Curbing Domain Name Registration Abuse: A Legal Framework in the Implementation of the Anti-Cybersquatting Provision of the Cybercrime Prevention Act of 2012

Ferdinand M. Negre[*]
Gonzalo D.V. Go III[**]

I. INTRODUCTION

Senator Vicente C. Sotto III, more popularly known as Tito Sotto, has recently been publicly criticized for his alleged violations of intellectual property rights when he failed to acknowledge a blogger after copying one of her entries verbatim,[1] and when he presented as his own, parts of Robert

* '93 M.I.P., Franklin Pierce Law Center; '91 J.D., Ateneo de Manila University School of Law. The Author previously wrote *Doctrine of Equivalents and its Equivalence in the Philippines*, 51 ATENEO L. J. 301 (2011) with Jonathan Q. Perez and *Trademark Law in a Knotshell: From Caves to Cyberspace*, 46 ATENEO L.J. 465 (2001). He currently teaches Trademark Law and the Internet Copyright Law and Intellectual Property Enforcement at the Ateneo Law School. He is a founding

F. Kennedy's 1966 Day of Affirmation speech which he translated into Filipino.[2] It was a completely different scenario more than a decade ago. Tito Sotto was then the victim of a violation of intellectual property rights when a certain Mario Cruz registered the domain name www.titosotto.com[3] and allegedly offered to sell the rights over this domain name to Senator Sotto for $50,000.00.[4] This is a classic case of "cybersquatting," which no law at that time categorically addressed.

This Article provides a legal framework for understanding the concept and activities of cybersquatting, and how the Anti-Cybersquatting Provision of the Cybercrime Prevention Act of 2012[5] addresses the pernicious ramifications of cybersquatting. Part II explains cybersquatting as a serious intellectual property concern, its origin, *modus operandi*, consequences, and earlier legal remedies. Part III discusses the constitutionality of the Anti-Cybersquatting Provision against vagueness, and how it is a valid exercise of police power. Finally, Part IV sets out parameters for the effective

---

partner of Bengzon Negre Untalan Intellectual Property Attorneys and was a Trademark Examiner and Hearing Officer at the then Bureau of Patents, Trademark and Technology Transfer.

** '06 J.D., Ateneo de Manila University School of Law, *with honors*. The Author is currently the Corporate Legal Counsel of Jollibee Foods Corporation, managing all intellectual property concerns of the Jollibee®, Chowking®, Mang Inasal®, Greenwich®, Red Ribbon®, 永和大王® (Yonghe King), 宏状元® (Hongzhuangyuan), and 三品王® (San Pin Wang) brands. He formerly worked as an associate at the SyCip Salazar Hernandez and Gatmaitan Law Offices.

The Author would like to acknowledge the research and editing assistance of Ms. Franchesca Abigail C. Gesmundo, Ms. Patricia Anne D. Sta. Maria, and Mr. Giancharlie P. Go.

Cite as 57 ATENEO L.J. 949 (2013).

1. Sarah Pope, On Plagiarism, The Pill, and Presumptuousness, *available at* http://www.thehealthyhomeeconomist.com/on-plagiarism-the-pill-and-presumptuousness/ (last accessed Feb. 28, 2013).
2. Shaira F. Panela, Kennedy daughter confirms plagiarism complaint vs Sotto, *available at* http://www.gmanetwork.com/news/story/281953/news/nation/kennedy-daughter-confirms-plagiarism-complaint-vs-sotto (last accessed Feb. 28, 2013).
3. At present, www.titosotto.com is already the official webpage of the Office of Senator Vicente C. Sotto III.
4. Leo Magno, *Senators don't own their domain names*, PHIL. DAILY INQ., Aug. 28, 2000, at G1.
5. An Act Defining Cybercrime, Providing for the Prevention, Investigation, Suppression, and the Imposition of Penalties Therefor and For Other Purposes [Cybercrime Prevention Act of 2012], Republic Act No. 10175 (2012).

implementation of the Anti-Cybersquatting Provision by prescribing the standards of its "bad faith" element, other punishable acts, exceptions to its scope, supplements to its perceived deficiencies, and details for obtaining jurisdiction over cybersquatting cases.

II. UNDERSTANDING CYBERSQUATTING

A. Domain Name as the Origin

The Internet is known to be the "information superhighway"[6] that links millions of computer users around the world, and allows them to share and transfer services and information.[7] Considering the vast range of available information on the Internet and its numerous users, companies and individuals avail of particular addresses in this superhighway to make locating the information they want to share easier.

Each computer or website on the Internet is assigned a numeric Internet Protocol address (IP address),[8] which is basically "a series of numbers and periods."[9] Remembering several digits and periods in order to navigate the Internet would be a difficult, if not impossible, task. A domain name is a user-friendly way to access an IP address because it functions like a nickname, with the characters of the domain name being easier to remember than the IP address (e.g., yahoo.com versus 69.147.125.65).[10] A domain name "is a computer address through which a company or an individual can be located by any other user with Internet access. Domain names serve to distinguish and locate the various computers, users, files, and resources accessible over the Internet."[11]

---

6. Gayle Weiswasser, *Domain Names, the Internet, and Trademarks: Infringement in Cyberspace*, 20 SANTA CLARA COMPUTER & HIGH TECH. L.J. 215, 227 (2003).

7. *Id.* at 216–17.

8. Dennis S. Prahl & Eric Null, *The New Generic Top-Level Domain Program: A New Era of Risk for Trademark Owners and the Internet*, 101 TRADEMARK REP. 1757, 1761 (2011) & KIRK A. DAMMAN, UNDERSTANDING THE LEGAL ASPECT OF E-COMMERCE: LEADING LAWYERS ON DEFENDING INTELLECTUAL PROPERTY, NAVIGATING PRIVACY CONCERNS, AND NEGOTIATING CONTRACTS 1 (2011).

9. DAMMAN, *supra* note 8, at 1.

10. *Id.*

11. Weiswasser, *supra* note 6, at 217 (citing Sally M. Abel, *Trademark Issues in Cyberspace: The Brave New Frontier*, 5 MICH. TELECOMM. TECH. L. REV. 91 (1999) & Dan L. Burk, *Trademarks Along the Infobahn: A First Look at the Emerging Law of Cybermarks*, 1 RICH. J.L. & TECH. 1 (1995)).

Kirk A. Damman, in his book on the legal aspect of e-commerce, explains how IP addresses work through what is known as the Domain Name System. He notes:

> The Domain Name System (DNS), which is essentially a global addressing system, allows Internet users to go to a specific website address by entering its corresponding domain name ... [The DNS does this] by translating domain names into IP addresses. The Internet Corporation for Assigned Names and Numbers (ICANN) coordinates and administers the DNS ... [and] is charged with facilitating the technical, managerial, and policy decisions of the Internet. While ICANN administers some DNS functions, the actual registration of domain names is delegated to various accredited registrars. Individual countries are responsible for administering their own domain names.[12]

Domain names are acquired by electronically registering the name with an ICANN accredited registrar. The process of domain name registration usually involves the registry, the registrar, and the registrant:[13]

> The *registry* is a database of all domain names registered for a particular [top-level domain (TLD)]. Registries are part of the DNS. Each registry will be responsible for a particular TLD and is responsible for [the] domain name allocation and [the] technical operation of its TLD. For example, VeriSign is the registry that is responsible for the [generic TLD (gTLD)] .com.
>
> The *registrar* typically acts as a middleman between the registry and the registrant. The registrar must be accredited by the registry responsible for the TLDs it offers. GoDaddy.com is an example of a well-known registrar. Registrars pay registries an annual fee for each TLD they register for a registrant. For example, since VeriSign controls the .com gTLD, it will provide the domain name to the registrar at a particular price, and the registrar in turn sells it to the registrant.
>
> The *registrant* is the party that registers the domain name. The registrant is responsible for providing certain information to the registrar and paying all fees associated with [ ] domain name registration. After the registrant has provided the appropriate information to the registrar, the registrar will confirm that the chosen domain name is available with the registry.
>
> The registration term of domain names varies, depending on the type of TLD. However, all domain name registrations are valid only for a limited time. ... Domain name registrations are [renewable], and like the initial registration period, the renewal period may depend on the type of TLD registered.
>
> If a party forgets to renew a gTLD domain name, all is not lost. Registrars will allow the former registrant to renew the domain name within [30] days of expiration of a gTLD. During this period, the former registrant is the

12. DAMMAN, *supra* note 8, at 1.

13. *Id.* at 3.

> only party that may register or renew the domain name. The grace period and renewal policies vary for each [country code TLD (ccTLD)] provider.[14]

B. Trigger Point: Uniqueness of Each Domain Name

There are at least two parts to every domain name: the top-level domain and the second-level domain.[15]

As an illustration, the Ateneo de Manila University web address is www.ateneo.edu. The ".edu" is the TLD, "ateneo" is the second-level domain, and "www" is the third-level domain. The third-level domain is not controversial because it is controlled by the owner of the second-level domain.[16]

> The TLD "follows the dot ('.') in every web address."[17]
>
> TLDs are divided into three general groups: (1) *generic top-level domains* (gTLDs), (2) *country-code top-level domains* (ccTLDs), and (3) *internationalized domain names* (IDNs).
>
> ...
>
> gTLDs are the most common type of TLD. Common gTLDs include: .com (originally intended for use by commercial organizations, but available to anyone), .net (originally intended for use by sites directly related to the Internet, but available to anyone), .org (originally intended for use by nonprofit organizations, but available to anyone), .edu (used by educational organizations), and so on. Other familiar gTLDs include .gov (reserved for agencies of the [United States (U.S.)] government), .mil (reserved for the [U.S.] military), .int (reserved for international organizations established by treaty), .aero (reserved for members of the air transport industry), .biz (for use by businesses only), .coop (reserved for cooperative associations), .info and .museum (reserved for museums), .name (reserved for individuals), and .pro (being developed for professionals and related entities).
>
> ...
>
> ccTLDs are two-letter TLDs specially designated for a particular country or autonomous territory, such as [.ph for the Philippines,] .uk for the [United

14. *Id.* (emphasis supplied).

15. Aura Lichtenberg & Melissa Solomon, *What Social Squatting Means for Trademark Holders: How to Protect Your Brand on Social Networking Sites*, 22 DCBA BRIEF 36, 36 (2009) (citing Paul Mockapetris, Domain Names — Implementation and Specification (A Memo in Response to Requests for Comments from the Network Working Group), *available at* http://tools.ietf.org/ html/rfc883 (last accessed Feb. 28, 2013)).

16. Prahl & Null, *supra* note 8, at 1761.

17. Lichtenberg & Solomon, *supra* note 15, at 37 (citing Mockapetris, *supra* note 15).

> Kingdom (U.K.),] and .ca for Canada. In general, ccTLDs are administered by nationally designated registration authorities in each country or territory. IDNs are TLDs that allow for domain names in non-Latin scripts, such as Arabic, Japanese, or Cyrillic (e.g., <<foreign language>> for Saudi Arabia).[18]

The second-level domain is "the name that directly precedes the dot in every web address."[19] The third-level domain comprises "the string immediately to the left" of the second-level domain,[20] and is controlled by the owner of the second-level domain.[21] "The most common third-level domain is 'www,' although the mobile website indicator 'm' is gaining popularity as mobile phones become ubiquitous (for instance, m.yahoo.com is the mobile version of Yahoo's website)."[22]

Most legal issues "arise regarding the second-level domain because there cannot be two identical second-level domains under the same [TLD]."[23] Of course, acquiring the right domain name is important because "[w]ithout [the appropriate] domain name, a company would be practically invisible on the Internet, as customers would not know where to find [their website]."[24] Companies then tend to choose domain names that either have high recall value because they are already established trade names, or are easy to remember because they are often used in everyday speech.[25]

To acquire a domain name, "an individual or company must first request the name and file an application with an accredited domain name registrar."[26] Because domain names are assigned on a first-come, first-served basis, problems arise "when a company chooses a name that has already been registered as a trademark by another company, or when two or more companies, each with legitimate claims to the name, want to use [the same domain name]."[27] If the desired domain name has already been registered in

---

18. DAMMAN, *supra* note 8, at 2 (emphasis supplied).
19. Lichtenberg & Solomon, *supra* note 15, at 37 (citing Mockapetris, *supra* note 15).
20. Prahl & Null, *supra* note 8, at 1761 (citing Kremer v. Cohen, 325 F.3d 1035, 1038 (2003) (U.S.)).
21. Prahl & Null, *supra* note 8, at 1761 n.26.
22. *Id.* at 1761.
23. Lichtenberg & Solomon, *supra* note 15, at 36 (citing Daniel A. Tysver, Domain Name Disputes, a*vailable at* http://www.bitlaw.com/internet/domain.html (last accessed Feb. 28, 2013)).
24. Weiswasser, *supra* note 6, at 217.
25. *Id.* at 217-18.
26. Lichtenberg & Solomon, *supra* note 15, at 37 (citing Tysver, *supra* note 23).
27. Weiswasser, *supra* note 6, at 218.

favor of someone else, an individual may either try to acquire it from such person or choose another name altogether.[28]

C. The Modus Operandi of Cybersquatters

Cybersquatters are "individuals [who] attempt to profit from the Internet by reserving and later reselling or licensing domain names back to the companies that spent millions [ ] developing the goodwill of a trademark."[29]

The World Intellectual Property Office (WIPO) explains how cybersquatters work:

> Cybersquatting [ ] involves the pre-emptive registration of trademarks by third parties as domain names. Cybersquatters exploit the first-come, first-served nature of the domain name registration system to register names of trademarks, famous people or businesses with which they have no connection. Since registration of domain names is relatively simple, cybersquatters can register numerous examples of such names as domain names. As the holders of these registrations, cybersquatters often then put the domain names up for auction, or offer them for sale directly to the company or person involved, at prices far beyond the cost of registration. Alternatively, they can keep the registration and use the name of the person or business associated with that domain name to attract business for their own sites.[30]

Cybersquatting "has received much attention because it directly undermines several of the objectives of trademark law, namely, to protect consumers from source confusion and to allow consumers to quickly ascertain the quality of a product identified by the trademark."[31] The immediate effect of cybersquatting is that visitors to the cybersquatter's website are often led to believe that whatever is offered on that site is related to or is in fact the product of the company whose name is being used. The cybersquatter is then able to take advantage of the goodwill attached to another's name, at the expense of the unsuspecting consumers.[32]

Landmark cases of cybersquatting in the U.S. and the U.K. are summarized, thus:

---

28. Lichtenberg & Solomon, *supra* note 15, at 37 (citing Tysver, *supra* note 23).

29. Intermatic Incorporated v. Toeppen, 947 F.Supp. 1227, 1234 (N.D. Ill. 1996) (U.S.).

30. World Intellectual Property Organization, Frequently Asked Questions: Internet Domain Names, *available at* http://www.wipo.int/amc/en/center/faq/domains.html (last accessed Feb. 28, 2013).

31. Janet Moreira, *Making an Informed Choice Between Arbitration or Litigation: The Uniform Domain-Name Dispute Resolution Policy vs. The Anti-Cybersquatting Act*, 44 IDEA 147, 147 (2003).

32. *Id.*

In America, the case of [*Panavision Int'l, L.P. v. Toeppen*] concerned a defendant (Toeppen) who registered the domain name 'panavision.com' and displayed aerial photographs of Pana, Illinois. At no time did Toeppen use the site for commercial purposes. When the photographic equipment company Panavision (which owned the registered trademark PANAVISION) sought to obtain the site, Toeppen demanded they purchase it for [$13,000.00]. When Panavision refused, Toeppen registered a site with the name 'panaflex,' also a registered [trademark] of Panavision. Importantly, Toeppen was found to have registered a vast number of other sites using the names of famous [trademarks], in order to extract money from the rightful proprietors. Finding that Toeppen's acts diluted Panavision's trademarks, the Appellate Court affirmed the decision of the trial court, which held:

'Toeppen was able not merely 'to lessen the capacity of a famous mark to identify and distinguish goods or services,' but to eliminate the capacity of the Panavision marks to identify and distinguish Panavision's goods and services on the Internet. The Court finds that Toeppen's conduct, which prevented Panavision from using its marks in a new and important business medium, has diluted Panavision's marks within the meaning of the statute.'

Importantly[,] the [C]ourt considered that the very purpose of dilution law was to protect [trademarks] from damage.

'Whereas traditional trademark law sought primarily to protect consumers, dilution laws place more emphasis on protecting the investment of the trademark owners. Still, dilution laws do promote consumer welfare: if trademarks are valuable to consumers, then protecting businesses' investments in trademarks will benefit consumers by increasing the willingness of businesses to invest in the creation of recognized marks.'

[Trademarks] are primarily aimed at consumers, who come to believe that a [trademark] signals a certain level of quality. In the [C]ourt's view, not only did Toeppen's actions prevent Panavision from exerting control over their own marks but they would also force customers to trawl through countless websites identified by a search engine, in order to locate the real Panavision website. This confusion would only serve to mislead consumers and increase their search costs. Hence a number of parties would be affected by the diluting effects of the domain names.

In the [U.K.], the leading case was [*British Telecommunications Plc. v. One in a Million, Ltd.*] The case was an appeal brought by the firm One in a Million, which had been found guilty of [trademark] infringement under [Section] 10 (3) of the [Trade Marks Act of 1994 (TMA)] and passing off under the common law. The company had purchased a number of domain names associated with well-known brands with the intention of selling these to the genuine companies. The claimants sought injunctions and assignment of the domain names.

While the majority of the case concerned the tort of passing off, the more interesting aspect for the purposes of this article is the finding on infringement under [section] 10 (3). Section 10 (3) prevents the use of [trademarks] or 'signs' that detrimentally affect other [trademarks], yet One

> in a Million did not use the famous names as [trademarks] and did not display the logos; it was simply that the literal letters of the [trademark] were transposed into the technical address of a domain name.
>
> In the Court of Appeals, Lord Justice Aldous stated he agreed with the finding of Jonathan Sumption QC that the Section could be applied to the actions of One in a Million, without much comment. The case therefore suggests that domain names can come within the meaning of 'a sign' within the TMA. At first blush[,] this appears somewhat contradictory with the definition of [trademark] in [Section] 1 (1), which defines a [trademark] as 'any sign capable of being represented graphically[.]' clearly the implication is that the term 'sign' is broader than the term '[trademark]' and this is perhaps confirmed by the wording of [Section] 3 (1), which provides that signs which do not satisfy the requirements of [Section] 1 (1) cannot be registered as [trademarks]. No further explanation of what a 'sign' might be is provided by the TMA.
>
> This approach has been criticised since it is widely accepted that domain names do not primarily function as origin identifiers. Moore therefore considers the decision to reflect policy considerations, 'otherwise it would create a mismatched legal system where infringers would be caught in the 'real' world and then could evade liability in the virtual world.' *Prima facie*[,] the case suggests there is sufficient scope for the prevention of cybersquatting under English law.[33]

Because there is a lack of specific requirements for the registration process, the policy followed is "first-come, first-served." To this day, any person may register any domain name, with very little substantial restrictions. This has created problems for those who have fallen victim to "speculators" who register names rightfully belonging to others (the practice of "cybersquatting"), in hopes of being able to convince such owners to pay them an amount of money in exchange for relinquishing the domain name's registration.[34]

33. Anan Shawqi Younes, *Trade marks and domain names: exploring the inadequacy of existing protection for the economic value of trade marks*, 34(12) EUR. INTELL. PROP. REV. 847, 849-50 (2012) (citing Panavision Int'l., L.P. v. Toeppen, 945 F. Supp. 1296 (Dist. Court, C.D. Cal. 1996) (U.S.); J. Aldred, *The Economic Rationale of Trademarks: An Economist's Critique*, *in* TRADEMARKS AND BRANDS: AN INTERDISCIPLINARY CRITIQUE (L. Bentley & J. Davis eds., 2008); British Telecommunications Plc. v. One in a Million Ltd. (1999) 1 W.L.R. 03 (Civ. App.); & Mairead M. Moore, *Cybersquatting: Prevention Better than Cure?*, 17 INT'L. J. INFORMATION TECH. 220, 226 (2009)).

34. Juan Pablo Cortés Diéguez, *The UDRP reviewed: the need for a "uniform" policy*, 14 COMPUTER TELECOMMUNICATIONS L. REV. 133, 133 (2008).

D. Global Response to Cybersquatting

The phenomenon of cybersquatting and its pernicious effects have caught the ire of the global community, particularly those of owners of famous trademarks. This paved the way for the conceptualization and implementation of a cost-effective mechanism against cybersquatting, the Uniform Domain Name Dispute Resolution Policy (UDRP).

> The [U.S.] Government ordered the [ ] WIPO in 1998 to undertake an extensive international consultation process in order to design an efficient online procedure — quick and cost effective — to stop the most outrageous [trademark] violations. WIPO opted to recommend the use of a mandatory administrative procedure limited to fighting cybersquatting, which was universally condemned throughout the consultation process. The WIPO proposal was the blueprint of the [UDRP] implemented by ICANN on [1 December 1999]. The implementation of UDRP has a retrospective application, hence being applicable to all domains, including those registered before the UDRP came into effect. However, this provision was limited by a [U.S.] court, which held that the UDRP binds only those domain name registrants who had entered into the registration agreement with the UDRP clause.
>
> The creation of the UDRP had a double aim. First, it was intended to deal efficiently with the most blatant violations of [trademark] law (cybersquatting); and secondly, it was created to protect the registry (ICANN) and the registrars from [trademark] litigation.
>
> ...
>
> The UDRP is legally a mandatory administrative procedure that resembles a documents-only arbitration. Nevertheless, it does not follow the arbitration laws; panels are unaccountable and decisions are not legally binding, allowing parties to initiate a legal action any time during the UDRP procedure. Parties adhere to the UDRP through a clause in their contract, which is formed between the registry (ICANN) and the registrar [i.e., [I]nternet service provider] and between the registrar and the registrant (domain name holder). The contractual clause states that certain [trademark] disputes (cybersquatting disputes) will be resolved by one of the ICANN's approved dispute resolution providers.[35]

Currently, there are four dispute resolution providers approved by ICANN:[36]

(1) Asian Domain Name Dispute Resolution Center;[37]

---

35. *Id.* at 133-34.

36. Internet Corporation for Assigned Names and Numbers (ICANN), List of Approved Dispute Resolution Services, *available at* http://www.icann.org/en/help/dndr/udrp/providers (last accessed Feb. 28, 2013).

37. Asian Domain Name Dispute Resolution Center, *available at* https://www.adndrc.org/index.html (last accessed Feb. 28, 2013).

(2) National Arbitration Forum;[38]

(3) WIPO Arbitration and Mediation Center;[39] and

(4) The Czech Arbitration Court Arbitration Center for Internet Disputes.[40]

E. Addressing Pre-2012 Cybersquatting Using Philippine Laws

Having no legal definition before 2012, cybersquatting committed then in the Philippines would have been considered as trademark infringement, trademark dilution, trade name infringement, false designation of origin, or unfair competition.

Trademark infringement was characterized in Section 155 of the Intellectual Property Code of the Philippines (IP Code) as committed by

> [a]ny person who shall, without the consent of the owner of the registered mark:
>
> 155.1. Use in commerce any reproduction, counterfeit, copy, or colorable imitation of a registered mark or the same container or a dominant feature thereof in connection with the sale, offering for sale, distribution, advertising of any goods or services including other preparatory steps necessary to carry out the sale of any goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive; or
>
> 155.2. Reproduce, counterfeit, copy[,] or colorably imitate a registered mark or a dominant feature thereof and apply such reproduction, counterfeit, copy or colorable imitation to labels, signs, prints, packages, wrappers, receptacles[,] or advertisements intended to be used in commerce upon or in connection with the sale, offering for sale, distribution, or advertising of goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive, shall be liable in a civil action for infringement by the registrant for the remedies hereinafter set forth: *Provided*, That the infringement takes place at the moment any of the acts stated in Subsection 155.1 or this subsection are committed regardless of whether there is actual sale of goods or services using the infringing material.[41]

38. National Arbitration Forum, *available at* http://domains.adrforum.com/ (last accessed Feb. 28, 2013).

39. World Intellectual Property Association, *available at* http://www.wipo.int/pressroom/en/articles/2012/article_0002.html (last accessed Feb. 28, 2013).

40. Arbitration Center for Internet Disputes, *available at* http://www.adr.eu/ (last accessed Feb. 28, 2013).

41. An Act Prescribing the Intellectual Property Code and Establishing the Intellectual Property Office, Providing for its Powers and Functions, and For Other Purposes [INTELLECTUAL PROPERTY CODE OF THE PHILIPPINES],

Although the owner of a registered trademark or well-known mark has the exclusive right to prevent its unauthorized use,[42] "trademark infringement is a question of fact"[43] and may only be established after proving the validity of the plaintiff's mark, the plaintiff's ownership of the mark, and that the use of the mark or its colorable imitation by the alleged infringer results in likelihood of confusion.[44] The legitimate owner of a domain name ought to adduce as evidence his certificate of trademark registration duly issued by the Intellectual Property Office of the Philippines, the absence of which would negate his cause of action for trademark infringement.

The IP Code provision on trademark infringement poses an additional challenge to a trademark registrant who is a foreign individual or corporation not doing business in the Philippines. While the registrant has advantages denied to non-registrants or ordinary users by virtue of his trademark registration, and he enjoys the statutory presumptions arising from such registration — validity of the registration, ownership, and the exclusive right to use the registered marks[45] — he may not successfully sue on the basis of his certificate of registration of trademark alone. As a condition for availing the rights and privileges of his trademark duly registered in the Philippines,

---

Republic Act No. 8293, § 155 (1998) [hereinafter INTELLECTUAL PROPERTY CODE].

42. *Id.* § 147. The rights of the owner of a registered trademark or well-known mark are defined thus:

> Section 147. *Rights Conferred.* — 147.1. The owner of a registered mark shall have the exclusive right to prevent all third parties not having the owner's consent from using in the course of trade identical or similar signs or containers for goods or services which are identical or similar to those in respect of which the trademark is registered where such use would result in a likelihood of confusion. In case of the use of an identical sign for identical goods or services, a likelihood of confusion shall be presumed.
>
> 147.2. The exclusive right of the owner of a well-known mark defined in Subsection 123.1(e) which is registered in the Philippines, shall extend to goods and services which are not similar to those in respect of which the mark is registered: *Provided*, That use of that mark in relation to those goods or services would indicate a connection between those goods or services and the owner of the registered mark: *Provided further*, That the interests of the owner of the registered mark are likely to be damaged by such use.

Id.

43. Corporation v. Daway, 416 SCRA 315, 320 (2003).

44. *See* McDonald's Corporation v. L.C. Big Mak Burger, Inc., 437 SCRA 10, 24 (2004).

45. INTELLECTUAL PROPERTY CODE, § 138.

he has "to show proof that, on top of Philippine registration, [his] country grants substantially similar rights and privileges to Filipino citizens."[46]

Trademark dilution arises if the cybersquatter damages the interests of a well-known mark owner by using a domain name identical with, confusingly similar to, or constituting a translation of a well-known mark in relation to those goods or services, indicating a connection between these goods or services and the owner of the registered well-known mark.[47] Philippine jurisprudence has described it as

> the lessening of the capacity of a famous mark to identify and distinguish goods or services, regardless of the presence or absence of: (1) competition between the owner of the famous mark and other parties; or (2) likelihood of confusion, mistake[,] or deception. Subject to the principles of equity, the owner of a famous mark is entitled to an injunction 'against another person's commercial use in commerce 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.' This is intended to protect famous marks from subsequent uses that blur distinctiveness of the mark or tarnish or disparage it.[48]

The legal provisions on trademark infringement and trademark dilution do not confer on any owner of a registered trademark or well-known mark the right to preclude third parties from using their names or pseudonyms for purposes of identification or information so long as such usage cannot mislead the public as to the source of the goods or services.[49] Cybersquatters in the Philippines prior to 2012 would have conveniently defended their rights over the domain name bearing a mark identical or confusingly similar to a registered trademark or a well-known mark in the Philippines by arguing that such was his name or nickname, so long as the use of his name did not constitute trade name infringement.

Trade name infringement is unlawful and is committed when a person subsequently uses another's trade name, whether as his own trade name, mark, or collective mark, or in any such use of a similar trade name or mark likely to mislead the public.[50] Cybersquatting might still be punished as trade name infringement if the subject domain name was identical or confusingly

46. Phillip Morris, Inc. v. Fortune Tobacco Corporation, 493 SCRA 333, 349 (2006).

47. INTELLECTUAL PROPERTY CODE, §§ 123 (f) & 155.

48. Levi Strauss & Co. v. Clinton Apparelle, Inc., 470 SCRA 236, 255 (2005) (citing Toys "R" Us v. Akkaoui, 40 U.S.P.Q. 2d 1836 (N.D. Cal. 1996) (U.S.)).

49. INTELLECTUAL PROPERTY CODE, § 148.

50. *Id.* § 165.2 (b).

similar to an existing trade name.[51] The elements in proving trademark and trade name infringement are the following:

> (1) The trademark being infringed is registered in the Intellectual Property Office [of the Philippines]; however, in infringement of trade name, the same need not be registered;
>
> (2) The trademark or trade name is reproduced, counterfeited, copied, or colorably imitated by the infringer;
>
> (3) The infringing mark or trade name is used in connection with the sale, offering for sale, or advertising of any goods, business[,] or services; or the infringing mark or trade name is applied to labels, signs, prints, packages, wrappers, receptacles[,] or advertisements intended to be used upon or in connection with such goods, business[,] or services;
>
> (4) The use or application of the infringing mark or trade name is likely to cause confusion or mistake or to deceive purchasers or others as to the goods or services themselves or as to the source or origin of such goods or services or the identity of such business; and
>
> (5) It is without the consent of the trademark or trade name owner or the assignee thereof.[52]

A trade name "need not be registered with the [Intellectual Property Office of the Philippines] before an infringement suit may be filed by its owner against the owner of an infringing trademark[,]"[53] more so against the cybersquatter using as his domain name something identical or confusingly similar to the trade name. All that the trade name owner needs to prove to win in a trade name infringement case against the cybersquatter is that the trade name was previously used by the former in trade or commerce in the Philippines.[54] Unfortunately, this legal protection applies only to trade names and not to personal names.

It is possible for the cybersquatter to be prosecuted for "false designation of origin" only if he uses a domain name constituting or bearing any false designation of origin, false or misleading description of fact, or false or misleading representation of fact in Philippine commerce, and upon showing that his use of the domain name was likely to confuse, mislead, or deceive as to the origin, sponsorship, approval, nature, characteristics, qualities, or geographic origin of the goods, services, or commercial activities offered on

---

51. *Id.* §§ 165.1 & 165.2.

52. Prosource International, Inc. v. Horpag Research Management SA, 605 SCRA 523, 530 (2009) (citing RUBEN E. AGPALO, THE LAW ON TRADEMARK, INFRINGEMENT AND UNFAIR COMPETITION 142-43 (2000)).

53. Coffee Partners, Inc. v. San Francisco Coffee & Roastery, Inc., 614 SCRA 113, 122 (2010).

54. Philips Export B.V. v. Court of Appeals, 206 SCRA 457, 466-67 (1992).

his website.[55] By not using the domain name in commerce, the cybersquatter would be able to effectively remove his act from the scope of false designation and to further his intention of depriving others of the right to register their subject domain name.

A would-be domain name owner might also consider proceeding against the cybersquatter by filing an unfair competition case, which may take the form of (1) a civil case based on the damages incurred from the cybersquatter's unfair competition in commercial or industrial enterprises through the use of "deceit, machination[,] or any other unjust, oppressive[,] or highhanded method,"[56] or (2) a criminal case, if the cybersquatter employed deception or bad faith in passing off the goods, business, or service for those of the legitimate owner.[57] The Supreme Court had the opportunity

55. INTELLECTUAL PROPERTY CODE, § 169.

56. An Act to Ordain and Institute the Civil Code of the Philippines [CIVIL CODE], Republic Act No. 386, § 28 (1950).

57. *See* INTELLECTUAL PROPERTY CODE, § 168. Section 168 provides:

> Section 168. *Unfair Competition, Rights, Regulation and Remedies.* —
>
> 168.1. A person who has identified in the mind of the public the goods he manufactures or deals in, his business or services from those of others, whether or not a registered mark is employed, has a property right in the goodwill of the said goods, business or services so identified, which will be protected in the same manner as other property rights.
>
> 168.2. Any person who shall employ deception or any other means contrary to good faith by which he shall pass off the goods manufactured by him or in which he deals, or his business, or services for those of the one having established such goodwill, or who shall commit any acts calculated to produce said result, shall be guilty of unfair competition, and shall be subject to an action therefor.
>
> 168.3. In particular, and without in any way limiting the scope of protection against unfair competition, the following shall be deemed guilty of unfair competition:
>
> (a) Any person, who is selling his goods and gives them the general appearance of goods of another manufacturer or dealer, either as to the goods themselves or in the wrapping of the packages in which they are contained, or the devices or words thereon, or in any other feature of their appearance, which would be likely to influence purchasers to believe that the goods offered are those of a manufacturer or dealer, other than the actual manufacturer or dealer, or who otherwise clothes the goods with such appearance as shall deceive the public and defraud another of his legitimate trade, or any subsequent vendor of such goods or any agent of any vendor engaged in selling such goods with a like purpose;

to elaborate on the requisites for unfair competition and the difference between it and trademark infringement in a 1999 case, in which it stated that

> [t]he essential elements of an action for unfair competition are (1) confusing similarity in the general appearance of the goods, and (2) intent to deceive the public and defraud a competitor. The confusing similarity may or may not result from similarity in the marks, but may result from other external factors in the packaging or presentation of the goods. The intent to deceive and defraud may be inferred from the similarity of the appearance of the goods as offered for sale to the public. Actual fraudulent intent need not be shown.
>
> Unfair competition is broader than trademark infringement and includes passing off goods with or without trademark infringement. Trademark infringement is a form of unfair competition. Trademark infringement constitutes unfair competition when there is not merely likelihood of confusion, but also actual or probable deception on the public because of the general appearance of the goods. There can be trademark infringement without unfair competition as when the infringer discloses on the labels containing the mark that he manufactures the goods, thus preventing the public from being deceived that the goods originate from the trademark owner.[58]

To be liable for trademark infringement, trademark dilution, trade name infringement, false designation of origin, or unfair competition, the cybersquatter should have used the domain name in commerce. Therefore, the cybersquatter would not be liable under any of these legal provisions if he merely purchased the domain name and maintained it blank, even if he had then deprived the legitimate owner the opportunity to register the same.

> (b) Any person who by any artifice, or device, or who employs any other means calculated to induce the false belief that such person is offering the services of another who has identified such services in the mind of the public; or
>
> (c) Any person who shall make any false statement in the course of trade or who shall commit any other act contrary to good faith of a nature calculated to discredit the goods, business or services of another.
>
> INTELLECTUAL PROPERTY CODE, § 168.

58. *McDonald's Corporation*, 437 SCRA at 37 (citing VICENTE B. AMADOR, TRADEMARKS UNDER THE INTELLECTUAL PROPERTY CODE 278 (1999); Shell Company of the Philippines Ltd. v. Insular Petroleum Refining Co., Ltd., 11 SCRA 436, 440 (1964); "La Insular" v. Jao Oge, 42 Phil. 366, 372 (1921); Alhambra Cigar, Co. v. Mojica, 27 Phil. 266, 270 (1914); Co Tiong Sa v. Director of Patents, 95 Phil. 1, 4 (1954); Clarke v. Manila Candy Co., 36 Phil. 100, 106 (1917); & Q-Tips, Inc. v. Johnson & Johnson, 108 F.Supp. 845, 865 (U.S. Dist. Court. 1952) (U.S.)).

A claim for damages arising from cybersquatting may likewise be pursued based on quasi-delict[59] if the cybersquatter acted with fault or negligence, or in violation of the law on human relations.[60] The concept of "abuse of right," which forms the basis for the laws on human relations in our Civil Code, was aptly discussed by the Court in *Carpio v. Valmonte*:[61]

> In the sphere of our law on human relations, the victim of a wrongful act or omission, whether done willfully or negligently, is not left without any remedy or recourse to obtain relief for the damage or injury he sustained. Incorporated into our civil law are not only principles of equity but also universal moral precepts which are designed to indicate certain norms that spring from the fountain of good conscience and which are meant to serve as guides for human conduct. First of these fundamental precepts is the principle commonly known as 'abuse of rights' under Article 19 of the Civil Code. It provides that '[*e*]*very person must, in the exercise of his rights and in the performance of his duties, act with justice, give everyone his due*[,] *and observe honesty and good faith.*' To find the existence of an abuse of right, the following elements must be present: (1) there is a legal right or duty; (2) which is exercised in bad faith; (3) for the sole intent or prejudicing or injuring another. When a right is exercised in a manner which discards these norms resulting in damage to another, a legal wrong is committed for which the actor can be held accountable. One is not allowed to exercise his right in a manner which would cause unnecessary prejudice to another or if he would thereby offend morals or good customs. Thus, a person should be protected only when he acts in the legitimate exercise of his right, that is when he acts with prudence and good faith; but not when he acts with negligence or abuse.
>
> Complementing the principle of abuse of rights are the provisions of Articles 20 and 21 of the Civil Code which read, thus:
>
> [Article] 20. Every person who, contrary to law, willfully or negligently causes damage to another, shall indemnify the latter for the same.
>
> [Article] 21. Any person who willfully causes loss or injury to another in a manner that is contrary to morals or good customs or public policy shall compensate the latter for the damage.
>
> The foregoing rules provide the legal bedrock for the award of damages to a party who suffers damage whenever one commits an act in violation of some legal provision, or an act which though not constituting a transgression of positive law, nevertheless violates certain rudimentary rights of the party aggrieved.[62]

59. CIVIL CODE, art. 2176.

60. CIVIL CODE, arts. 19-21.

61. Carpio v. Valmonte, 438 SCRA 38 (2004).

62. *Id.* at 46-48 (citing CIVIL CODE, arts. 19-21) (emphasis supplied).

III. CONSTITUTIONALITY OF THE ANTI-CYBERSQUATTING PROVISION

On 12 September 2012, the Cybercrime Prevention Act of 2012 was enacted into law. This is the only Philippine law which categorically defines and punishes cybersquatting as a crime, being an offense against the confidentiality, integrity, and availability of computer data and systems.[63]

Section 4 (a) (6) of the Philippine Cybercrime Law (the Anti-Cybersquatting Provision) defined "cybersquatting" as

> [t]he acquisition of a domain name over the [I]nternet in bad faith to profit, mislead, destroy reputation, and deprive others from registering the same, if such a domain name is:
>
> (i) Similar, identical, or confusingly similar to an existing trademark registered with the appropriate government agency at the time of the domain name registration[;]
>
> (ii) Identical or in any way similar with the name of a person other than the registrant, in case of a personal name; and
>
> (iii) Acquired without right or with intellectual property interests in it.[64]

To constitute "cybersquatting," these elements must be present:

(1) There must be an acquisition of a domain name over the Internet (i.e., domain name registration);

(2) The domain name registration was attended with bad faith;

(3) Bad faith was characterized as the intention to profit, mislead, destroy reputation, and deprive others from registering the same domain name; and

(4) The registered domain name is either:

   (a) Identical or similar to a trademark registered with the appropriate government agency as of the date of domain name registration;

   (b) Identical or similar with the name of a natural person other than the registrant;

   (c) Acquired without right; or

   (d) Acquired with intellectual property interests in it.[65]

A natural person found guilty of cybersquatting under the Anti-Cybersquatting Provision shall be punished with imprisonment from a

63. *See generally* Cybercrime Prevention Act of 2012.

64. *Id.* § 4 (a) (6).

65. Cybercrime Prevention Act of 2012, § 4 (a) (6).

minimum of six years to a maximum of 12 years, or a minimum fine of ₱200,000.00 up to a maximum amount commensurate to the damage incurred, or both.[66] In addition, should cybersquatting be done on behalf of or for the benefit of a juridical entity, such juridical entity shall be held liable for a fine equivalent to at least double the fines imposable up to a maximum of ₱10,000,000.00.[67] Cybersquatting is punished in its consummated and attempted stages,[68] and the punishment extends to those who willfully abet or aid in its commission.[69]

Upon its enactment, the Cybercrime Prevention Act of 2012 proved to be controversial. In less than a month upon its enactment into law, the Philippine Cybercrime Law and/or some of its salient provisions were assailed before the Supreme Court by different sectors of society for being unconstitutional. Pending oral arguments and ultimate resolution of the consolidated petitions, the Supreme Court temporarily restrained the implementation and enforcement of the provisions of the Philippine Cybercrime Law for 120 days.[70]

A. Negating Vagueness

Critics may question the constitutionality of the Anti-Cybersquatting Provision for being vague and argue that the term "acquisition in bad faith" has no settled definition by prior judicial or administrative precedents. As such, violates due process for not giving fair warning or sufficient notice of what it seeks to penalize.

A statute is said to be vague when it lacks comprehensible standards that men of common intelligence must necessarily guess at its meaning and differ as to its application, and hence, repugnant to the Constitution because it "(1) violates due process for failure to accord persons, especially the parties [targeted] by it, fair notice of the conduct to avoid; and (2) leaves law enforcers unbridled discretion in carrying out its provisions and becomes an arbitrary flexing of the [g]overnment muscle."[71]

> [The 'void-for-vagueness'] doctrine has been formulated in various ways, but is most commonly stated to the effect that a statute establishing a

66. *Id.* § 8.

67. *Id.* § 9.

68. *Id.* § 5 (b).

69. *Id.* § 5 (a).

70. Supreme Court of the Philippines, Temporary Restraining Order (A Notice of Resolution Dated Oct. 9, 2012 in the Consolidated Petitions of Biraogo v. National Bureau of Investigation, et al.), *available at* http://sc.judiciary.gov.ph/jurisprudence/2012/october2012/203299.pdf (last accessed Feb. 28, 2013).

71. People v. Nazario, 165 SCRA 186, 195 (1988).

> criminal offense must define the offense with sufficient definiteness that persons of ordinary intelligence can understand what conduct is prohibited by the statute. It can only be invoked against that specie of legislation that is utterly vague on its face, i.e., that which cannot be clarified either by a saving clause or by construction.
>
> ...
>
> [T]he doctrine does not apply as against legislations that are merely couched in imprecise language but which nonetheless specify a standard though defectively phrased; or to those that are apparently ambiguous yet fairly applicable to certain types of activities. The first may be 'saved' by proper construction, while no challenge may be mounted as against the second whenever directed against such activities. With more reason, the doctrine cannot be invoked where the assailed statute is clear and free from ambiguity[.]
>
> The test in determining whether a criminal statute is void for uncertainty is whether the language conveys a sufficiently definite warning as to the proscribed conduct when measured by common understanding and practice. It must be stressed, however, that the 'vagueness' doctrine merely requires a reasonable degree of certainty for the statute to be upheld — not absolute precision or mathematical exactitude ... Flexibility, rather than meticulous specificity, is permissible as long as the metes and bounds of the statute are clearly delineated. An act will not be held invalid merely because it might have been more explicit in its wordings or detailed in its provisions, especially where, because of the nature of the act, it would be impossible to provide all the details in advance as in all other statutes.[72]

The Anti-Cybersquatting Provision may be critically scrutinized by comparing it with the U.S. Trademark Act's provision on cyberpiracy[73] (U.S. Cyberpiracy Provision), which the former closely resembles. The U.S. Cyberpiracy Provision states that

> a person shall be liable in a civil action by the owner of a mark, including a personal name which is protected as a mark under this section, if, without regard to the goods or services of the parties, that person (i) has a bad faith intent to profit from that mark, including a personal name which is protected as a mark under this section; and (ii) registers, traffics in, or uses a domain name that —
>
> (1) in the case of a mark that is distinctive at the time of registration of the domain name, is identical or confusingly similar to that mark;
>
> (2) in the case of a famous mark that is famous at the time of registration of the domain name, is identical or confusingly similar to or dilutive of that mark; or

72. Estrada v. Sandiganbayan, 369 SCRA 394, 439-40 (2001).

73. 15 U.S.C. § 1125 (d) (2010).

(3) is a trademark, word, or name protected by reason of [S]ection 706 of [T]itle 18 or [S]ection 220506 of [T]itle 36.[74]

In order for both the Anti-Cybersquatting Provision and the U.S. Cyberpiracy Provision to apply, the cybersquatter needs to acquire a domain name which represents an already registered trademark; but for a domain name representing a personal name, only the U.S. Cyberpiracy Provision requires the personal name to be protected as a mark. For both provisions, the acquisition of domain name must be attended with bad faith and intent, whether or not the subject domain name will be used for similar or related goods and services.

The Anti-Cybersquatting Provision did not expound on what "acquisition in bad faith" meant, but only defined the intent which the cybersquatter should possess in acquiring a domain name in bad faith — that is, to profit, mislead, destroy the reputation of, and deprive others from registering the subject domain name. The U.S. Cyberpiracy Provision, however, goes further and enumerates nine factors in determining the element of bad faith. They are:

(1) The trademark or other intellectual property rights of the person, if any, in the domain name;

(2) The extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person;

(3) The person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;

(4) The person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name;

(5) The person's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site;

(6) The person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct;

(7) The person's provision of material and misleading false contact information when applying for the registration of the domain name, the person's intentional failure to maintain accurate contact

74. *Id.* § 1125 (d) (1) (A).

information, or the person's prior conduct indicating a pattern of such conduct;

(8) The person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties; and

(9) The extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous within the meaning of subsection (c).[75]

Parenthetically, even the UDRP has provided circumstances that can prove bad faith intent. They are:

(1) Circumstances indicating that [the registrant has] registered or [he 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 [ ] documented out-of-pocket costs directly related to the domain name; or

(2) [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

(3) [The registrant has] registered the domain name primarily for the purpose of disrupting the business of a competitor; or

(4) By using the domain name, [the registrant has] intentionally attempted to attract, for commercial gain, [i]nternet users to its [website] or other [online] location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of [his website] or location or of a product or service on [his website] or location.[76]

These determinative factors appear significant in proving the bad faith element, but their absence in the Anti-Cybersquatting Provision may not be considered as a constitutional infirmity by way of vagueness. This law may not be invalidated simply "because it could have been more explicit in its wordings or detailed in its provisions."[77] Philippine jurisprudence has

75. *Id.* § 1125 (d) (1) (B) (i).

76. ICANN, *Uniform Domain-Name Dispute-Resolution Policy*, ¶ 4 (b) (Oct. 24, 1999), *available at* http://www.icann.org/en/help/dndr/udrp/policy (last accessed Feb. 28, 2013) [hereinafter *Uniform Domain-Name Dispute-Resolution Policy*].

77. *Estrada*, 369 SCRA at 440.

recognized that it is in fact impossible to place in a law every detail in order to provide for all possible circumstances which may come within its scope,[78] and this holds equally true when it comes to the Cybercrime Prevention Act of 2012. As long as the meaning of the element of "acquisition in bad faith" may be determined through statutory construction, the same should not be considered as vague. The Supreme Court's explanation behind its ruling in *Romualdez v. Sandiganbayan*[79] regarding the validity of Section 5 of the Anti-Graft and Corrupt Practices Act[80] notwithstanding a lack of detailed definition of the word "intervene," is instructional, thus:

> As to petitioner's claim that the term *intervene* is vague, this Court agrees with the Office of the Solicitor General that the word can easily be understood through simple statutory construction. The absence of a statutory definition of a term used in a statute will not render the law 'void for vagueness,' if the meaning can be determined through the judicial function of construction. Elementary is the principle that words should be construed in their ordinary and usual meaning.
>
> ...
>
> '[T]here is no positive constitutional or statutory command requiring the legislature to define each and every word in an enactment. Congress is not restricted in the form of expression of its will, and its inability to so define the words employed in a statute will not necessarily result in the vagueness or ambiguity of the law so long as the legislative will is clear, or at least, can be gathered from the whole act [.]'
>
> [I]t is a well-settled principle of legal hermeneutics that words of a statute will be interpreted in their natural, plain[,] and ordinary acceptation and signification, unless it is evident that the legislature intended a technical or special legal meaning to those words. The intention of the lawmakers — who are, ordinarily, untrained philologists and lexicographers — to use statutory phraseology in such a manner is always presumed.
>
> The term *intervene* should therefore be understood in its ordinary acceptation, which is to 'to come between.'[81]

Based on the foregoing, the Anti-Cybersquatting Provision's element of "acquisition in bad faith" is not vague because applying statutory construction will shed light on its meaning. The term "acquire" should be

78. *Id.*

79. Romualdez v. Sandiganbayan, 435 SCRA 371 (2004).

80. Anti-Graft and Corrupt Practices Act, Republic Act No. 3019, § 5 (1960).

81. *Romualdez*, 435 SCRA at 387-88 (citing Caltex v. Palomar, 18 SCRA 247, 256 (1966); Estrada v. Sandiganbayan, 421 Phil. 290, 347-38 (2001); Mustang Lumber, Inc. v. Court of Appeals, 257 SCRA 430, 448 (1996); & Philippine Long Distance Telephone Company v. Eastern Telecommunications Philippines, Inc., 213 SCRA 16, 26 (1992)).

given its ordinary meaning which is "to gain possession of"[82] and applying this meaning in connection with domain names, should simply refer to domain name registration.

The term "bad faith" has its jurisprudential definition. Bad faith is "a state of mind indicated by acts and circumstances[,] ... provable by [circumstantial] ... evidence,"[83] implying "a conscious and intentional design to do a wrongful act for a dishonest purpose or moral obliquity,"[84] and "contemplates a state of mind affirmatively operating with furtive design or with some motive of self-interest or ill will or for ulterior purpose."[85] In an earlier trademark case (having similar application to domain names), where it was ruled that appropriation of a trademark in bad faith does not necessarily ripen into ownership (despite the first-to-use rule in effect at that time), bad faith was considered as already present upon proof of mere knowledge of prior existence of an identical or confusingly similar mark.[86] The concept of bad faith is not capable of exact measurement. It is a state of mind made visible through acts and circumstances attended by malice or ill will. The registration of a domain name in bad faith is grounded on the cybersquatter's wrongful act aimed at a dishonest purpose. However, upon taking a closer look at the Anti-Cybersquatting Provision, it may be gleaned that the enumerated reasons for registering the domain name (i.e., intention to profit, mislead, destroy reputation, and deprive others from registering the subject domain name) constitute the bad faith element itself.

Considering the novelty of this bad faith element and the concept of cybersquatting in Philippine laws, cybersquatting jurisprudence from foreign states and international domain name dispute resolution providers may be considered and treated with persuasive effect. Foreign authorities have provided these indications of the cybersquatter's bad faith or malicious intent. Some of these are contained in the UDRP and have already been cited previously. Some other indicators are:

(1) Registrant breached his warranty under the relevant domain name registration agreement for actually infringing, or failing to

82. THE MERRIAM-WEBSTER DICTIONARY 25 (1997 ed.).

83. Vda. De Laig v. Court of Appeals, 82 SCRA 294, 305 (1978) (citing Zumwalt, et al. v. Utilities Ins. Co., 228 S.W. 2d 750, 754 (Miss. 1950) (U.S.)).

84. Far East Bank and Trust Company v. Court of Appeals, 241 SCRA 671, 675 (1995).

85. Air France v. Carrascoso, 18 SCRA 155, 166-67 (1966).

86. Shangri-La International Hotel Management, Ltd. v. Developers Group of Companies, Inc., 486 SCRA 405, 424 (2006).

ensure that he is not infringing, upon or violate the rights of any third party;[87]

(2) Registrant provided no[88] or false[89] contact information in his domain name registration application;[90]

(3) Registrant, a licensee, registered and used the licensed mark without the trademark owner's permission;[91]

(4) Registrant failed to perform a trademark search, even where it would have only have revealed a pending application;[92]

(5) Registrant registered a well-known mark as his domain name;[93]

(6) Registrant had constructive notice of the real owner's trademark rights;[94]

87. Harvard Law School Berkman Center for Internet & Society, UDRP Opinion Guide (A Summary of the Opinions of UDRP Panellists on Various Issues Compiled by the Berkman Center for Internet & Society) § 3.1.1.3, *available at* http://cyber.law.harvard.edu/udrp/opinion/ (last accessed Feb. 28, 2013) (citing Empresa Brasileira de Telecomunicações S.A.–Embratel v. Kevin McCarthy, No. D2000-0164, 2000 WL 33674371, at *6 (WIPO Arb. Mediation Ctr. May 15, 2000) & Young Genius Software AB v. MWD, James Vargas, No. D2000-0591, 2000 WL 35595520, at *9 (WIPO Arb. Mediation Ctr. Aug. 7, 2000)).

88. Symplicity Corporation v. Bob Gately, No. D2000-0425, ¶ 6.10 (July 12, 2000).

89. Hunton & Williams v. American Distribution Systems, Inc., et al., No. D2000-0501, 2000 WL 35595615, ¶ 6 (3) (WIPO Arb. Mediation Ctr. Aug. 1, 2000).

90. Harvard Law School Berkman Center for Internet & Society, *supra* note 86, § 3.1.1.3.3.

91. *Id.* § 3.1.1.3. (citing The Aarque Companies v. Aarque Graphics, Forum File No. A0004000094669 (Nat'l Arb. Forum June 16, 2000), *available at* http://domains.adrforum.com/domains/decisions/94669.htm (last accessed Feb. 28, 2013)).

92. Harvard Law School Berkman Center for Internet & Society, *supra* note 86, § 3.1.1.3.6 (citing Kate Spade, LLC v. Darmstadter Designs, No. D2001-1384, 2002 WL 31269760, ¶ 6.9 (WIPO Arb. Mediation Ctr. Jan. 3, 2002)).

93. Harvard Law School Berkman Center for Internet & Society, *supra* note 86, § 3.1.1.3.7 (citing The Caravan Club v. Mrgsale, Claim No. FA0007000095314 (Nat'l Arb. Forum Aug. 30, 2000), *available at* http://www.adrforum.com/domains/decisions/95314.htm (last accessed Feb. 28, 2013)).

94. Harvard Law School Berkman Center for Internet & Society, *supra* note 86, § 1.1.3.8 (citing Barney's Inc. v. BNY Bulletin Board, No. D2000-0059, 2000 WL 35577184, ¶ 7 (WIPO Arb. Mediation Ctr. Apr. 2, 2000)).

(7) Registrant registered a domain name that is identical or confusingly similar to any mark known to him, which mark is not necessarily famous or well-known;[95]

(8) Stockpiling: the registration of multiple domain names;[96]

(9) Registrant's non-use of the domain name;[97]

(10) Absence of registrant's legitimate use of the domain name;[98] and

(11) Absence of registrant's right or interest in the personal name used in the domain name, whether such name is registered[99] or not registered.[100]

(12) Registrant has used the domain to link to other sites or have otherwise diverted or redirected Internet traffic.[101]

(13) Typosquatting: the registration of a misspelling or variation of a registered mark.[102]

---

95. Harvard Law School Berkman Center for Internet & Society, *supra* note 86, § 3.1.1.3.9 (citing Moana Pacific Fisheries Limited v. Turner New Zealand, No. D2000-0139, 2000 WL 33674360, ¶ 6.5 (WIPO Arb. Mediation Ctr. Apr. 26, 2000)).

96. Harvard Law School Berkman Center for Internet & Society, *supra* note 86, § 3.1.1.3.10 (citing Diageo PLC v. John Zuccarini, individually and T/A Cupcake Patrol, No. D2000-0996, 2000 WL 35641494, at *6 (WIPO Arb. Mediation Ctr. Aug. 22, 2000)).

97. Harvard Law School Berkman Center for Internet & Society, *supra* note 86, § 3.1.1.3.11 (citing Ceyx Technologies v. Ceyx.com, No. D2001-0681, 2001 WL 1701123, at *5-6 (WIPO Arb. Mediation Ctr. July 9, 2001)).

98. Harvard Law School Berkman Center for Internet & Society, *supra* note 86, § 3.1.1.3.11 (citing McNeil Consumer Brands, Inc. v. Mirweb Solutions, No. D2000-0612, ¶ 6 (ii) (WIPO Arb. Mediation Ctr. Aug. 3, 2000)).

99. Playboy Enterprises International, Inc. v. Good Samaritan Program, No. D2001-0241, 2001 WL 1700845, ¶ 5 (c) (WIPO Arb. Mediation Ctr. May 17, 2001).

100. Julia Fiona Roberts v. Russell Boyd, No. D2000-0210, 2000 WL 33674395, at *3-4 (WIPO Arb. Mediation Ctr. May 29, 2000). *See also* Pierce Brosnan v. Network Operations Center, No. D2003-0519, 2003 WL 23203067, at *4-5 (WIPO Arb. Mediation Ctr. Aug. 27, 2003).

101. Harvard Law School Berkman Center for Internet & Society, *supra* note 86, § 3.1.1.3.13 (citing Zwack Unicum RT. v. Erica J. Duna, No. D2000-0037, 2000 WL 33716767, ¶ 6.3 (WIPO Arb. Mediation Ctr. Mar. 10, 2000) & Club Monaco Corporation v. Charles Gindi, No. D2000-0936, 2000 WL 35640937, at *6-7 (WIPO Arb. Mediation Ctr. Oct. 17, 2000)).

102. Harvard Law School Berkman Center for Internet & Society, *supra* note 86, § 3.1.1.3.14 (citing Playboy Enterprises International, Inc. v. SAND WebNames

(14) Registrant's failure to respond to a cease and desist letter or other communications.[103]

(15) Use of trademark owner's mark in metatags to attract search engines.[104]

(16) Registration of domain names to tarnish the trademark or personal name at issue.[105]

This list covers circumstances with one unifying element: the cybersquatter taking undue advantage of a registered trademark or a personal name. The undue advantage may come about in the form of profit to the cybersquatter, tarnishing of the goodwill of the registered trademark or the person whose name was registered, or misleading the public as to the true source, sponsorship, or affiliation of the domain and products or services exhibited therein.

B. Valid Exercise of Police Power

The Anti-Cybersquatting Provision enables the State to prosecute and punish a person who obtains in bad faith a domain name identical or similar to registered trademarks and personal names, with the intention (among others) of achieving financial gain and undue advantage to the detriment of their real owners. There can be no real question as to the police power of the State to regulate this opportunistic deed for the purpose of suppressing or restraining the unauthorized use, passing off, and ultimate dilution of registered trademarks and personal names.

Police power is an inherent attribute of sovereignty. The Supreme Court has previously expounded that

> [i]t is a power not emanating from or conferred by the [C]onstitution, but inherent in the [S]tate, plenary, suitably vague[,] and far from precisely defined, rooted in the conception that man in organizing the [S]tate and imposing upon the government limitations to safeguard constitutional rights did not intend thereby to enable individual citizens or group of citizens to

— For Sale, No. D2001-0094, 2001 WL 1705467, at *4 (WIPO Arb. Mediation Ctr. Apr. 3, 2001)).

103. Harvard Law School Berkman Center for Internet & Society, *supra* note 86, § 3.1.1.3.15 (citing NFL Properties, Inc., et al. v. BBC AB, No. D2000-0147, 2000 WL 33674362, at *4 (WIPO Arb. Mediation Ctr. Apr. 22, 2000)).

104. Harvard Law School Berkman Center for Internet & Society, *supra* note 86, § 3.1.1.3.16 (citing Vodafone Group PLC v. Desiree Mendoza, No. D2001-1037, 2001 WL 1701381, at *9 (WIPO Arb. Mediation Ctr. Dec. 4, 2001)).

105. LEGO Juris A/S v. Bangfei Jiang, No. D2012-1235 (WIPO Arb. Mediation Ctr. Aug. 21, 2012), *available at* http://www.wipo.int/amc/en/domains/search/text.jsp?case=D2012-1235 (last accessed Feb. 28, 2013).

> obstruct unreasonably the enactment of such salutary measures to ensure communal peace, safety, good order[,] and welfare.[106]

Police power has been defined as the power vested by the Constitution in the legislature to create laws, whether penal or not, aimed at safeguarding what they judge to be good for and favorable to their constituents.[107] As an aspect of police power is maintaining social order, "the legislature may even forbid and penalize acts formerly considered innocent and lawful provided that no constitutional rights [are] abridged."[108] Laws enacted in the exercise of police power find justification in the saying *salus populi est suprema lex* (the god of the people is the Supreme Law), which calls one to prioritize the greater good over individual interests.[109] Provided "the means are reasonably necessary for the accomplishment of the [end in view,] not unduly oppressive upon individuals,"[110] and in "the [interest] of the public generally [rather than] of a particular class,"[111] the legislature may adopt such regulations as it deems proper restricting, limiting, and regulating the use of private property in the exercise of its police power.[112]

The Anti-Cybersquatting Provision is an important provision of the Cybercrime Prevention Act of 2012 and is a public order law.

> [Public order] laws were crafted to maintain minimum standards of decency, morality[,] and civility in human society. These laws may be traced all the way back to ancient times, and today, they have also come to be associated with the struggle to improve the citizens' quality of life, which is guaranteed by our Constitution. *Civilly*, they are covered by the 'abuse of rights' doctrine embodied in the preliminary articles of the Civil Code concerning [h]uman [r]elations, to the end, in part, that any person who willfully causes loss or injury to another in a manner that is contrary to morals, good customs, or public policy shall compensate the latter for the damage. This provision is, together with the succeeding articles on human relations, intended to embody certain basic principles 'that are to be observed for the rightful relationship between human beings and for the stability of the social order.'
>
> ...

106. Lozano v. Martinez, 146 SCRA 323, 339 (1986) (citing Edu v. Ericta, 35 SCRA 481, 488 (1970)).

107. JOAQUIN G. BERNAS, S.J., THE 1987 CONSTITUTION OF THE PHILIPPINES: A COMMENTARY, 95-98 (1996).

108. People v. Siton, 600 SCRA 476, 485 (2009).

109. *Id.* at 481.

110. United States v. Toribio, 15 Phil. 85, 98 (1910).

111. *Id.*

112. *Id.* at 98-99.

> *Criminally*, public order laws encompass a whole range of acts — from public indecencies and immoralities, to public nuisances, to disorderly conduct. The acts punished are made illegal by their offensiveness to society's basic sensibilities and their adverse effect on the quality of life of the people of society. For example, the issuance or making of a bouncing check is deemed a public nuisance, a crime against public order that must be abated. As a matter of public policy, the failure to turn over the proceeds of the sale of the goods covered by a trust receipt or to return said goods, if not sold, is a public nuisance to be abated by the imposition of penal sanctions. Thus, public nuisances must be abated because they have the effect of interfering with the comfortable enjoyment of life or property by members of a community.[113]

It is not the profit generation *per se* which the Cybercrime Prevention Act of 2012 punishes. The law is not intended or designed to coerce a cybersquatter to sell the subject domain name at cost or lower than his cost of acquisition. The thrust of the law is to "protect and safeguard the integrity of computer, computer and communications systems, networks, and databases, and the confidentiality, integrity, and availability of information and data stored therein, from all forms of misuse, abuse, and illegal access by making punishable under the law such conduct or conducts."[114] This law punishes the act of cybersquatting not as an offense against property, but as an offense against public order.

It is certainly within the prerogative of the lawmaking body to prohibit the unauthorized obtaining of domain names bearing others' registered trademarks or personal names, tantamount to acts inimical to public welfare. Perhaps the act itself may not be inherently immoral. Nevertheless, it may become punishable should the State deem it wise to treat is as such. As the Supreme Court has previously held,

> [a]cts *mala in se* are not the only acts which the law can punish. An act may not be considered by society as inherently wrong, hence, not *malum in se*, but because of the harm that it inflicts on the community, it can be outlawed and criminally punished as *malum prohibitum*. The state can punish acts *malum prohibitum* in the exercise of its police power.[115]

The enactment of the Cybercrime Prevention Act of 2012, particularly its Anti-Cybersquatting Provision, is a declaration by the legislature that, as a matter of public policy, abusing the integrity of computer and communications systems is deemed a public nuisance to be abated by the

---

113. *Siton*, 600 SCRA at 494-96 (citing PHIL. CONST. art. VI, § 5; CIVIL CODE, art. 19; Sea Commercial Company, Inc. v. Court of Appeals, 319 SCRA 210, 222 (1999); Ruiz v. People, 475 SCRA 476, 489 (2005); & Tiomico v. Court of Appeals, 304 SCRA 216, 223 (1999)) (emphasis omitted).

114. Cybercrime Prevention Act of 2012, § 2.

115. *Lozano*, 146 SCRA at 338.

imposition of penal sanctions. Considering the factual and legal antecedents that led to the adoption of this legal provision against cybersquatting, it is not difficult to understand the public concern which prompted its enactment.

IV. EFFECTIVE IMPLEMENTATION OF THE ANTI-CYBERSQUATTING PROVISION

The Anti-Cybersquatting Provision, although sufficient on its own to withstand constitutionality issues, is on its face far from complete in substance for effective implementation. The prosecution of cybersquatters should be guided by the following parameters.

A. Prescribing the Standards of the "Bad Faith" Element

As defined in the Anti-Cybersquatting Provision, cybersquatting is "the acquisition of a domain name over the Internet [(i.e., domain name registration)] in bad faith to profit, mislead, destroy reputation, and deprive others from registering the same."[116] The primary element of the Anti-Cybersquatting Provision is bad faith, without which an act of domain name registration may not be considered as cybersquatting. Bad faith generally implies or involves "dishonesty of belief or purpose."[117] However, bad faith in the Anti-Cybersquatting Provision is not used in its general sense. The Anti-Cybersquatting Provision's bad faith element may only be considered present if the domain name registration was attended by the cybersquatter's intention to profit, mislead, destroy reputation, and deprive others from registering the subject domain name.

Bad faith is apparent if the cybersquatter registers a domain name which is a well-known mark. "In determining whether a mark is a well-known mark, the competent authority shall take into account any circumstances from which it may be inferred that the mark is well known."[118] Some circumstances include prior enforcement of exclusive rights to the mark by the owner, the length and and place of registration of such mark, the prevalence of the mark in certain sectors of society, the mark's value, etc.[119]

> Well-known trade and service marks enjoy in most countries protection against signs[,] which are considered a reproduction, imitation, or translation of that mark[,] provided that they are likely to cause confusion in the relevant sector of the public. Well-known marks are usually protected, irrespective of whether they are registered or not, in respect of

116. Cybercrime Prevention Act of 2012, § 4 (a) (6).

117. BLACK'S LAW DICTIONARY 134 (7th ed. 1999).

118. World Intellectual Property Organization (WIPO), Determination of Well-Known Marks, *available at* http://www.wipo.int/about-ip/en/development_iplaw/pub833-02.htm#TopOfPage (last accessed Feb. 28, 2013).

119. *Id.* art. 2 (1) (b).

> goods and services[,] which are identical with, or similar to, those for which they have gained their reputation. In many countries, they are also, under certain conditions[,] protected for dissimilar goods and services.[120]

To illustrate, "Jollibee" is a well-known mark and the mere use of any mark, most especially in the Philippines, that includes "JOLLI" or "JOLLY" would immediately cause consumers to believe that the goods or services offered under the mark are sponsored by Jollibee.

> [S]ince the first Jollibee was opened in the 1970s, Jollibee already used the JOLLIBEE mark to distinguish its services from those of other food establishments. Jollibee continues to use the JOLLIBEE mark in each Jollibee outlet and in almost all product packaging, advertising[,] and in promotional materials. The JOLLIBEE mark has become so well known in the Philippines that the mere use of the mark that includes 'JOLLI' or 'JOLLY' would immediately cause consumers to believe that the goods or services offered under the mark are sponsored by Jollibee.[121]

WIPO even cited the Jollibee trademark as a global exemplar for successful franchising business.[122] Obviously, the domain name jollibee.com should rightfully belong to the trademark owner of Jollibee, and any registration of domain names identical or confusingly similar thereto is considered as cybersquatting. The cybersquatter is considered in bad faith upon his registration of jollibee.com because he may not feign ignorance of the existence of this well-known mark, implying that another person or entity already owns this famous mark. By registering a domain name which represents a famous mark, the cybersquatter profits through increased traffic to his website from mistaken hits that may translate to commissions from advertisements exhibited therein. Being a gTLD (.com), this domain name will be the first website address to come to mind for those searching for the Jollibee brand online. This misleads the online searcher that the said website and any of its contents are owned, controlled, maintained, or sponsored by the famous brand. It likewise destroys the reputation of the famous brand because of its seeming intellectual property control system lapse. Since a domain name is unique, the cybersquatter has effectively deprived the well-known brand from registering the same. Clearly, bad faith may be presumed in cases of unauthorized domain name registrations of well-known marks.

For domain name registration of personal names or trademarks other than well-known marks, bad faith has to be clearly shown to prove cybersquatting through the cybersquatter's intention to profit, mislead,

---

120. WIPO, Well-known marks, *available at* http://www.wipo.int/sme/en/ip_business/marks/well_known_marks.htm (last accessed Feb. 28, 2013).

121. Jollibee Food Corporation v. Atlas Publishing Company Inc., IPC No. 14-2006-00113, Mar. 7, 2007.

122. WORLD INTELLECTUAL PROPERTY ORGANIZATION, IN GOOD COMPANY: MANAGING INTELLECTUAL PROPERTY ISSUES IN FRANCHISING 48 (2012).

destroy reputation, and deprive others from registering the same domain name.

Unlike in the UDRP where bad faith is deemed present upon proof of any of the reasons mentioned (i.e., to profit, mislead, destroy reputation, or deprive others from registering the same domain name),[123] the Anti-Cybersquatting Provision uses the conjunction "and" to mean that it is only upon showing that all these reasons were intended by the cybersquatter during the domain name registration, that the bad faith element may be established. It is elementary in the rules of statutory construction "that when the language of the law is clear and unequivocal[,] the law must be taken to mean exactly what it says."[124] The Anti-Cybersquatting Provision is categorical in using the conjunction "and," leaving no doubt that it intends that all these reasons have to be present to enable one to prove the bad faith element of cybersquatting. Even assuming that there exists an ambiguity in

---

123. *Uniform Domain-Name Dispute-Resolution Policy*, *supra* note 75, ¶ 4 (b). Paragraph 4 (b) of the UDRP Policy states —

> b. *Evidence of Registration and Use in Bad Faith.* For the purposes of Paragraph 4(a)(iii) [in proving that your domain name has been registered and is being used in bad faith], the following circumstances, in particular but without limitation, if found by the Panel to be present, shall be evidence of the registration and use of a domain name in bad faith:
>
> (i) circumstances indicating that you have registered or you have 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 your documented out-of-pocket costs directly related to the domain name; or
>
> (ii) you have 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 you have engaged in a pattern of such conduct; or
>
> (iii) you have registered the domain name primarily for the purpose of disrupting the business of a competitor; or
>
> (iv) by using the domain name, you have intentionally attempted to attract, for commercial gain, [i]nternet users to your [website] or other [online] location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of your [website] or location or of a product or service on your [website] or location.

Id. (emphasis supplied).

124. Insular Bank of Asia and America Employees' Union (IBAAEU) v. Inciong, 132 SCRA 663, 673 (1984).

the construction of the Anti-Cybersquatting Provision, the resulting effect will be the same because that penal provision will be "construed strictly against the government[ ] and literally in favor of the accused."[125] It will be easier for the accused to be acquitted if the prosecution has the burden of proving all the four reasons, rather than just any one of them. However, it behooves us to dissect what comprises each and every reason to fully understand how to establish bad faith in cybersquatting cases. Some of the reasons may be construed to appear as inconsistent against another. What if the cybersquatter merely parked the website bearing the subject domain name and exhibited a blank page therein, is there bad faith even if the registrant is merely waiting for the right time and price in order to offer it for sale? Will a blank website be considered misleading for purposes of establishing bad faith? Is the registrant's use of the domain name to showcase other items not within the same product or service line of the complainant, or even in some territories where the complainant is not operating, a means to destroy the reputation of the latter?

The Cybercrime Prevention Act of 2012 endeavors to "protect and safeguard the integrity of computer, computer and communication systems, networks, and databases, [ ] and the information and data stored therein from all forms of misuse, abuse, and illegal access."[126] This seeming incongruence between and among the reasons for bad faith may go against the real intention of the law. Where a literal interpretation of any part of a statute would operate unjustly, or lead to absurd results, or is inconsistent with the meaning of an act as a whole, it should be rejected. All laws "should receive a sensible construction,"[127] and if a literal interpretation of general terms would lead to injustice, oppression, or absurdity, it must be presumed that the legislature intended exceptions to its language which would avoid such results.[128] Penal statutes "should receive a sensible construction ... so as to avoid an unjust or an absurd conclusion."[129] Where there is ambiguity, "such interpretation as will avoid inconvenience and absurdity is to be adopted."[130] Every section, provision, or clause of the statute "must be expounded by reference to each other in order to arrive at the effect contemplated by the legislature."[131] The intention of the legislator must be ascertained from the whole text of the law and every part of the act

125. People v. Soriano, 407 SCRA 367, 375 (2003).

126. Cybercrime Prevention Act of 2012, § 2.

127. In Re: Allen, 2 Phil. 630, 641 (1903).

128. *Id.*

129. People v. Rivera, 59 Phil. 236, 242 (1933).

130. Serana v. Sandiganbayan, 542 SCRA 224, 244 (2008).

131. Commissioner of Internal Revenue v. TMX Sales, Inc., 205 SCRA 184, 188 (1992).

is to be taken into view.[132] A statute must be interpreted "as a whole [ ] under the principle that the best interpreter of a statute is the statute itself."[133]

> Legislative intent must be ascertained from a consideration of the statute as a whole. The particular words, clauses[,] and phrases should not be studied as detached and isolated expressions, but the whole and every part of the statute must be considered in fixing the meaning of any of its parts and in order to produce harmonious whole. A statute must be so construed as to harmonize and give effect to all its provisions whenever possible. The meaning of the law, it must be borne in mind, is not to be extracted from any single part, portion[,] or section or from isolated words and phrases, clauses or sentences but from a general consideration or view of the act as a whole. Every part of the statute must be interpreted with reference to the context. This means that every part of the statute must be considered together with the other parts, and kept subservient to the general intent of the whole enactment, not separately and independently. More importantly, the doctrine of associated words (*[n]oscitur a [s]ociis*) provides that where a particular word or phrase in a statement is ambiguous in itself or is equally susceptible of various meanings, its true meaning may be made clear and specific by considering the company in which it is found or with which it is associated.[134]

Cybersquatting is defined in the Anti-Cybersquatting Provision as "[t]he acquisition of a domain name over the [I]nternet in bad faith to profit, mislead, destroy reputation, and deprive others from registering the same."[135] It can be inferred that what the law intended to constitute as bad faith is the intention of the cybersquatter to do all the enumerated reasons. Meaning, the bad faith element of the Anti-Cybersquatting Provision is present only upon showing that the cybersquatter was motivated to register the subject domain name by his intention to (1) profit from the domain name registration; (2) mislead the public through the domain name registration; (3) destroy the reputation of the owner of the trademark or personal name which is identical or confusingly similar to that the registered domain name of the cybersquatter; and (4) deprive others from registering the same domain name.

---

132. *See* Aboitiz Shipping Corporation v. City of Cebu, 13 SCRA 449, 453 (1965).

133. Loyola Grand Villas Homeowners (South) Association, Inc. v. Court of Appeals, 276 SCRA 681, 694 (1997).

134. Aisporna v. Court of Appeals, 113 SCRA 459, 466-67 (1982) (citing Araneta v. Concepcion and Araneta, 99 Phil. 709, 712-13 (1956); Tamayo v. Gsell, 35 Phil. 953, 980 (1916); Lopez and Javelona v. El Hogar Filipino, 47 Phil. 249, 286 (1925); People v. Palmon, 86 Phil. 350, 353-54 (1950); & 82 C.J.S. *Statutes* § 399 (Westlaw 2012)).

135. Cybercrime Prevention Act of 2012, § 4 (6).

By virtue of the conjunction "and," the cybersquatter may only be held guilty of cybersquatting if proven beyond reasonable doubt that his intention to register the domain name was due to all of these reasons, and not just one or some of them. No other actual or constructive fraud, or a design to mislead or deceive another, may be able to establish bad faith under the Anti-Cybersquatting Provision. Nevertheless, it is worthwhile to underscore that the Anti-Cybersquatting Provision does not require that the cybersquatter actually profits, misleads, destroys reputation, and deprives others from registering the domain name during the registration of the domain name. It is enough to prove that the cybersquatter was motivated by these reasons in having the subject domain name registered.

The cybersquatter's intention to profit from the domain name registration may be based on the possible number of website visitors the unauthorized use of another's trademark or personal name may attract. It may also be based on a cybersquatter's potential to earn money from pay-per-click advertising, sponsored links (i.e., the website visitor, upon clicking an icon exhibited in the website, will be brought to another website, which is that of the sponsor), re-directs (i.e., the website visitor, upon typing in the domain name in the browser, is led not to the cybersquatter's website but to its sponsor's), or even from the collection of information from visitors for marketing purposes such as names, email and physical addresses, contact numbers, etc.

The cybersquatter's intention to mislead the public through the domain name registration may be seen in his failure to provide contact information, or in his use of a fictitious or false name or contact details in registering the domain name, as well as his ride to fame on the personal names and trademarks of others. His website has a potential of communicating to the public that it and its contents are owned, controlled, maintained, or sponsored by the owner of the trademark or personal name. Unless perhaps the domain name is a generic word not constituting a well-known mark, it may not be believable that the cybersquatter would come up with the exact same word as that of the personal name or trademark owned by another. Arguing that the cybersquatter maintains the website blank should not negate intent to mislead because the Anti-Cybersquatting Provision looks at bad faith only upon domain name registration; use thereof at any point in time is immaterial.

The cybersquatter's intention to destroy the reputation of the owner of the trademark or personal name may be obvious if the cybersquatter is or acts on behalf of a competitor and uses the subject domain name to sell, advertise, or endorse competing products. There is also the intention to destroy reputation if the domain name was created to criticize (subject to fair use) the products and services of other persons or entities who own the trademark or personal name identical or confusingly similar to that being used as a domain name.

Last, and arguably the easiest to prove among the reasons constituting bad faith, is the cybersquatter's intention to deprive others from registering the same domain name. Indeed, there "cannot be two identical second-level domains under the same [TLD]."[136] Once the cybersquatter registers a domain name using identical letters or words of another's trademark or personal name, the real owner thereof may no longer register an exactly the same domain name. There is always deprivation of use of a domain name for the real owner, even if the cybersquatter just leaves the website blank, or provides no or false names and contact information upon domain name registration.

B. Other Punishable Acts in Cybersquatting

The scope of the Anti-Cybersquatting Provision extends to "[a]ny person who willfully abets or aids in the commission" of cybersquatting,[137] and even to him who "willfully attempts to commit" cybersquatting.[138]

An act of a person who aids or abets in cybersquatting (which is *malum prohibitum*) may be tantamount to the acts of an accomplice in cases of *mala in se*. An accomplice is "one who knows the criminal design of the principal and cooperates knowingly or intentionally therewith by an act which, even if not rendered, the crime would be committed just the same."[139] For one to be considered an accomplice, "two elements must be present: (1) the community of criminal design, that is, knowing the criminal design of the [cybersquatter], he concurs with the latter in his purpose and (2) the performance of previous or simultaneous acts that are not indispensable to the commission of the crime."[140]

Applying this principle in cybersquatting, a person may be considered as aiding or abetting the commission of cybersquatting if he knows that the domain name to be registered is identical or confusingly similar to another person's existing registered trademark, well-known mark, or personal name, and he still allows the cybersquatter to name himself as the domain name registrant or use his mailing or email address, contact numbers, or other information as may be required in applying for domain name registration.

Aiding or abetting cybersquatting may be readily apparent if the accomplice was directly assisting the cybersquatter in his domain name registration pursuit, through acts such as supplying the cybersquatter with the

136. Lichtenberg & Solomon, *supra* note 15, at 36 (citing Tysver, *supra* note 23).

137. Cybercrime Prevention Act of 2012, § 5 (a).

138. *Id.* § 5 (b).

139. People v. Corbes, 270 SCRA 465, 472 (1997) (citing People v. Lingad, 98 Phil. 5, 12 (1955)).

140. People v. Tamayo, 389 SCRA 540, 554 (2002).

necessary information needed in the application, reserving the domain name in preparation for its registration by the cybersquatter, or advising on how to perpetrate cybersquatting. It may also be construed as aiding or abetting cybersquatting if the accomplice permitted the cybersquatter to use his credit card, Paypal, or other payment instruments to pay for any of the domain name registration fees.

An attempt to commit cybersquatting is also punishable. A person is guilty of an attempt to commit a crime when he begins the execution of his purpose but does not realize the consummation of his object because of reasons outside his will and not because of his own voluntary desistance.[141] There may be an attempt to commit cybersquatting if a person already submitted for registration his domain name application bearing all the required details for registration, but such application was not processed because the website of the domain name registrar timed out (and not because the applicant retracted his application). It is also possible to commit attempted cybersquatting if all necessary information for domain name registration was submitted to the domain name registrar but the company of the credit card used for paying the registration fees did not clear the transaction for payment.

C. Exceptions to the Scope of Anti-Cybersquatting Provision

The Anti-Cybersquatting Provision is not absolute and may yield to better rights of legitimate domain name registrants. It may not apply to a registrant who has already used the domain name in legitimate commerce prior to the notice of a cybersquatting case against him, or where the name used is a dictionary term and the domain name is used for nonprofit (or even profit-oriented)[142] pursuits. A domain name registrant may not be considered performing acts of cybersquatting if the use of his website is considered as "fair use," much more if the complainant has no legitimate rights over the domain name tantamount to reverse domain name hijacking. This Section of the Article tackles the various exceptions applicable to the Anti-Cybersquatting Provision.

(1) Before any dispute notice to the registrant, he already used, or demonstrated 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.[143]

141. United States v. Luna, 4 Phil. 269, 270 (1905).

142. Netrepreneur Connections Enterprises, Inc. v. Anton Sheker, Seo.Com.Ph, No. DPH2011-0003, ¶ 6 (c) (WIPO Arb. Mediation Ctr. 2011), *available at* http://www.wipo.int/amc/en/domains/decisions/word/2011/dph2011-0003.doc (last accessed Feb. 28, 2013).

143. *Uniform Domain-Name Dispute-Resolution Policy*, *supra* note 75, ¶ 4 (c) (i).

An amateur Internet beauty contest operator in New Jersey, U.S. retained his registration over MissWorld.com,[144] where dispute notice was only received by him upon filing of the real Miss World contest organizer's complaint in January 2001, and not through its public relations officer's August 1996 offer to buyout the domain name for $500.00 (there being no other communications by the parties between these dates).[145]

Demonstrable preparations to use the domain name in dispute were found in the "World.com Project" aimed at creating a network of geographical related websites which included Madrid.com,[146] "The Jolt Network" for online entertainment justifying the acquisition of jolt.com and jolt.net,[147] and in the plan to create pi.com as an online office support Internet portal providing secretaries and executives with a range of services such as concierge services and travel bookings.[148]

Legitimate interests over pwc.com[149] were present upon showing that it was "employed in conjunction with an advertising subscription database, operated by a third party advertising consolidator, to return search results from the database on the basis of correspondence between terms in the domain names and search terms for which advertisers have paid subscriptions on a performance basis."[150] In another notable case, fuji.com was successfully defended by its registrant, a U.S.-based wine and cigar publisher, against the more famous Japanese photography company after showing that the former has used and or traded using the corporate name Fuji since 1992 for goods and services different from photography.[151]

---

144. At present, this domain name is already being used by the real Miss World contest organizer.

145. Miss World (Jersey) Limited v. Gerald Goldfaden, No. D2001-0113, 2001 WL 1705481, ¶ 6.8-7.2 (WIPO Arb. Mediation Ctr. Apr. 6, 2001).

146. Empresa Municipal Promoción Madrid S.A. v. Easylink Services Corporation, No. D2000-0409, 2003 WL 1473743, at *9 (WIPO Arb. Mediation Ctr. Feb. 26, 2003).

147. The Jolt Company v. Digital Milk, Inc., Case No. D2001-0493, 2001 WL 1701021, ¶ 6 (B) (WIPO Arb. Mediation Ctr. Aug. 2, 2001).

148. Physik Instrumente GMBH. & Co. v. Stefan Kerner and Jeremy Kerner and Magic Moments Design Limited, No. D2000-1001, 2000 WL 35642119, at *13 (WIPO Arb. Mediation Ctr. Oct. 3, 2000).

149. At present, this domain name is already being used by PriceWaterhouseCoopers.

150. PWC Business Trust v. Ultimate Search, No. D2002-0087, 2002 WL 1271912, ¶ 4.3 (WIPO Arb. Mediation Ctr. May 22, 2002).

151. Fuji Photo Film Co. Limited and Fuji Photo Film USA Inc. v. Fuji Publishing Group LLC, No. D2002-1110, 2000 WL 35595625, at *5 (WIPO Arb. Mediation Ctr. July 2, 2000).

(2) The registered domain name is comprised of a dictionary term, not aimed to profit from and exploit a registered trademark.[152]

A common, generic word may be registered as domain name, provided it does not capitalize on the goodwill created by the trademark owner, if any.

> It is not a per se breach of the UDRP to register the trademark of another as a domain name where the trademark is a generic word. The [UDRP] was not intended to permit a party[,] who elects to register as a trademark or service mark a common word[,] to bar all others from using the common word in combination with other common words, unless it is clear that the use involved is seeking to capitalize on the goodwill created by the mark holder.[153]

An individual is allowed to register and use a domain name to attract internet traffic based on the appeal of commonly used descriptive or dictionary terms, in the absence of circumstances indicating that the registrant's aim in registering the disputed domain name is to profit from and exploit one's trademark.[154] Domain names bearing dictionary terms such as *metro*,[155] *lovely girl*,[156] and *visions*[157] were adjudged to rightfully belong to their respective registrants.

(3) The registrant (as an individual, business, or other organization) has been commonly known by the domain name, even if he has acquired no trademark or service mark rights.[158]

An ordinary American web developer with the online nickname "Sting" won against Sting, the world famous singer, over sting.com[159] because he was the original registrant of the domain name. Although the singer is world

---

152. Match.com, LP v. Bill Zag and NWLAWS.ORG, No. D2004-0230, 2004 WL 3255032, ¶ 6 (C) (WIPO Arb. Mediation Ctr. June 2, 2004).

153. *Id.* ¶ 6 (B).

154. National Trust for Historic Preservation v. Barry Preston, No. D2005-0424, 2005 WL 5154886, ¶ 6 (C) (WIPO Arb. Mediation Ctr. Aug. 10, 2005).

155. MIP METRO Group Intellectual Property GmbH & Co. KG v. Masoud Ziaie Moayyed, No. DIR2007-0005 (WIPO Arb. Mediation Ctr. Feb. 15, 2008), *available at* www.wipo.int/amc/en/domains/decisions/word/2007/dir2007-0005.doc (last accessed Feb. 28, 2013).

156. Porto Chico Stores, Inc. v. Otavio Zambon, No. D2000-1270, 2000 WL 35643678 (WIPO Arb. Mediation Ctr. Nov. 15, 2000).

157. Weather Shield MFG., Inc. v. Lori Phan, No. D2007-1247, 2007 WL 4173478 (WIPO Arb. Mediation Ctr. Oct. 10, 2007).

158. *Uniform Domain-Name Dispute Resolution Policy*, *supra* note 75, ¶ 4 (c) (ii).

159. At present however, this domain name is already being used by the world-famous singer Sting.

famous under the name "Sting," it is not his personal name and it does not follow that he has exclusive rights to "Sting" as a trademark or service mark.[160]

Is being known under a particular name tantamount to having rights in that name as a trademark or service mark? Some famous personalities like actress Julia Roberts,[161] author Jeanette Winterson,[162] and investment banker Steven Rattner[163] were able to recover the domain names bearing their names from cybersquatters. The name of a famous or at least widely known person was considered as constituting an unregistered trademark or service mark sufficient for purposes of opposing cybersquatters.[164] WIPO, on the other hand, espouses a different view:

> [T]he *Report of the WIPO Internet Domain Name Process* of [30 April 1999], on which ICANN based the Uniform Policy, at paragraphs 165-168, states as follows:
>
> The preponderance of views, however, was in favor of restricting the scope of the procedure, at least initially, in order to deal first with the most offensive forms of predatory practices and to establish the procedure on a sound footing. Two limitations on the scope of the procedure were, as indicated above, favored by these commentators. The first limitation would confine the availability of the procedure to cases of deliberate, bad faith abusive registrations. The definition of such abusive registrations is discussed in the next section. The second limitation would define abusive registration by reference only to trademarks and service marks. *Thus, registrations that violate trade names, geographical indications*[,] *or personality rights would not be considered to fall within the definition of abusive registration for the purposes of the administrative procedure.* Those in favor of this form of limitation pointed out that the violation of trademarks (and service marks) was the most common form of abuse and that the law with respect to trade names, geographical indications[,] and personality rights is less evenly harmonized throughout the world, although international norms do exist requiring the protection of trade names and geographical indications. We are persuaded by the wisdom of proceeding firmly but cautiously and of tackling, at the first stage, problems which all agree require a solution. ... [W]e consider that it is premature to extend the notion of abusive registration beyond the violation of trademarks and service marks at this stage. After experience has been gained with the operation of the

160. Gordon Sumner, P/K/A Sting v. Michael Urvan, No. D2000-0596, 2000 WL 33939204, ¶ 6.5 (WIPO Arb. Mediation Ctr. July 24, 2000).

161. *Julia Fiona Roberts*, 2000 WL 33674395.

162. Jeanette Winterson v. Mark Hogarth, D2000-0235, 2000 WL 33674403 (WIPO Arb. Mediation Ctr. May 22, 2000).

163. Steven Rattner v. BuyThisDomainName (John Pepin), No. D2000-0402, 2000 WL 35595516 (WIPO Arb. Mediation Ctr. July 3, 2000).

164. *Gordon Sumner, P/K/A Sting*, 2000 WL 33939204.

> administrative procedure and time has allowed for an assessment of its efficacy and of the problems, if any, which remain outstanding, the question of extending the notion of abusive registration to other intellectual property rights can always be re-visited.
>
> It is clear from this statement that personality rights were not intended to be made subject to the proposed dispute resolution procedure. In adopting the procedure proposed in the WIPO Report, ICANN did not vary this limitation on its application. It must be concluded, therefore, that ICANN did not intend the procedure to apply to personality rights.[165]

Commonly used fairly short, non-fanciful names such as *Gail*,[166] *Tammy*,[167] and *Donna*[168] may be registered as domain names on a first-come, first-served basis, as long as the registrant does not use that domain name in a related field to any registered trademark using the same name.

> (4) 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.[169]

The concept of fair use is commonly applied in the law of copyright.[170] Fair use has been defined as a privilege to use the copyrighted material in a reasonable manner without the consent of the copyright owner or as copying the theme or ideas rather than their expression.[171] The IP Code itself has provisions on fair use:

> Section 185. *Fair Use of a Copyrighted Work.* — 185.1. The fair use of a copyrighted work for criticism, comment, news reporting, teaching including multiple copies for classroom use, scholarship, research, and similar purposes is not an infringement of copyright. Decompilation, which is understood here to be the reproduction of the code and translation of the forms of the computer program to achieve the inter-operability of an independently created computer program with other programs may also

165. *Id.* ¶ 6.4 (citations omitted) (emphasis supplied).

166. Gail Guarulhos Indústria e Comércio Ltda. v. Kevin Watson, No. D2006-0655, 2006 WL 4006149 (WIPO Arb. Mediation Ctr. July 7, 2006).

167. Etam, PLC v. Alberta Hot Rods, No. D2000-1654, 2001 WL 1705280 (WIPO Arb. Mediation Ctr. Jan. 31, 2001).

168. Rusconi Editore S.P.A. v. FreeView Publishing Inc., No. D2001-0875, 2001 WL 1701265 (WIPO Arb. Mediation Ctr. Oct. 10, 2001).

169. *Uniform Domain-Name Dispute-Resolution Policy*, *supra* note 75, ¶ 4 (c) (iii).

170. *See generally* Habana v. Robles, 310 SCRA 511 (1999) & ABS-CBN Broadcasting Corporation v. Philippine Multi-Media System Inc., 576 SCRA 262 (2009).

171. 18 AM. JUR. 2D *Copyright* § 78 (Westlaw 2012).

constitute fair use. In determining whether the use made of a work in any particular case is fair use, the factors to be considered shall include:

(a) the purpose and character of the use, including whether such use is of a commercial nature or is for non-profit educational purposes;

(b) the nature of the copyrighted work;

(c) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and

(d) the effect of the use upon the potential market for or value of the copyrighted work.[172]

There is also "fair use" in using in good faith one's own name, address, pseudonym, or a geographical name, or exact indications concerning the kind, quality, quantity, destination, value, place of origin, or time of production or of supply, of one's goods or services, so long as such use is confined to the purposes of mere identification or information and will not mislead the public as to the source of the goods or services.[173]

This fair use doctrine applies in cyberspace as it does in the real world,[174] and also in connection with trademarks. Trademark fair use is "permissible, unauthorized use of another's name, logo, or other type of mark"[175] in domain names, metatags, keywords, hyperlinks, etc. on the Internet.

Certain domain names deemed confusingly similar to registered trademarks may be fairly used for noncommercial criticism, commentary, parody, fan, and not-for-profit[176] sites. Covancecampaign.com was not ordered to be transferred to the trademark owner of "Covance" because the domain was used for a noncommercial criticism site of Covance. Additionally, there was a bold disclaimer making it clear from the very outset that such site has no connection with the trademark owner.[177] Garyjennings.com was not awarded to the estate of the author Gary Jennings upon the domain name registrant's showing that the domain was being used for providing reviews of the author's works and by indicating in the website

172. INTELLECTUAL PROPERTY CODE, § 185.

173. *See* INTELLECTUAL PROPERTY CODE, § 148.

174. Brookfield Communications, Inc. v. West Coast Entertainment Corporation, 174 F.3d 1036, 1065 (9th Cir. 1999) (U.S.).

175. Philip J. Greene, *Questioning Faith — An Examination of the Fair Use Defense within Internet Domain Name Disputes, and the Role of Good or Bad Faith*, LOY. U. NEW ORLEANS SCH. L. — L. & TECH. ANN., Vol. 4 2004, at 45.

176. Avnet, Inc. v. AV-Network, Inc., No. D2000-0097, 2000 WL 33709223, ¶¶ 6.5 & 6.8 (WIPO Arb. Mediation Ctr., Apr. 25, 2000).

177. Covance, Inc. and Covance Laboratories Ltd. v. The Covance Campaign, No. D2004-0206, 2004 WL 3255081, at *9-10 (WIPO-Arb. Mediation Ctr. Apr. 30, 2004).

that it is not affiliated or endorsed by the author.[178] Also, gormiti.mobi was used as a noncommercial fan site for "Gormiti" toys from Italy, but the absence of any evidence of a commercial intent behind the domain name registration and use disabled the trademark owner from recovering the domain name based on fair use.[179]

The owner of the trademark "Harry Winston," a very well-known, longstanding trademark for fine jewelry, diamonds, and timepieces, lost to the luxury pet boutique owner of Winston, a hairy dog, over the domain name hairywinston.com, after the latter proved that her intention in registering and using the domain name was to parody the famous name and trademark which would successfully differentiate the parody from the original so as to obviate any significant risk of confusion or deception.[180]

In *Chelsea and Westminister Hospitals NHS Foundation Trust v. Frank Redmond*,[181] the WIPO Arbitration and Mediation Center held that a domain name registrant

> has a right or legitimate interest in a domain name, which is identical or confusingly similar to a registered mark of another party [based on fair use] if (a) the domain name has been registered and is being used genuinely for the purpose of criticising the owner of the mark; (b) the registrant believes the criticism to be well-founded; (c) the registrant has no intent for commercial gain; (d) it is immediately apparent to Internet users visiting the website at the domain name that it is not a website of the owner of the mark; (e) the respondent has not registered all or most of the obvious domain names suitable for the owner of the mark; (f) where the domain name is one of the obvious domain names suitable for the owner of the mark, a prominent and appropriate link is provided to the latter's website (if any); and (g) where there is a likelihood that email intended for the complainant will be sent using the domain name in issue, senders are immediately alerted in an appropriate way that their emails have been misaddressed.[182]

178. Estate of Gary Jennings and Joyce O. Servis v. Submachine and Joe Ross, No. D2001-1042, 2001 WL 1701386, at *5-6 (WIPO Arb. Mediation Ctr. Oct. 25, 2001).

179. Giochi Preziosi S.P.A. v. VGMD NetWeb S.L., No. D2009-0542, 2009 WL 2143120, at *6 (WIPO Arb. Mediation Ctr. July 2, 2009).

180. Harry Winston Inc. and Harry Winston S.A. v. Jennifer Katherman, No. D2008-1267, 2008 WL 4893618, at *7 (WIPO Arb. Mediation Ctr. Oct. 18, 2008).

181. Chelsea and Westminister Hospital NHS Foundation Trust v. Frank Redmond, No. D2007-1379, 2007 WL 4687994 (WIPO Arb. Mediation Ctr. Nov. 14, 2007).

182. *Chelsea and Westminister Hospital NHS Foundation Trust*, 2007 WL 4687994, at *7-8.

(5) Reverse Domain Name Hijacking

Reverse Domain Name Hijacking is the use of the UDRP Policy "in bad faith to attempt to deprive a registered domain name holder of a domain name."[183] To prevail on such a claim, a respondent must show that the complainant knew of the respondent's unassailable rights or legitimate interests in the disputed domain name or the clear lack of bad faith registration and use, and nevertheless brought the complaint in bad faith.[184]

> The allegation of Reverse Domain Name Hijacking is also an allegation of bad faith and therefore needs to be looked at very carefully. What is meant by 'bad faith' in this context? Clearly, the launching of an unjustifiable [c]omplaint with malice aforethought qualifies, as would the pursuit of a [c]omplaint after the [c]omplainant knew it to be insupportable. This Panel takes the view that 'bad faith' in this context extends also to a person who, while maybe not knowing an allegation to be insupportable, makes the allegation reckless as to whether it is supportable or not.
>
> ...
>
> Putting this in the kindest light that the Panel can, the Panel believes that in its eagerness to obtain the [d]omain [n]ame[,] the [c]omplainant lost all sense of proportion. It took on the guise of a third rate barrack room lawyer and advanced arguments that were tortuously artificial in the extreme, reckless both as to [ ] the justification for making those arguments and the seriousness of the overall charge against the [r]espondent, who was manifestly no cybersquatter. This [c]omplaint was a clear abuse of the [p]olicy designed to deprive the [r]espondent of her domain name. The allegations of bad faith were without substance and should never have been made.[185]

There was no Reverse Domain Name Hijacking where Clorox Co.'s actions in contacting the 17-year old domain name registrant at his school were motivated not by an attempt to harass and intimate, but rather, by an attempt to establish contact using the contact address provided in the domain name registration form for clorox.org.[186] Moreover, "[a]s the owner of the registered, if not famous, CLOROX mark, Clorox Co. was entitled to take

183. ICANN, *Rules for Uniform Domain-Name Dispute-Resolution Policy*, ¶ 1 (Oct. 30, 2009), *available at* http://www.icann.org/en/help/dndr/udrp/rules (last accessed Feb. 28, 2013).

184. Sydney Opera House Trust v. Trilynx Pty. Limited, No. D2000-1224, 2000 WL 35643705, at *7 (WIPO Arb. Mediation Ctr. Oct. 31, 2000).

185. Smart Design LLC v. Carolyn Hughes, No. D2000-0993, 2000 WL 35641491, at *15 (WIPO Arb. Mediation Ctr. Oct. 18, 2000).

186. The Clorox Company v. Marble Solutiohs A/K/A Adam Schaeffer, No. D2001, 2001 WL 1701300, at *4 (WIPO Arb. Mediation Ctr. Nov. 20, 2001).

whatever reasonable steps it deemed necessary to protect its trademark rights."[187]

D. Augmenting the Perceived Deficiencies in the Anti-Cybersquatting Provision

The Philippine Cybercrime Law did not define "trademark" for purpose of the Anti-Cybersquatting Provision. However, "it is an elementary rule [in statutory construction] that when the law speaks in clear and categorical language, there is no need, in the absence of legislative intent to the contrary, for any interpretation."[188] Words and phrases used in a statute "should be given their plain, ordinary, and common usage meaning."[189] Thus, "trademark" should necessarily mean "a distinctive sign which identifies certain goods or services as those produced or provided by a specific person or enterprise."[190] Cybersquatting may be committed if the subject domain name is identical or confusingly similar to a registered trademark or service mark.

On the other hand, the Anti-Cybersquatting Provision uses "domain name" in its dictionary meaning which refers to "a name [ ] that is the primary [i]nternet address for a website [(e.g., Merriam-Webster.com)]."[191] To constitute as cybersquatting, the domain name must be one of these four types:

(1) Type one: Domain name is identical or similar to a trademark registered with the appropriate government agency as of the date of domain name registration;[192]

(2) Type two: Domain name is identical or similar with the name of a natural person other than the registrant;[193]

(3) Type three: Domain name is acquired without right;[194] or

187. *Id.* at *4.

188. Domingo v. Commission on Audit, 297 SCRA 163, 168 (1998).

189. Mustang Lumber Inc. v. Court of Appeals, 257 SCRA 430, 448 (1996) (citing RUBEN E. AGPALO, STATUTORY CONSTRUCTION 131 (2d ed. 1990)).

190. World Intellectual Property Organization, Intellectual Property — some basic definitions, *available at* http://www.wipo.int/about-ip/en/studies/publications/ip_definitions.htm (last accessed Feb. 28, 2013).

191. Merriam-Webster Incorporated, Merriam Webster Word Central, *available at* http://www.wordcentral.com/cgibin/student?book=Student&va=domain%20name (last accessed Feb. 28, 2013).

192. Cybercrime Prevention Act of 2012, § 4 (6) (i).

193. *Id.* § 4 (6) (ii).

194. *Id.* § 4 (6) (iii).

(4) Type four: Domain name is acquired with intellectual property interests in it.[195]

Several questions arise from this enumeration. In type one, trademark registration with which "appropriate government agency" is needed: Intellectual Property Office of the Philippines or in any other intellectual property offices in the world? If the Anti-Cybersquatting Provision refers merely to IPO Philippines, it will effectively weaken the protection of well-known marks not registered in the Philippines. In type two, does the owner of personal name need to be alive at the time of domain name registration? How about celebrities and other famous persons who have passed away? Type three appears straightforward because a quick reference to the Cybercrime Prevention Act of 2012's definition of terms will enable us to understand that a domain name is "acquired without right" if domain name registration was undertaken without or in excess of authority or not covered by established legal defenses, excuses, court orders, justifications, or relevant principles under the law.[196] However, type four creates even more confusion by leaving the courts to guess on the meaning of "intellectual property interests." Does it pertain to pecuniary interests or intellectual property rights? If it pertains to intellectual property rights, what sets it apart from type three?

Cybersquatting is also committed by registering in bad faith domain names identical or similar with a personal name belonging to one other than the registrant. The term "personal name" obviously includes complainant's name duly registered with the relevant civil registrar,[197] and should also cover nicknames or aliases. It is appropriate, for example, for the family of Philippine's king of comedy, Dolphy, to claim registration rights over his more popular nickname, although his real name is Rodolfo Vera Quizon, Sr.[198]

A person who acquires a domain name from its original or subsequent registrants should likewise be covered by the Anti-Cybersquatting Provision or the Philippine Cybercrime Law even if he has not been registered as domain name owner thereof. Upon the consummation of the sale, donation, or transfer, the existing domain name registrant will have to access his domain name's registration record to reflect that the buyer, donee, or transferee has acquired the domain name from him; and that the transferee

195. *Id.*

196. *Id.* § 3 (h).

197. Republic of the Philippines v. Court of Appeals, 209 SCRA 189, 195-96 (1992).

198. Agence France Presse, et al., *Curtains down for Dolphy at 83*, GMA NEWS, July 10, 2012, *available at* http://www.gmanetwork.com/news/story/264905/news/nation/curtains-down-for-dolphy-at-83 (last accessed Feb. 28, 2013).

should be the new registrant of record for that domain.[199] This is still "domain name registration" as an element of cybersquatting. It is upon the registration of the new domain name registrant when the transferee's bad faith intent will be assessed.

The Cybercrime Prevention Act of 2012 punishes the act of cybersquatting by imprisonment and fine.[200] In spite of the silence as to the cybersquatter victim's right to claim for civil damages against the cybersquatter and/or the domain name registrar or registry in case of bad faith or reckless disregard of the victim's rights over the domain name, this remedy is still available because (1) "every person who, contrary to law, wilfully [ ] causes damage to another, shall indemnify the latter for the same,"[201] and (2) "every person criminally liable is also civilly liable."[202] The cybersquatting victim is entitled to claim for all damages[,] which are the natural and probable consequences of cybersquatting.[203]

> Generally, the basis of civil liability arising from crime is the fundamental postulate of our law that '[e]very man criminally liable is also civilly liable.' Underlying this legal principle is the traditional theory that when a person commits a crime he offends two entities[,] namely[:] (1) the society in which he lives in or the political entity called the State whose law he had violated; and (2) the individual member of that society whose person, right, honor, chastity[,] or property was actually or directly injured or damaged by the same punishable act or omission. However, this rather broad and general provision is among the most complex and controversial topics in criminal procedure. It can be misleading in its implications especially where the same act or omission may be treated as a crime in one instance and as a tort in another or where the law allows a separate civil action to proceed independently of the course of the criminal prosecution with which it is intimately intertwined. Many legal scholars treat as a misconception or fallacy the generally accepted notion that the civil liability actually arises from the crime when, in the ultimate analysis, it does not. While an act or

199. INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS, BEGINNER'S GUIDE TO DOMAIN NAMES 12 (2010).

200. Cybercrime Prevention Act of 2012, § 8. The Cybercrime Prevention Act of 2012 states:

> Section 8. *Penalties.* — Any person found guilty of any of the punishable acts enumerated in Sections 4 (a) and 4 (b) of this Act shall be punishable with imprisonment of *prision mayor* or a fine of at least [₱200,000.00] up to a maximum amount commensurate to the damage incurred or both.

Id.

201. CIVIL CODE, art. 20.

202. An Act Revising the Penal Code and Other Penal Laws [REVISED PENAL CODE], Act No. 3815, art. 100 (1932).

203. CIVIL CODE, art. 2202.

> omission is felonious because it is punishable by law, it gives rise to civil liability not so much because it is a crime but because it caused damage to another. Viewing things pragmatically, [it can readily be seen] that what gives rise to the civil liability is really the obligation and the moral duty of everyone to repair or make whole the damage caused to another by reason of his own act or omission, done intentionally or negligently, whether or not the same be punishable by law. In other words, criminal liability will give rise to civil liability only if the same felonious act or omission results in damage or injury to another and is the direct and proximate cause thereof. Damage or injury to another is evidently the foundation of the civil action. Such is not the case in criminal actions for, to be criminally liable, it is enough that the act or omission complained of is punishable, regardless of whether or not it also causes material damage to another.
>
> Article 20 of the New Civil Code provides: 'Every person who, contrary to law, wilfully or negligently causes damage to another, shall indemnify the latter for the same.'
>
> Regardless, therefore, of whether or not a special law so provides, indemnification of the offended party may be had on account of the damage, loss[,] or injury directly suffered as a consequence of the wrongful act of another. [ ] Every crime gives rise to a penal or criminal action for the punishment of the guilty party, and also to civil action for the restitution of the thing, repair of the damage, and indemnification for the losses.[204]

The verdict of guilt for cybersquatting may contain an order authorizing the cancellation of the cybersquatter's registration over the domain name, and its confiscation and transfer in favor of the cybersquatting victim.[205] Although this has legal basis, the court hearing the cybersquatting case does not have jurisdiction over the person of the domain name registrar, and may not be in a position to mandate the latter to cause the cancellation or transfer. Hence, any decision to cancel or transfer domain name registration is at most suggestive, but should nevertheless be considered as a proof of

---

204. Banal v. Tadeo Jr., 156 SCRA 325, 329-30 (1987) (citing REVISED PENAL CODE, art. 100; Quemel v. Court of Appeals, 22 SCRA 44, 46 (1968); & United States v. Bernardo, 19 Phil. 265, 295 (1911)).

205. REVISED PENAL CODE, art. 45. Article 45 of the Revised Penal Code, states:

> Article 45. *Confiscation and Forfeiture of the Proceeds or Instruments of the Crime.* — Every penalty imposed for the commission of a felony shall carry with it the forfeiture of the proceeds of the crime and the instruments or tools with which it was committed.
>
> Such proceeds and instruments or tools shall be confiscated and forfeited in favor of the Government, unless they be the property of a third person not liable for the offense, but those articles which are not subject of lawful commerce shall be destroyed.

Id.

ownership over the subject domain name, which the domain name registar may use in assessing on whether or not to actually cancel or transfer the domain name registration in favor of the claimant.

It is incumbent upon the Philippine government, perhaps through the Intellectual Property Office of the Philippines in particular, to establish arrangements with domain name registrars to assist in implementing any orders arising from cybersquatting cases to cancel and transfer domain name registration. After all, upon rendering a guilty verdict on cybersquatting, if the cybersquatter will be imprisoned but the domain name he previously registered remains under his ownership and not be transferred to the legitimate claimant, the domain name registration abuse, which the Anti-Cybersquatting Provision seeks to curb is therefore thwarted.

However, if the complaint for cybersquatting is found to be frivolous and declared as a case of Reverse Domain Name Hijacking, the respondent may use the verdict and incidents of the cybersquatting case as evidence in support of a case for malicious prosecution. For a malicious prosecution suit to prosper, the plaintiff must prove the following: (1) that the prosecution did occur, and the defendant was himself the prosecutor or that he instigated its commencement; (2) that the criminal action finally ended with an acquittal; (3) that there was an absence or probable cause; and (4) that the prosecution was impelled by legal malice — an improper or a sinister motive.[206] "Stripped of legal jargon, malicious prosecution means persecution through the misuse or abuse of judicial processes; or the institution and pursuit of legal proceedings for the purpose of harassing, annoying, vexing[,] or injuring an innocent person."[207]

E. Obtaining Jurisdiction Over Cybersquatters by Philippine Courts

The Regional Trial Court [hereinafter trial court] has the authority to try cybersquatting cases.

> Section 21. *Jurisdiction.* — The Regional Trial Court shall have jurisdiction over any violation of the provisions of this Act including any violation committed by a Filipino national regardless of the place of commission. Jurisdiction shall lie if any of the elements was committed within the Philippines or committed with the use of any computer system wholly or partly situated in the country, or when by such commission any damage is caused to a natural or juridical person who, at the time the offense was committed, was in the Philippines.[208]

206. Ponce v. Legaspi, 208 SCRA 377, 388 (1992).

207. Villanueva v. United Coconut Planters Bank, 327 SCRA 391, 400 (2000).

208. Cybercrime Prevention Act of 2012, § 21.

Accordingly, jurisdiction vests upon the trial court upon showing that the cybersquatter is a Filipino citizen[209] during the commission of the act of cybersquatting, regardless of the place of commission. A Filipino citizen is one (1) who is already a Filipino citizen upon the adoption of the Constitution; (2) whose father or mother is a Filipino citizen; (3) born before 17 January 1973 of a Filipino mother and who elected Philippine citizenship upon reaching majority age; and (4) who is a naturalized Filipino.[210] The trial court's jurisdiction over Filipinos worldwide appears to be aspirational rather than practical. If the Filipino cybersquatter is in the Philippines, jurisdiction over his person should not be an issue. However, what will be the treatment if he currently resides in Turkey but he was in the U.S. when he registered the subject domain name? To make this issue more complicated, what if the same cybersquatter who was a Filipino during the commission of cybersquatting is no longer a Filipino citizen upon the filing of the cybersquatting case? To stretch the issue a little further, does the trial court retain jurisdiction over the same cybersquatter even if the trademark infringed upon is a well-known mark owned by a non-Filipino not doing business in the Philippines?

Jurisdiction is also said to vest upon the trial court if any element of cybersquatting was committed within the Philippines. Cybersquatting has the following elements:

(1) There must be an acquisition of a domain name over the Internet (i.e., domain name registration);

(2) The domain name registration was attended with bad faith;

(3) Bad faith was characterized as the intention to profit, mislead, destroy reputation, and deprive others from registering the same domain name; and

(4) The registered domain name is either:

    (a) Identical or similar to a trademark registered with the appropriate government agency as of the date of domain name registration;

    (b) Identical or similar with the name of a natural person other than the registrant;

    (c) Acquired without right; or

    (d) Acquired with intellectual property interests in it.[211]

---

209. A Filipino national means a Filipino citizen. *See generally* Tecson v. Commission on Elections, 424 SCRA 277 (2004).

210. PHIL. CONST. art. IV, § 1.

211. Cybercrime Prevention Act of 2012, § 4 (a) (6).

By not qualifying the types of domain name acquired over the Internet, the domain name being referred to in the Anti-Cybersquatting Provision pertains not only to gTLDs (such as .com) but also to ccTLDs (such as .ph) and IDNs. The domain name registrar of .ph is dotPH Domains, Inc. with address in Pasig City.[212] The trial court may not have jurisdictional issues with .ph being located within the Philippines. This is not the case for .com and other ccTLDs, which are being administered by several independent domain name registrars located outside the Philippines.

The trial court may take cognizance of a cybersquatting case even if a non-Filipino cybersquatter is involved, if he acquired the subject domain name (1) while in the Philippines; (2) using any computer system wholly or partly situated in the Philippines; (3) damaging a natural or juridical person who was in the Philippines upon his cybersquatting; or (4) with bad faith in the context of the Anti-Cybersquatting Provision — meaning, the foreigner upon registering the domain name had the intention to profit from cybersquatting at the expense of a Filipino; mislead Filipinos through that domain name; destroy the reputation of a Filipino individual, partnership, or corporation; deprive a Filipino in registering his name as domain name; and deprive without right a Filipino trademark registrant in registering his trademark as domain name.

Cybersquatting cases are classified as actions *in personam*. Where the action is *in personam*, or one brought against a person on the basis of his personal liability, jurisdiction over the person of the cybersquatter is necessary for the Trial Court to validly try and decide the case. When the defendant is a non-resident of the Philippines, "personal service of summons within the [S]tate where he is essential to the acquisition of jurisdiction over his person."[213]

Jurisdiction over the person of the accused may be acquired through "compulsory process, such as a warrant of arrest, or through his voluntary appearance, such as when he surrenders to the police or to the [Trial Court]."[214] The sheriff or the court process server of the Trial Court may personally serve the compulsory processes if the cybersquatter is within the Philippines. If the cybersquatter is abroad, the Trial Court may seek international mutual assistance and extradition by invoking applicable international instruments on international cooperation in criminal matters for the purposes of investigating or proceeding with the cybersquatting case, or for the collection of evidence in electronic form in relation thereto.[215]

---

212. DotPH: The Official Domain Registry of the Philippines, *available at* http://www.dot.ph/corporate/contactus (last accessed Feb. 28, 2013).

213. Banco do Brasil v. Court of Appeals, 333 SCRA 545, 557 (2000).

214. Miranda v. Tuliao, 486 SCRA 377, 386 (2006).

215. Cybercrime Prevention Act of 2012, § 22.

Judgment in cybersquatting cases is likewise *in personam*, which is binding upon the parties and their successors in interest.[216] The respondent may be imprisoned, and the fine imposed may be enforced against him personally or his estate upon his demise. Where the judgment provides for the forfeiture of the domain name in favor of the complainant in cases of .ph where the domain name registrar is within the Philippines, the same judgment, shall likewise constitute as authority of the domain name registrar to transfer the subject domain name to the complainant. For cybersquatting cases where the relevant domain name registrar is outside the Philippines, that judgment (although recommendatory at best) may serve as proof of ownership over the subject domain name which the domain name registar may use in assessing on whether or not to actually cancel or transfer the domain name registration in favor of the complainant.

V. CONCLUSION

Protecting one's intellectual property assets online is no longer optional during this period of fast-paced internet commerce development. A brand to be resilient ought to possess strong trademarks and strong systems for protecting its trademarks worldwide, whether in the physical world or in cyberspace. The Cybercrime Prevention Act of 2012, which intensifies trademark protection in domain names, is an ambitious contribution by the Philippines to the global fight against cybersquatting by intensifying trademark protection in domain names. The personal name or registered trademark owner is now empowered to fight cybersquatting in an accessible and cost-efficient domestic venue. To vindicate his intellectual property rights, the trademark or personal name owner merely needs to prove that an element of cybersquatting is committed here, and that the cybersquatter registered the domain name in bad faith, regardless of the cybersquatter's subsequent use thereof.

216. Munoz v. Yabut, 650 SCRA 344, 367 (2002).