assigned a unique identification number known as an Internet Protocol (IP) address. These IP addresses correspond to an alphanumeric domain name.[3] For example, a user can access Google's website by entering either the alphanumeric domain name (www.google.com) or the host computer's IP address (64.233.177.94) into their web browser.

IP addresses are assigned through an "address lending" method in order to allow for future expansion, and an IP address may be assigned to more than one domain name.[4] These IP addresses are not static and can be invalidated at any time due to location, load, and security concerns.[5] Accordingly, one cannot own an IP address.[6] Instead, individuals or corporations purchase the right to a domain name in order to ensure continued accessibility to their website. These domain names are purchased through a registrar and should be viewed as independent from the content of a website. Instead, they provide an accessible and user-friendly alternative to keeping track of changing IP addresses.

A standard domain name has three parts: a Top Level Domain (TLD), a Second Level Domain (SLD), and a root.[7] A domain name begins with an SLD (Google, for example), followed by the root (symbolized by a period), and the TLD (COM, NET, ORG, etc.) TLDs are further divided into two sub-categories: Generic Top Level Domains (gTLDs) are the most common and include .COM, .NET, and .ORG, while Country Code Top Level Domains (ccTLDs) are maintained by individual states. These include .CA (Canada), .JP (Japan), and .UK (United Kingdom).[8]

Domain names are organized in a retrieval system known as the Domain Name Service (DNS), which "holds a directory of all computers that maintain TLD directories."[9] Accordingly, if a user wishes to access *Google.com*, for example, the DNS breaks down the domain name into its respective parts and retrieves the corresponding IP address from its database. Once the domain name is linked to an IP address, the user's computer connects to the DNS and the user is able to access the website.[10]

(b) ICANN

ICANN, a nonprofit corporation in the United States, is accountable for assigning and coordinating the management of gTLDs.[11] The corporation is also in charge of the accreditation

---

[2] *Ibid* at 462-63, citing *Brookfield Communications, Inc v West Coast Entm't Corp*, 174 F (3d) 1036 at 1044 (9th Cir 1999).
[3] *Ibid* at 463.
[4] Daniel Hancock, "You Can Have It, But Can You Hold It?: Treating Domain Names as Intangible Property" (2010) 99:1 Ky LJ 185 at 188 [Hancock].
[5] *Ibid*.
[6] *Ibid*.
[7] Batavia, *supra* note 1 at 463.
[8] *Ibid* at 463-64.
[9] *Ibid*.
[10] Hancock, *supra* note 4 at 189.
[11] *Ibid*.

of companies that sell domain names to end-users, known as registrars, and plays a major role in the dispute resolution process both within the United States and abroad.

The international scope of gTLDs and ICANN's domestic nature raises a number of jurisdictional issues. While the corporation administers the technical functions of domain names, its bylaws limit ICANN's policy-making ability to this role.[12] Disputes involving domain names are therefore either handled by the court system, or in some cases, through ICANN's internal dispute resolution process. If a dispute arises under the latter process, ICANN's *Uniform Domain Name Resolution Policy* (UDRP) allows either party to choose whether to bring the complaint to the court system instead.[13] Given that ICANN is located in the United States and is maintained by the United States Department of Commerce,[14] issues arise as to whether international courts have jurisdiction over the maintenance of domain names with a gTLD.

(c) CIRA

CIRA is Canada's local ccTLD registry. Any domain names that end in .CA must be registered with CIRA before they are sold to the registrar, thereby ensuring that all registrars and registrants meet CIRA's eligibility criteria. This includes guaranteeing that all registrants are "Canadian citizens, residents, companies or other legal entities as defined by Canadian law," and that the registration activity has a physical presence in Canada.[15] The CIRA operates under Canadian law and only recognizes court orders from the Canadian judicial system.[16] Similar to ICANN, CIRA plays a role in the dispute resolution process within the country, and binds registrars to abiding by their respective agreements. On the question of jurisdiction, CIRA has acknowledged that if a Canadian user registers a domain name in a foreign country (including .COM, or .UK), the user will likely be subject to that country's legal system.[17] This deferral of power essentially limits CIRA's authority to domain names with a .CA ccTLD.

III. DOMAIN NAMES AS PROPERTY

Until recently, Canadian and American jurisprudence was divided on the issue of treating domain names as property. To determine whether the Canadian government is legally capable of seizing domain names, it must be established whether they are defined as "property" or whether they should be approached through another lens, such as contract law. Both Canadian and American courts have found proprietary interests in domain names.

---

[12] Jacqueline D Lipton, "Bad Faith in Cyberspace: Grounding Domain Name Theory in Trademark, Property, and Restitution" (2010) 23:2 Harv JL & Tech 447 at 448-49 [Lipton], citing Internet Corporation for Assigned Names and Numbers, by-law, *Bylaws for Internet Corporation for Assigned Names and Numbers* (30 July 2014), art 1 §1(3).

[13] Internet Corporation for Assigned Names and Numbers, "Uniform Domain Name Dispute Resolution Policy" (24 October 1999), s 4(k), online: <www.icann.org>.

[14] Hancock*, supra* note 4 at 189.

[15] Canadian Domain Name Consultative Committee, *Framework for the administration of the .CA domain name system*, Canadian Internet Registration Authority, 1998, s 1.7 [*CIRA* Framework].

[16] *Ibid.*

[17] *Ibid*, s 1.3.

IV. CANADIAN APPROACH

One of the first cases to address domain names in Canada was *Easthaven v Nutrisystem Inc*. [18] Easthaven, a corporation registered in Barbados, owned the domain name *Sweetsucess.com*. Nutrisystem.com Inc. owned certain "Sweet Success" trademarks in the United States, which it used in connection with a line of weight loss products. Easthaven had acquired the impugned domain name through Tucows, a registrar, whose head office is in Toronto. Given the various geographical locales, questions about jurisdiction arose.

Easthaven asserted that a domain name is property, and that "the property is located where registration of it takes place," which in this case was Toronto.[19] While the court acknowledged that a domain name could be characterized as intangible property, Justice Nordheimer disagreed and preferred the submission of Nutrisystem, who asserted that "a domain name is not property but it is simply a bundle of rights like a copyright."[20] In this respect, the court stated that "a domain name lacks a physical existence…[It] is simply a unique identifier for a particular Internet site located on a particular computer. That computer may be located anywhere in the world."[21] Accordingly, its characterization cannot be interpreted as constituting either "property" or "intangible property" as defined by Blacks Law Dictionary.[22]

While the Ontario Court of Appeal would later reverse this definition, Justice Nordheimer's portrayal of a domain name as "simply a unique identifier" is technically correct. There are major technological differences between a domain name and a website. A website hosts physical files and information, while a domain name is essentially a means of accessing that information. Daniel Hancock likens this relation to that of a library call number and a book. A book, like a website, contains valuable information; both derive their value from the content provided to their readers. The purpose of the call number, like a domain name, is simply to direct a reader to a certain book or website.[23] As Hancock explains, "even well-crafted domain names, such as *Freecreditscore.com*, do not themselves necessarily convey trustworthy information, but they only serve to direct people to the websites where the information is located." [24] In adopting the unique identifier approach, domain names are seen as a means to access information. As a result, it is difficult to justify finding proprietary value in the string of alphanumeric characters themselves.

The landscape in Canada changed with the Ontario Court of Appeal's decision in *Tucows.com Co v Lojas Renner S.A.*[25] The court in *Tucows* sought to determine whether a domain name is "personal property" within the meaning of rule 17.02(a) of the Ontario *Rules of Civil Procedure.*[26] While the court acknowledged the *Easthaven* characterization of domain names, the developing view among international jurisprudence and academics appeared to define

---

[18] 55 OR (3d) 334, 2001 CanLII 27992 (ONSC) [*Easthaven*].
[19] *Ibid* at para 23.
[20] *Ibid*.
[21] *Ibid* at para 25.
[22] *Black's Law Dictionary*, 10th ed, *sub verbo* "property" ("any external thing over which the rights of possession, use, and enjoyment are exercised"); *Black's Law Dictionary*, 10th ed, *sub verbo* "intangible property" ("property that lacks a physical existence").
[23] Hancock, *supra* note 4 at 201.
[24] *Ibid*.
[25] 2011 ONCA 548 (CanLII), 106 OR (3d) 561 [*Tucows*].
[26] RRO 1990, Reg 194, s 17.02(a).

domain names as "a new type of intangible property."[27] Accordingly, the court cited evidence from Professors Ziff and J.W. Harris with approval to conclude that domain names constitute intangible personal property.[28]

Professor Ziff describes the idea of property as "perfectly straightforward: the term refers to those things one can own."[29] Ziff characterizes property as a bundle of rights, enforceable against others.[30] In other words, "the term property signifies a set of relationships among people that concern claims to tangible and intangible items."[31] The right to exclude others is a necessary condition for some "thing" to be considered "property." As such, bundles of rights belonging to everyone cannot be the property of anyone.[32] The court compared Ziff's definition to that of J.W. Harris in *Property and Justice*. Harris argues:

> [P]roperty comprises (1) ownership and quasi-ownership interests in things (tangible or ideational); (2) other rights over such things which are enforceable against all-comers (non-ownership proprietary interests); (3) money; and (4) cashable rights.[33]

Both Harris and Ziff emphasize the importance of "a collection of rights over things that can be enforced against others."[34] Accordingly, the court found that the bundle of rights accompanying the impugned domain name satisfied both Harris and Ziff's definitions of property. While this characterization has not been challenged at the Supreme Court level, this paper will assume this definition to apply across the country.

It is worth noting that the *CIRA Registrant Agreement*[35] contradicts the Ontario Court of Appeal's judgment. The agreement stipulates that "[t]he Registrant acknowledges and agrees that a Domain Name is not property and that a Domain Name Registration does not create any proprietary right for the Registrant…"[36] Despite this agreement, it has been established at common law that domain name registration does, in fact, create a proprietary right.

This provision gives rise to the question of possible alternative methods of classification. For example, certain courts in the United States have adopted a contract law approach to this issue. If the Supreme Court of Canada were to characterize domain names as the result of a contractual agreement, this provision would be afforded greater weight.[37]

---

[27] *Tucows, supra* note 25 at para 50.
[28] *Ibid* at paras 62, 65.
[29] Bruce Ziff, *Principles of Property Law,* 5th ed (Toronto: Carswell, 2010) at 2.
[30] *Ibid*.
[31] *Ibid*.
[32] *Tucows, supra* note 25 at para 58.
[33] *Ibid* at para 59, citing JW Harris, *Property and Justice* (Oxford: Clarendon Press, 1996) at 139.
[34] *Tucows*, *supra* note 25 at para 60.
[35] The *CIRA Registrant Agreement* is an agreement between CIRA and those who wish to register a CA domain name.
[36] The Canadian Internet Registration Authority, "Registrant Agreement" (12 October 2010), s 3.2, online: <www.services.cira.ca>.
[37] For a further discussion of the contract law approach to domain names, see Eddie Hurter, "The international domain name classification debate: are domain names 'virtual property', intellectual property, property, or not property at all?" (2009) 42:3 Comp & Intl LJS Afr 288 [Hurter].

V. AMERICAN APPROACH

American jurisprudence has varied with respect to the characterization of domain names as property. *Network Solutions Inc v Umbro International Inc et al*[38] is often cited as the first of two American cases to address the issue.[39] In this appeal, Umbro brought a garnishment proceeding against Network Solutions in order to recover thirty-eight domain names.[40] In response, Network Solutions framed the issue using contract law, claiming that the domain names were simply registration agreements.[41] As a result, they argued that a domain name was a contractual right given to the registrant and is therefore not subject to garnishment. The court adopted this theory and, like Justice Nordheimer, viewed a domain name as a unique identifier. Domain names were defined by the court as "vernacular shorthand for the registration services that enable the Internet addressing system to recognize a particular domain name as a valid address."[42] Following this decision, *Umbro* has been cited as characterizing a domain name as a contractual arrangement, rather than as a property right.[43] However, it has been maintained that this is a misinterpretation of the case.[44] *Umbro* simply declared that the impugned domain name contract could not be considered a "liability" and not subject to garnishment.[45] The court specifically chose not to address the question of whether a domain name constituted a form of intellectual property.[46] Accordingly, subsequent jurisprudence re-visited the issue in order to provide a better framework for domain names in the United States.

Kremen v Cohen[47] addressed a conversion claim brought to the Ninth Circuit with respect to the domain name *Sex.com*.[48] Kremen had acquired the domain name in 1994 for use as one of the Internet's first pornographic websites. Cohen was a con man who unlawfully transferred the domain name into his possession through a forged letter to the registrar.[49] Soon after, Cohen fled to Mexico where he was declared a fugitive from justice.[50] As a result, Kremen brought an action against the domain name registrar, Network Solutions. Kremen brought up four issues to the court: (1) Network Solutions breached an implied contract by transferring the domain name to Cohen; (2) Network Solutions violated the registrar's agreement with the United States government; (3) Kremen had a property right with respect to the domain name, and that Network Solutions, by giving it away, committed the tort of conversion; and (4) Kremen sought to hold Network Solutions liable as a bailee of the domain name.[51] In response, the court held that there was no implied contract between Kremen and Network Solutions due to lack of consideration.[52]

---

[38] 529 SE (2d) 80 (Super Ct Va 2000) [*Umbro*].
[39] Hancock, *supra* note 4 at 191.
[40] *Ibid* at 191-92.
[41] *Ibid* at 192.
[42] *Umbro, supra* note 38 at para 5.
[43] Hancock, *supra* note 4 at 192.
[44] *Ibid*; see also *CRS Recovery Inc v John Laxton*, 600 F (3d) 1138 at para 8 (9th Cir 2010) [*CRS*].
[45] *Umbro, supra* note 38 at para 6.
[46] *Ibid* at para 5.
[47] 337 F (3d) 1024 (9th Cir 2002) [*Kremen*].
[48] Hancock, *supra* note 4 at 194.
[49] *Kremen, supra* note 47 at 1026.
[50] *Ibid* at 1027.
[51] *Ibid* at 1027-28.
[52] Hancock, *supra* note 4 at 195 (at the time of registration of the domain name (1994) there was no charge for registering domain names with Network).

There was also no violation found with respect to the agreement between the registrar and the United States government.

On the issue of conversion, the court applied an established common-law test to determine whether domain names are a species of property. Justice Kozinski states that "[f]irst, there must be an interest capable of precise definition; second, it must be capable of exclusive possession or control; and third, the putative owner must have established a legitimate claim to exclusivity."[53] The court found that domain names satisfy all three criteria and held that they constitute a form of intangible property.[54] As a result, the appellant was successful in his claim for conversation against Network Solutions.[55] While other American courts have revisited the issue since *Kremen*, the characterization of domain names as a species of property has been upheld. Accordingly, the question of whether domain names are tangible or intangible remains a subject of debate, their classification as some form of property has been established in the United States.[56]

VI. LEGSILATIVE CONTEXT

It has been shown that the United States has assumed jurisdiction over all gTLDs through ICANN. Canada, on the other hand, has maintained their jurisdiction over domain names with a .CA ccTLD. Given the court's acceptance of domain names as constituting property, an analysis of domestic legislation will apply this concept to the issue of property seizure. By classifying domain names as a form of intangible personal property, legislation with respect to search and seizure can be applied to the digital domain. This allows governments to assume control over domain names that relate to criminal offences. However, the international community remains concerned with respect to conflicting legislation between intellectual property rights and domain names.

VII. CANADIAN LEGISLATION

Canadian legislation governing property seizure is primarily located in the *Criminal Code*[57] and the *Controlled Drugs and Substances Act.*[58] In short, the state is able to seize any property as it relates to a number of listed offences. As a result, if a domain name with a .CA ccTLD links to a website which aids the commission of a listed predicate offense, it is possible that the domain name may be subject to seizure.[59] Once seized, the domain name is subject to the provisions of the *Seized Property Management Act*.[60]

The *Code* defines property as "real and personal property of every description and deeds and instruments relating to or evidencing the title or right to property, or giving a right to recover or receive money or goods."[61] In adopting the *Tucows* interpretation of property, a domain name is a form of intangible personal property. Ownership of a domain name includes a bundle of

---

[53] *Kremen*, *supra* note 47 at 1030.
[54] *Ibid.*
[55] *Ibid* at 1036.
[56] See *CRS, supra* note 44.
[57] RSC 1985, c C-46, s 83.13 [*Code*].
[58] SC 1996, c 19, ss 11, 16 [*CDSA*].
[59] See e.g. *ibid*, s 11(8).
[60] SC 1993, c 37, s 3.
[61] *Supra* note 57, s 2.

rights, including the right to exclude others. It is therefore evident that a domain name may be considered property for the purposes of the *Code*.

The *Code* allows for property seizure when the property in question is addressed in one of its provisions. Section 462.37(1) requires that following a conviction of a designated offence,[62] a court shall order that any property derived from the proceeds of crime be subject to forfeiture.[63] As a result, the courts may issue a warrant to search and seize any property as it relates to an indictable offense. Pursuant to section 462.32 of the *Code*, peace officers may be authorized to search any "building, receptacle or place…[for] any property in respect of which an order of forfeiture may be made under subsection 462.37(1) or (2.01) or 462.38(2)."[64] For the purposes of this analysis, the term "place" will be treated as equivalent to "anywhere" as this term has been judicially defined in a number of provinces.[65] Accordingly, a domain name may be seized as property if the government can prove, on a balance of probabilities, that the domain name was obtained or derived directly or indirectly as a result of the commission of a designated offence in Canada.[66]

If a website aids in the commission of a designated offence by way of providing access to illicit material, it is possible for a court to find that the relevant domain name was obtained through the proceeds of a crime. Further, if these websites generate revenue through the use of advertising or paid access, the domain name may be found to be property obtained by a crime. In other words, if a domain name with a .CA ccTLD is determined to be derived from the proceeds of crime, it may be subject to seizure by the Crown.

While the proceeds of crime provisions may act as a blanket allowance for domain name seizure in relation to many indictable offences, the *Code* contains additional provisions related to specific predicate offences. Crimes associated with terrorism and child pornography are particularly relevant in this respect, as the Internet provides a medium for these activities to proliferate. Section 83.14 allows for a judge of the Federal Court to issue an order of forfeiture for "property owned or controlled by or on behalf of a terrorist group; or property that has been or will be used, in whole or in part, to facilitate or carry out a terrorist activity."[67] The Internet is a valuable tool for these groups. Through the use of websites and social media, terrorist groups are able to finance, train, plan, and execute their objectives.[68] Accordingly, this paper contends that if a website contains information which has been, or will be, used to facilitate terrorist activity contrary to section 83.01, its domain name, as a form of property, may be subject to seizure.

The Internet has also become a useful tool for propagating sexual exploitation, particularly of children. The *Code* allows for the courts to order the seizure of any property relating to convictions regarding child pornography, luring a child, or agreement or arrangement of a sexual offence against a child.[69] In order for the forfeiture to occur, the court must be

---

[62] *Ibid,* s 462.3(1)(a) (designated offence is defined as "any offence that may be prosecuted as an indictable offence under this or any other Act of Parliament, other than an indictable offence prescribed by regulation").
[63] *Ibid*, s 462.37.
[64] *Ibid,* s 462.32(1).
[65] See *R v Brennan*, 35 NSR 106, 1902 CarswellNS 7 at para 6; see also *Laporte v Laganière*, 29 DLR (3d) 651, [1972] QJ No 35 at paras 42-43.
[66] *Code*, *supra* note 57, s 462.37(1).
[67] *Ibid*, s 83.14(1).
[68] United Nations Office on Drugs and Crime, "The Use of the Internet for Terrorist Purposes" (September 2012), online: <www.unodc.org> at 3.
[69] *Supra* note 57, ss 163.1, 172.1, 172.2.

satisfied, on a balance of probabilities, that the property: "(a) was used in the commission of the offence; and (b) is the property of (i) the convicted person or another person who was a party to the offence..."[70] The *Code* stipulates that the person who has the management, control, or custody of any personal property be deemed the owner of it.[71]

As a form of intangible property, these provisions may be found to apply to domain names. If images of child pornography are accessible through *Xyz.ca*, for example, the domain name may be subject to seizure as it relates to the distribution of child pornography provision under the *Code*. Similarly, if *Xyz.ca* aids in the commission of a terrorism-related offence, the domain name may be seized pursuant to 83.14(5) of the *Code*.

Lastly, Canadian legislation allows for the seizure of property pursuant to an order by a court of criminal jurisdiction of a foreign state or entity situated in Canada.[72] This is particularly relevant in the digital context given that websites can be accessed worldwide. If an individual is convicted of a crime while abroad, which is made in relation to a website with a .CA ccTLD, the *Code* allows for our courts to seize the domain name without the hassle of going through the Canadian criminal justice system. These statutory measures play an important role in combatting virtual crimes.

Much of the additional legislative provisions related to property seizure are contained within the *CDSA*. This is likely to allow law enforcement officers to seize tangible property including drugs, paraphernalia, and cash. However, these provisions may also apply to domain names if they are related to a designated substance offence. Section 11 of the *CDSA* allows for the courts to issue a warrant if they are satisfied that property is related to an offence.[73] Similarly, upon conviction of a designated substance offence, courts are obligated to seize the offence-related property.[74]

In 2003, two Canadian websites began shipping cannabis to consumers across the country.[75] Bud Buddy and Budmail allowed users to log onto their website and pick from a variety of strains of marijuana. The product is then shipped to consumers using Canada Post or private courier services.[76] Both Bud Buddy and Budmail were hosted on domain names with a .BIZ gTLD, thereby putting both websites under the jurisdiction of the United States government and out of the reach of Canadian authorities. As of this date, no litigation has occurred with respect to these websites. Websites such as these take advantage of loopholes in the current system and highlight the jurisdictional difficulties associated with domain names.

VIII. AMERICAN LEGISLATION

American legislation with respect to domain names and property seizure is primarily focused on two issues: protecting the rights of trademark holders and prosecuting criminal offences.

---

[70] *Ibid*, s 164.2(1).
[71] *Ibid*, s 588.
[72] *Mutual Legal Assistance in Criminal Matters Act*, RSC 1985, c 30 (4th Supp), s 9.3(1).
[73] *Supra* note 58, s 11(1)(c).
[74] *Ibid,* s 16(1).
[75] David Weisz, "Mail-Order marijuana a budding business", *Capital News Online* (26 September 2008), online: <www.capitalnews.ca>.
[76] *Ibid*.

In 1999, Congress passed the *Anticybersquatting Consumer Protection Act*.[77] The *ACPA* aims to "protect consumers and promote electronic commerce by amending certain trademark infringement, dilution, and counterfeiting laws…"[78] Essentially, the statute creates a cause of action if a person "traffics in, or uses in bad faith a domain name that is confusingly similar to" a registered trademark.[79] While the *ACPA* does not itself empower the state to seize these domain names, it does allow for *in rem* actions against cybersquatters.[80] Those who are found to be in violation of the *ACPA* may face an injunction and are liable to pay damages to the trademark holder.

As a compliment to the *ACPA*, the *Federal Trademark Dilution Act of 1951*[81] provides protection to famous marks against uses that weaken their uniqueness.[82] The *FTDA* allows a trademark owner to seek an injunction against another person's commercial use of a mark or trade name, if such use begins after the mark has become famous and causes dilution of the distinctive quality of the mark.[83] Pursuant to the Supreme Court's decision in *Moseley v V Secret Catalogue, Inc.*, the *FTDA* "unambiguously requires a showing of actual dilution, rather than a likelihood of dilution."[84] In the case of the Internet, dilution may involve proof that a domain name is similar, but unrelated to, a corporate name or registered trademark. This evidential requirement led Congress to enact supplementary legislation in 2006. The *Trademark Dilution Revision Act of 2006,*[85] was largely focused on overturning the Supreme Court's decision. Under the *TDRA*, only proof of a likelihood of dilution is sufficient for trademark holders to obtain relief.[86]

With respect to prosecuting criminal offences, the United States has applied its existing legislation to the domain name context. Unlike Canada, the United States has successfully seized many domain names in recent years. Just as Canada's *Code* allows for a blanket seizure of offence-related property, American legislation allows for the seizure of property related to most felony offences. Domain names are therefore seized pursuant to the appropriate section of the US Code. For instance, 18 USC §981 allows for the forfeiture of any real or personal property related to money laundering, such as trafficking in nuclear, chemical, biological, or radiological weapons technology or material, counterfeiting, and terrorism.[87] 18 USC §982 expands on section 981 and lists additional criminal offences to which property seizure may apply. This includes offences relating to fraud, securities, and theft.[88] Similarly, 18 USC §2323 mandates the forfeiture of "any property used, or intended to be used" to commit or facilitate intellectual property offences, including the trafficking of music, movies, and counterfeit goods.[89] Lastly, 18 USC §1955 allows for any property used in violation of the country's gaming laws, to be seized

---

[77] 15 USC §1125(d) (1999) [*ACPA*].
[78] *Ibid*.
[79] Hancock, *supra* note 4 at 189 [quotations omitted].
[80] For a further discussion on cybersquatting, see Hurter, *supra* note 37.
[81] 15 USC §1125(c) (2012) [*FTDA*].
[82] Batavia, *supra* note 1 at 468.
[83] *Supra* note 81, 15 USC §1125(c)(1).
[84] 123 S Ct 1115 (2003) at 1124.
[85] US, HR 683, 109th Cong, 2006, amending *Trademark Dilution Revision Act of 1946* [*TDRA*].
[86] Dale M Cendali & Bonnie L Schriefer, "The Trademark Dilution Revision Act of 2006: A Welcome – and Needed – Change" (2006) 105 Mich L Rev 108 at 109 [Cendali].
[87] 18 USC §981, ss (a)(1)(A)-(1)(C).
[88] 18 USC §982.
[89] 18 USC §2323, ss (a)(1)(A)-(1)(B).

and forfeited to the United States government.[90] While this list of offences is not exhaustive, it is clear that under American law, the courts may seize any property constituting, or derived from, the commission of an offence.

IX. INTERNATIONAL APPROACH TO DOMAIN NAME REGULATION

The World Intellectual Property Organization (WIPO) is an international intergovernmental organization with 177 member states.[91] In 2001, WIPO issued a report from the Second WIPO Internet Domain Name Process conference. Among other considerations, the report explored the international framework with respect to domain name regulations. The report recognizes that "the Internet presents special challenges for policy development and implementation,"[92] and identifies four relevant features of the current context: (1) the Internet is a global medium; (2) the Internet creates a global space for activity with a series of territorial connections; (3) the rapid acceptance and adoption of the Internet; and (4) the Internet's diverse range of people utilizing the Internet for a diverse range of purposes.[93] In consideration of these principles, WIPO member states outlined three options for the "further development and implementation of intellectual property with respect to domain names."[94] These options should be taken into account if domestic lawmakers attempt to reform the current domain name framework. This will allow for greater continuity between states and result in less confusion for domain name registrants.

The first model for intellectual property policy implementation is self-regulation.[95] In its current state, self-regulation is already apparent in cases of domain name management. The ccTLD administrators, such as CIRA, are not obligated to apply ICANN's UDRP, and are free to draft their own policies and regulations applicable within the country.[96] Self-regulation allows for greater flexibility in the modification of rules, and the ability to accommodate local circumstances.[97] However, self-regulation comes with a risk of conflicting rules for users and increased confusion in determining what is permissible.[98]

A second model is one that applies common rules with respect to intellectual property and domain names by way of contractual agreements with ICANN. This model would call for the development of rules governing what constitutes an infringement of intellectual property rights in domain names.[99] The ICANN model would allow for the swift adoption and implementation of these guidelines, and ensure "coherence in policy application across the generic top-level domain name space."[100] However, this approach relies heavily on legislative restraint and self-regulation to avoid conflicting laws and regulations.[101]

---

[90] 18 USC §1955, ss (d).
[91] The World Intellectual Property Organization, "The Recognition of Rights and the Use of Names in the Internet Domain Name System: Report of the Second WIPO Internet Domain Name Process" (3 September 2001), online: <www.wipo.int>.
[92] *Ibid* at para 58.
[93] *Ibid* at paras 59-64.
[94] *Ibid* at para 68.
[95] *Ibid* at para 69.
[96] *Ibid* at para 70.
[97] *Ibid* at para 71.
[98] *Ibid* at para 72.
[99] *Ibid* at para 73.
[100] *Ibid* at para 74.
[101] *Ibid* at para 76.

Lastly, international treaties may be drafted "with respect to intellectual property questions relating to domain names."[102] This approach could allow for greater international consultation and the application of a uniform domain name policy that would adequately balance the rights of domain name owners and trademark holders.[103] However, the inflexible nature and lengthy negotiation process that accompany these agreements are not compatible with the "speed of response required by the Internet."[104]

It should be noted that these models should not be considered as alternatives, as they can be used cumulatively and in conjunction with domestic legislation. While Canada and the United States share a similar legislative framework, this is not the case globally. The complex jurisdictional issues surrounding domain names and the Internet generally, suggest that states should consider a multi-national approach with respect to domain name regulation. As such, both governments and regulatory authorities must be wary of the international implications of domain name regulation in future development.

X. ALTERNATIVE MODELS CONSIDERED

Although courts in both Canada and the United States have determined that domain names constitute a form of property, academic scholarship has highlighted difficulties associated with the personal property right model and suggested that there may be appropriate alternative approaches to this characterization. These include the unique identifier approach, the contract law approach, and the virtual property approach. While the first two options offer guidance with respect to the shortfalls of the personal property right model, neither offers a viable framework in the long-term. By contrast, the virtual property approach may assist in the development of a future framework with respect to domain names.

XI. UNIQUE IDENTIFIER MODEL

The courts in *Easthaven* and *Umbro* both adopted a "unique identifier" approach to the characterization of domain names. While the library call-number analogy is appropriate, the analysis overlooks the value of domain names as they relate to trademarks. Contrary to the court's analysis, domain names often hold value as more than a string of alphanumeric characters. This is particularly evident in the legislation and case law with respect to cybersquatting.[105] To address this problem, the United States Congress enacted the *ACPA*[106] and the *FTDA*.[107]

Some courts have cited the *ACPA* as evidence that the United States government "intended domain names to be treated as a type of property."[108] While the issue of cybersquatting remains problematic, it would be imprudent to suggest that these provisions on their own confirm that domain names have a proprietary right. Rather, it is more likely that Congress was primarily concerned with protecting commercial interests through this legislation, while leaving the question of domain name classification to the court system.

---

[102] *Ibid* at paras 77-80.
[103] *Ibid* at para 78.
[104] *Ibid* at para 79.
[105] For a further discussion on cybersquatting, see Hurter, *supra* note 37.
[106] *Supra* note 77.
[107] *Supra* note 81.
[108] Hancock, *supra* note 4 at 205.

XII. CONTRACT LAW MODEL

The courts in both *Umbro* and *Kremen* have considered a contract law approach to domain names. A domain name may therefore be categorized as a form of a contractual license between a registrar and a registrant.[109] In this sense, the individual or organization that uses a particular domain name is not actually an owner, rather, they simply hold the right to use the domain name until they either relinquish the right, or are in breach of their agreement.

A problem arises with respect to the contract law approach. When a user acquires a domain name, it results in the creation of "a valuable asset that is freely traded on the open market and that is occasionally stolen by a bad faith actor."[110] Accordingly, difficulties with respect to conversion claims, cybersquatting, and trademark infringement will be exacerbated as contractual rights often conflict with property rights. If a contract law approach is adopted, courts will have to decide whether registrars have a duty to protect certain trademarks or domain names, and if so, when they can be held liable for breaching this duty. This approach would also require a drastic change in the legislative framework with respect to virtual property, as governments would have less control over the regulation of the domain name system. While individuals and corporations have advocated for this approach in the past, it is unadvised for courts to revert back to the contract law framework with respect to domain names.

XIII. VIRTUAL PROPERTY MODEL

Historically, property has been classified as falling under one of two broad groups: real and personal property. These broad categories include the ownership of land, objects, and other moveable and immovable property. More recently, the inclusion of intellectual property rights have protected artistic works and other "labours of the mind."[111] Given the expansive growth of the Internet, it may be time for scholars and lawmakers to recognize a third form of property – virtual property. While virtual property is purely hypothetical and is not legally recognized, academic scholar Eddie Hurter suggests that it should include property interests that are both intangible and exclusionary.[112] "In a lay sense," Hurter explains, "'virtual property' will generally refer to a representation of a place or object within the context of an electronic, or so-called 'virtual' environment that, if it existed in the brick and mortar world, would be a physical object or piece of land."[113]

Virtual property can be distinguished from real and personal property by virtue of the fact that it is intangible.[114] However, virtual and intellectual property differs slightly. Virtual property is exclusionary and can only be used by one individual at a time,[115] whereas products of intellectual property can be read or viewed by multiple audiences at once. There is also less need for government regulation and legislation with respect to virtual property. Hurter argues that it is easier to obtain protection "because, unlike a trade mark or patent, no thorough, time consuming and expensive examination process is required, and there is no originality requirement, which is

---

[109] See Lipton, *supra* note 12 at 474.
[110] *Ibid*.
[111] Hurter, *supra* note 37 at 304.
[112] *Ibid.*
[113] *Ibid.*
[114] *Ibid.*
[115] *Ibid.*

an essential element in securing a copyright."[116] By combining virtual "things," including domain names, websites, and electronic assets, into a new class of property, there will be a greater "opportunity for developing uniform and consistent law and precedent, applicable to many types of emerging interests."[117] A universal adoption of this third category of property interests may alleviate the difficulties faced by the courts in applying the existing real and personal property laws to the digital domain, while providing a framework for future legislation.

XIV. DRAWBACKS TO THE PERSONAL PROPERTY RIGHT MODEL

A number of potential drawbacks arise from applying principles of property law to the virtual domain. Domain name registration is handled on a first-come, first-serve basis. As a result, many individuals register corporate names or trademarks in the hopes of later selling them at a higher value.[118] These users have become known as cyber squatters, and can be described as a form of virtual trespassers.[119] However, some cyber squatters have seen themselves as property speculators operating in a virtual market.[120] By taking a risk in investing in a domain name, these speculators are hoping that another party will eventually pay a higher price for its value.[121] If an entrepreneur decides to register a series of domain names beginning with the letter "I" (such as iFood.com or iWallet.com) in the hopes that Apple will release a related product, is this any different than buying adjoining land to a busy restaurant in the hopes that they will decide to expand? Similarly, existing principles of property law may not fit perfectly into the personal property model. If a domain name is an independent form of property, how could a trademark owner have a better claim to that property than the original owner of the domain name itself? Or, could a domain name owner adversely possess the rights to a trademarked name if the holder does not assert their claim to ownership?

Further difficulties may arise with respect to personal or geographic names. Does President Obama have a better title to www.barackobama.com than the domain name's first registrant simply because he is famous? Can an individual who is not affiliated with any government entity register a www.windsorontario.com domain name? While many of these concerns are addressed by statute, these difficulties highlight the potential drawbacks to the personal property right approach, as courts are left applying principles of property law to domain names on a case-by-case basis. In some instances, these principles work to protect the Internet from being saturated by obscene and illegal material. In others, confusion arises with respect to basic rights such as rightful ownership and adverse possession.

The present paper suggests that the property characterization remains the most appropriate in the context of domain name seizures. Firstly, the propertization of domain names has judicial support in both Canada and the United States, though it has not been considered at the Supreme Court level in either country. Secondly, the current legislative framework allows for the application of existing principles of property law to domain names, particularly in the case of search and seizure. Lastly, a property-based approach is more consistent with the free market attitude towards buying and selling domain names. While virtual property has the potential to

---

[116] *Ibid* at 305.
[117] *Ibid* at 306.
[118] Batavia, *supra* note 1 at 467.
[119] Lipton, *supra* note 12 at 453.
[120] *Ibid*.
[121] *Ibid* at 454.

evolve into its own class of rights, it is also possible to apply the current categorization of domain names as a class of intangible personal property.

XV. DOMAIN NAME SEIZURE IN ACTION

A 2011 FBI Operation entitled "In Our Sites" resulted in the seizure of 150 domain names belonging to websites "engaged in the illegal sale and distribution of counterfeit goods and copyrighted works."[122] Following the seizure, the domain names were no longer linked to the websites, and were instead replaced with an FBI splash page informing the user that the domain name has been seized.[123] This splash page references 18 USC §§ 981 and 2323 and informs the user of the penalties associated with criminal felony copyright laws.[124] Although the majority of the seized domain names were linked to websites hosted abroad, most shipped counterfeit goods to the United States.[125] As such, American jurisdiction over ICANN and all gTLDs allowed the government to seize these domain names, even though the companies were not themselves located within the United States.

By contrast, if this operation were to occur in Canada, the government would be much more limited in their ability to seize these domain names. The domain name would require a .CA ccTLD, meaning that the registrant would have to be a Canadian citizen or resident and must have a physical presence in the country.[126] If the company behind the domain name were not located in Canada, the domain name could be deleted or suspended by CIRA[127] or may be subject to section 9.3(1) of the *Mutual Legal Assistance in Criminal Matters Act*.[128]

On April 15, 2011, the United States Department of Justice seized the domain names of two of the Internet's leading gambling websites. *Pokerstars.com* and *Fulltiltpoker.com* were among a number of online gaming websites whose domain names were seized as part of a crackdown on illegal gambling.[129] United States attorney Preet Bharara issued a statement saying that the websites "concocted an elaborate criminal fraud scheme, ultimately tricking some United States banks and effectively bribing others to assure the continued flow of billions in illegal gambling profits."[130] As a result, the websites' domain names were seized. Although these gaming sites operated on an international level, the Department of Justice's ability and motivation to investigate and prosecute allegations of fraud in the Internet gaming industry is evidence of the benefits of having a single governing body over domain names. However, with the United States assuming exclusive jurisdiction over gTLDs, the country risks overreaching its authority.

---

[122] Federal Bureau of Investigation, "Federal Courts Order Seizure of 150 Website Domains Involved in Selling Counterfeit Goods as Part of DOJ, ICE-HSI, and FBI Cyber Monday Crackdown" (28 November 2011), online: <www.fbi.gov> [FBI].
[123] *Ibid*.
[124] An example of the FBI splash page can be found online at <www.wired.com/images_blogs/business/2010/11/iceseizurenotice1.jpg>
[125] FBI*, supra* note 122.
[126] *CIRA* Framework*, supra* note 15, s 1.7.
[127] Canadian Internet Registration Authority, "General Registration Rules" (5 February 2015) s 11.1, online: <www.cira.ca>.
[128] *Supra* note 72*,* s 9.3(1).
[129] Gary Wise, "PokerStars settles, Acquires FTP", *ESPN* (31 July 2012), online: <www.espn.go.com>.
[130] Matt Richtel, "U.S. Cracks Down on Online Gambling", *The New York Times* (15 April 2011), online: <www.nytimes.com>.

This was the case in 2012 when the United States seized the domain name *Bodog.com*. *Bodog.com* is a Canadian-owned sports gaming website which operates in Canada and Costa Rica.[131] A United States Attorney's office investigation found that *Bodog.com* had sent at least $100 million to United States citizens and conducted a $42 million advertising campaign to attract gamblers to the website.[132] However, *Bodog.com* advanced the position that the lawsuit was irrelevant given that they have "never taken bets from the US."[133] It is hard to imagine another scenario where a government can seize critical assets and effectively suspend the operations of a foreign-owned corporation. However, given the exclusive jurisdiction over gTLDs, the United States is in a position to do just that. As of this date, litigation is pending as Calvin Ayre, the owner of *Bodog.com*, remains a fugitive from justice.[134] *Bodog.com* remains inactive, though the company has since changed its domain name to *Bodog.eu*, thereby bypassing the United States government's jurisdiction.

An analysis of domain name seizures in the context of online gaming illustrates the double-edged sword of the current framework. The United States, by way of ICANN, is able to prevent fraud and protect consumers regardless of the gaming company's physical location. However, the United States is also in a position to advance its own view of how the virtual domain should operate. In cases of obscenity, it is clear that domain names that propagate sexual exploitation should be shut down. However, the line is less clear with respect to online gaming. Gambling online may be viewed as immoral in the United States, yet common in Europe. As such, a question arises as to whether American law should be imposed on all websites with gTLDs. Moreover, if companies such as Bodog can simply change their domain name to one with a ccTLD like .EU, should the United States waste its time and resources into seizing these domain names in the first place? While these issues are not directly relevant in the context of Canadian domain name seizure, they reflect the apparent gaps in the current framework.

XVI. CONCLUSION

It is evident that the Canadian government is capable of seizing domain names with a .CA ccTLD where they link to websites that are connected to one of the offences listed in the country's governing legislation. This includes websites that are used to traffic controlled substances, websites that contain obscene material such as child pornography, and those which host copyrighted media. However, as a result of the implementation of ICANN, any websites with a gTLD remain in the jurisdiction of the United States and are subject to their legislation.

Governments derive the power to seize domain names as a result of their characterization as intangible personal property. While courts and academics have proposed alternative models with respect to the characterization of domain names, there is clear utility in the property rights model. This model allows for courts and legislatures to apply existing legislation with respect to property seizure and trademark protection in the virtual context. This allows governments to effectively shutdown access to websites, which aid in, or derive from, the commission of an offence.

---

[131] The Associated Press, "Bodog Gambling Site Shut Down, Canadian Owner Indicted" *CBC* (29 February 2012), online: <www.cbc.ca>.
[132] *Ibid*.
[133] *Ibid*.
[134] Justin Fenton, "Authorities pursuing extradition of gambling mogul Calvin Ayre", *The Baltimore Sun* (13 October 2014), online: <www.baltimoresun.com>.

As a result, the United States has assumed jurisdiction over domain names with a gTLD, thereby applying their domestic legislation to cyber-space. This imposition is evidence of the double-edged nature of the current domain name framework. The legislative and judicial framework in the United States is suitable for the prosecution of offenders in the digital domain. However, this places a burden on foreign websites to abide by American law if they care to benefit from the use of a gTLD.

In light of this, further reformation of the framework is necessary. The digital world will continue to grow, and the law must evolve accordingly. Jurisdictional issues should be addressed first. Greater coordination is required on an international level to reduce conflicting legislation. Alternatively, if the United States continues to unilaterally assert their domestic legislation over websites with gTLDs, clear guidelines must be made accessible to foreign entities. Secondly, there must be a shift in the approach taken by legislators to clarify the common law position with respect to treating domain names as property. As it stands, existing legislation, including anti-cybersquatting measures and trademark protection, conflict with basic principles of property law. If lawmakers are settled on the propertization of domain names, legislative reforms are necessary. This may involve the creation of a new "virtual property" classification, or clarification with respect to how domain names fit as a species of personal property. Lastly, government organizations should continue to combat virtual crimes by way of domain name seizures, but must ensure that they are not overstepping their role as regulators.