THE EXEGESIS OF DOMAIN NAME PROTECTION AND CYBERSQUATTING IN NIGERIAN JURISPRUDENCE[1]

Abstract

This paper critically examines Nigeria's legal framework for domain name protection and addresses cybersquatting, with a comparative analysis of international best practices, particularly those of the United States, Kenya, and global regulations like the Uniform Domain Name Dispute Resolution Policy (UDRP). The study also highlights the increasing importance of domain names in the digital economy and the rising threats posed by cybersquatting, a practice where individuals register domain names in bad faith to exploit the goodwill of established trademarks. In Nigeria, the regulatory environment is shaped by the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 and the Trademarks Act, yet enforcement remains weak due to a lack of statutory authority for key regulatory bodies like the Nigerian Internet Registration Association (NIRA), low public awareness, and the absence of reported judicial precedents. An evaluation of the United States' Anti-Cybersquatting Consumer Protection Act (ACPA) and UDRP, alongside Kenya's progressive legal and dispute resolution frameworks, reveals the need for more comprehensive legislation, efficient enforcement mechanisms, and increased awareness in Nigeria. Furthermore, the paper identifies legal and institutional gaps, including subjectivity in dispute resolution, limited control over domain name extensions beyond .ng, and inadequate collaboration between agencies. The paper offers concrete recommendations such as enhancing NIRA's legal authority, adopting a Nigerian equivalent of the UDRP, expanding domain space governance, and implementing culturally sensitive awareness programs. The study underscores that just as physical property requires protection, digital assets must equally be safeguarded through comprehensive, enforceable, and culturally responsive legal frameworks. By doing so, Nigeria can ensure a more secure and trustworthy digital environment that supports innovation, commerce, and intellectual property rights in the digital age.

Keywords: Domain name, cybersquatting, trademarks protection, cyber space

1.0 Introduction

In the digital age, a domain name is more than just a string of letters and numbers- it is a gateway to the internet, a brand, and a valuable asset. As the internet has grown, so has the importance of having an online presence. Whether as an individual, a small business, or a large corporation, the Domain Name System helps one create a unique identity on the web and connect with people around the world. However, this heightened value brings forth vulnerabilities, and opportunistic cyber squatters are quick to exploit these weaknesses.

The registration of a domain name does not require adherence to strict criteria[2], which opens the possibility for individuals to register any name, regardless of whether it is already a trademark[3] owned by another party. This has led to issues for individuals and businesses that

[1]**By David Chukwuebuka Mkpo LLB (Hons), LLM, BL,** Lecturer, Department of International Law and Jurisprudence, Nnamdi Azikiwe University, Awka Anambra State, Nigeria. dc.mkpo@unizik.edu.ng +2347066347477

[2]E. Hurter, 'An evaluation of selected aspects of the alternative dispute resolution regulations for the resolution of domain name disputes in the. Za domain name space' (2007) *SA Mercantile Law Journal. Jan 1;19(2):165-85.*

[3]The World Intellectual Property Organisation (WIPO) defines a trademark as a sign capable of distinguishing the goods and services of one enterprise from those of other enterprises. Furthermore, Section 67(1) of the Trademarks Act Cap T13, Laws of Federation of Nigeria, 2004 defines a trademark as "a mark used or proposed

have registered trademarks, as their names can be registered as domain names by other users including malicious actors and cyber squatters. Given the importance of trademarks and domain names in Nigeria, there is a clear need for the introduction of appropriate legal protections and remedies against infringement by both innocent infringers and cyber squatters.

The purpose of this work is to examine the existing framework of domain name protection and cybersquatting in the Nigerian legal system, identify challenges and gaps in its application, explore domain name systems of other countries, and propose recommendations to enhance the efficacy of these measures in safeguarding digital assets and intellectual property.

2.0 Conceptual and Historical Context

2.1 Conceptual Framework

2.1.1 Domain Name

A domain name has been described as a unique string of keyboard characters that serves as the part of an internet or web address that is legally registered by a particular organisation or individual.[4] It refers to a unique word that is used to identify a particular website or web page on the internet. For examples, http://www.dcmkpo.com is a domain name, "google.com" identifies the website of the search engine, Google. Domain names are also used to send emails and identify other online services, because domain names are intellectual property, they can have enormous monetary value. The generic name business.com, for instance, was sold in 1999 for $7.5 million.[5]

A domain name is made up of several levels of domains. For instance, in the domain Name<works.internet.com.ng>, the <.ng> is called the top or first level domain, the <.com> is the second level domain, the<internet> is the third level domain, and the <works> is the fourth level domain. Multiple levels of domains organize internet addresses hierarchically for easier navigation and management. Top-Level Domains (TLDs) categorize websites by purpose or location, Second-Level Domains (SLDs) further specify entities, and subdomains create site sections.[6] Every domain name corresponds to one or more Internet Protocol (IP) addresses, which are the numbers that computers use to locate websites on the internet.[7]

2.1.2 Domain Name Protection

Domain name protection is a complex aspect of intellectual property law that involves the legal strategies and measures used to safeguard the exclusive rights and ownership of a

---

to be used in relation to goods for the purpose of indicating or so as to indicate a connection in the course of trade between the goods and some person having the right either as proprietor or as a registered user to use the mark, whether with or without any indication of identity of that person….'' see also Ferodo Ltd Vs Ibeto Ind. Ltd (1999) 2 NWLR (pt.592) 510 at 518 – 519

[4]Noah Webster, *Webster New World College Dictionary* (4th ed, Houghton Miffin Harcourt, 2010); Colin Mclntosh, *Cambridge Advanced Learner's Dictionary* (4th ed, Cambridge University Press, 2013).

[5]CL Branson 'Was $7.5 Million a Good Deal for Business. Com? The Difficulties of Obtaining Trademark Protection and Registration for Generic and Descriptive Domain Names' (2000) *Santa Clara Computer & High Tech. LJ.;17:285.*

[6]D Chan, 'Functional relations among constructs in the same content domain at different levels of analysis: A typology of composition models' (1998) *Journal of applied psychology* 83(2):234.

[7] P B Danzig, K Obraczka, and A Kumar, 'An analysis of wide-area name server traffic: A study of the internet domain name system' (1992) In Conference proceedings on Communications architectures & protocols (pp. 281-292).

particular internet domain name.[8]It deals with the specific laws and regulations that govern domain names, as well as the legal remedies and enforcement options available to protect against cybersquatting, trademark infringement, and other types of abuse.[9] The dire need for domain name protection was heightened in the late 20th century, as the internet became increasingly popular worldwide, Domain names were seen as the digital equivalent of trademarks.[10] This perception stemmed from the understanding that domain names served as unique identifiers for websites, similar to how trademarks distinguish products or services in the physical world.[11]

Domain name protection encompasses a range of issues, including resolving domain name disputes through alternative dispute resolution; securing trademark registration to provide a legal basis for protection against domain name infringement, and implementing technical solutions like domain name monitoring and defensive registrations to prevent abuse.[12]

2.1.3 Cybersquatting

This refers to the practice of registering a domain name that is identical or similar to a trademark or personal name with the intent to sell it at a profit or to confuse internet users.[13]Cyber squatters, often referred to as "cyber pirates," pre-emptively register domain names with the intent to profit by either selling them to the legitimate owners at inflated prices or by capitalizing on the confusion of customers who may mistakenly visit the website in search of the legitimate owners' products or services. Cyber squatters typically do not actively use the website, they registered, they are more interested in creating online chaos, birthing likelihood of confusion, hence making a trademark infringement case to be challenging,[14]by hijacking legitimate domain names, cyber squatters can divert traffic from the rightful owner's website to their own, potentially causing customers to become victims of fraud, identity theft, or other cybercrimes. This situation can damage a business's reputation and potentially expose the business to legal liability.[15]

Cybersquatting encompasses various forms, including typo squatting, identity theft, name jacking, and reverse cybersquatting. Typo squatting involves altering a domain's spelling by adding or omitting characters, as seen in examples like 'yajoo.com'.[16] Identity theft occurs when someone uses a company's identity to create a similar Uniform Resource Locator

[8]Chebude, Y. Shiferaw, A. Profe, and M. Dugasa, 'The Regulation of Domain Name Under Ethiopian. Trademark Law: Emerging Legal Issues' (Doctoral dissertation, Haramaya University 2022).

[9]M Leaffer, *Domain Names, Globilisation, and Internet Governance,* (Ind. J. Global Legal Stud., 1998) 139.

[10]K S Dueker, 'Trademark law lost in cyberspace: trademark protection for Internet addresses' (1996) Harv. JL &Tech..;9:48

[11] S L Dogan, M A Lemley, 'Trademarks and consumer search costs on the internet' (2004) Hous. L. Rev..;41:777.

[12]S Hao, A Kantchelian, B Miller, V Paxson, N Feamster, 'PREDATOR: proactive recognition and elimination of domain abuse at time-of-registration.' (2016), <https://dl.acm.org/doi/abs/10.1145/2976749.2978317> accessed on 15 April 2024.

[13]S Deo, and S Deo, 'Cybersquatting: Threat to domain name' (2021) *International Journal of Innovative Technology and Exploring Engineering*, 1432-4.

[14]Jennifer Golinveaux, 'What's in a domain name: Is cybersquatting trademark dilution?' (1998) *USFLRev*. 33, 641
<https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=cybersquatting+refers+to+the+practice+of+registering+a+domain+name+that+is+identical+or+similar+to+a+trademark+or+personal+name+with+the+intent+to+sell+it+at+a+profit+or+to+confuse+internet+users.++&btnG=#d=gs_qabs&t=1713180325255&u=%23p%3DfUOuuF4NU_AJ> accessed on 15 April, 2024.

[15] General Motors LLC v. Domains by Proxy, Inc / Mel Light (2012) D2012-1517.

[16]Sporty's Farm LLC v. Sportsman's Market, Inc. (2000) 202 F.3d 489; Shields v. Zuccarini, (2001) 254 F.3d 476.

(URL).[17] Name jacking occurs when names gain secondary significance in the marketplace, like those of celebrities such as Beyoncé or Taylor Swift. Proving bad faith in domain registration may be challenging if a person shares a name with a celebrity. Reverse cybersquatting involves falsely claiming ownership of a trademark to acquire a legitimate domain name.[18] This contrasts with traditional cybersquatting, where individuals purchase domain names containing trademarks with the intent of profiting from them. Cybersquatting is a crime against the property of an individual or a company/firm/trade in many countries, including Nigeria.[19] It stands as a significant concern globally.

2.2 Historical Context

The topic of safeguarding domain names and addressing cybersquatting is not novel. In fact, the history of these issues dates to the early days of the internet and has evolved significantly over the years. To understand the current legal framework in Nigeria, it is important to first examine the historical context that has shaped it.

For the purpose of this section, both the National Information Technology Development Agency (NITDA) and the Nigerian Internet Registration Association (NIRA) which are the regulatory bodies in Nigeria's information technology sector, are examined. NITDA was created in 2001 to regulate and oversee the development and implementation of information technology policies and practices in Nigeria, as mandated by the National Information Technology Development Act (2007).[20]

NIRA, on the other hand, was established in 2005, and it manages Nigeria's country code top-level domain (.ng). NIRA has been saddled with the responsibility of regulating the domain name system in Nigeria, and it is similar to how the Internet Corporation for Assigned Names and Numbers (ICANN) manages domain spaces globally.[21]The transfer of this responsibility was overseen by NITDA on behalf of the Nigerian government, with input from stakeholders in the internet community. NIRA was officially registered as an incorporated trustee in 2007.NIRA is a non-profit, non-government stakeholder-led association. NITDA signed a Memorandum of Association (on behalf of the Federal Government of Nigeria) with NIRA, which gives it oversight functions on NIRA's operations since NITDA has the mandate of implementing the nation's IT policy.[22] This relationship has witnessed a growing cordiality that will have a positive impact on both organizations.

NIRA operates on the 3-R model (Registry > Registrar > Registrant) for managing .ng domain names. This means NIRA does not directly handle registrations; they are conducted only through NIRA-accredited Registrars. These registrars, certified by NIRA, manage registrations, transfers, renewals, and modifications for .ng domain names. As of August

[17]Panavision Intern., LP v. Toeppen (1998) 141 F.3d 1316 <https://scholar.google.com/scholar_case?case=18039958431907373662&q=WIPO+arbitration+decisions+on+cybersquatting+-typo+squatting+&hl=en&as_sdt=2006#[1]> accessed on 16 April 2024.

[18]For instance, if someone registers FashionEmpire.com for their online fashion store, a competitor might start a business named ''Fashion Emporium" and then falsely claim ownership of the "Fashion Empire" trademark to take the domain name through legal means, by alleging cybersquatting.

[19]Cybercrimes (Prohibition, Prevention etc.,) Act, 2015, s. 25

[20]National Information Technology Development Agency Act, 2007, s. 1

[21]H. Klein 'ICANN and Internet governance: Leveraging technical coordination to realize global public policy' (2002) *The Information Society; 18(3):193-207.*

[22]Annual Report at the 4th Annual General Meeting of Nigeria Internet Registration Association Held on15th September 2011 at Lagos, available at <https://nira.org.ng/wp-content/uploads/2022/06/4TH-ANNUAL-REPORT.pdf> accessed on 8 May 2024.

2023, NIRA has 100 accredited registrars, who can appoint resellers for their operations.[23]The NIRA has its own set of rules and policies known as the NIRA Dispute Resolution Policy (NDRP). The NDRP is similar to the Uniform Dispute Resolution Policy (UDRP) and sets out the framework for the resolution of country code Top Level Domain (ccTLD) name disputes.

As the internet continued to grow in Nigeria, cybersquatting cases emerged, where individuals or entities registered domain names corresponding to trademarks or business names with the intent to profit or cause harm. Nigerian jurisprudence began to address cybersquatting through existing intellectual property laws, such as the Cybercrimes Act[24], which provided avenues for trademark owners to pursue legal action against cyber squatters. However, the Nigerian courts have not established legal precedents in cases involving cybersquatting, and this may hinder the development of the jurisprudence surrounding domain name protection and intellectual property rights. At the stage of writing this paper, there were no reported Nigerian court cases dealing with infringements by domain name registrants. This does not mean that there have been no conflicts. Domain name disputes have, thus far, been settled out of court. The writer anticipates that the Nigerian courts will address the issue soon. In the meantime, one can rely on the rulings and decisions made by English courts and other jurisdictions regarding cybersquatting.

3.0 Legal Framework

3.1. Examination of Existing Laws and Regulatory Bodies on Domain Name Protection and Cybersquatting in Nigeria

3.1.1 Constitution of The Federal Republic of Nigeria, 1999 (As Amended)

While the Nigerian Constitution does not expressly mention domain names or cybersquatting, several of its provisions lay a strong foundation for the protection of digital identities, intellectual property, and online economic activities. These sections support a broader interpretation of constitutional rights in the context of internet and cyberspace regulation.

To begin with, Section 1(3) establishes the supremacy of the Constitution over all other laws in Nigeria. It states that if any other law is inconsistent with the provisions of the Constitution, the Constitution shall prevail, and the other law shall be void to the extent of its inconsistency. This provides a legal backbone for challenging any regulatory or legislative gaps in domain name protection and reinforces the applicability of constitutional rights in the digital sphere. In addition, Section 16(1)(d) of the Constitution guarantees the right of every citizen to participate in economic activities outside the major sectors of the economy. In today's digital economy, domain names serve as critical economic tools, functioning as online presence, marketing platforms, and brand identifiers. Cybersquatting undermines this right by restricting individuals and businesses from accessing or controlling their digital assets, thereby impeding their participation in legitimate economic activities.

Closely related is Section 43, which provides every Nigerian with the right to acquire and own property. While traditionally interpreted to mean physical and immovable property, this provision can be extended to include intangible assets like domain names and trademarks in the digital space. Unauthorized appropriation of domain names by cyber squatters, especially

[23]History of Nira– NIRA (.ng) Website, <https://nira.org.ng/history-of-nira/> accessed on 8 May 2024

[24]J. Onele, Onyilofor E., 'Domain names and cybersquatting: implications for trademarks in Nigeria' (2018). *2018 Dec 19;9(4):115-33.*

those mimicking registered brands or personal identities, amounts to an infringement on this constitutional right to property ownership. Furthermore, Section 37 guarantees the privacy of citizens, protecting their homes, correspondence, and electronic communications. In the context of cybersquatting, the unauthorized use of a domain name to impersonate a brand or individual can lead to deceptive practices, potentially compromising users' privacy by tricking them into divulging personal information under false pretences.

Equally relevant is Section 39, which enshrines the right to freedom of expression and the right to receive and impart information without interference. Domain names are often the medium through which individuals and organizations communicate, express ideas, and disseminate information online. When cyber squatters unlawfully register and exploit domain names belonging to legitimate entities, they effectively interfere with the victim's right to freely operate a platform for expression and outreach, thereby infringing on this fundamental freedom. Lastly, Section 18(2) obliges the government to promote science and technology. This directive implies that the state has a responsibility to foster the development and protection of digital infrastructure, including domain name systems. Ensuring that individuals and businesses can securely register, use, and defend their domain names against malicious activities like cybersquatting is an essential part of promoting technological advancement and trust in the digital economy.

Ultimately, although not explicitly drafted for cyberspace, the Nigerian Constitution contains several provisions that, when interpreted within the evolving digital context, support a strong legal foundation for domain name protection. These constitutional guarantees, including economic rights, property ownership, privacy, freedom of expression, and technological development, underscore the need for a cohesive legal and institutional response to cybersquatting in Nigeria.

3.1.2 Cybercrimes (Prohibition, Prevention, Etc) Act, 2015

The Cybercrimes Act of 2015 marks Nigeria's inaugural legislation dedicated to addressing cyber security concerns. It was enacted in May 2015; it aligns with the 2011 ECOWAS Directive aimed at combating cybercrimes[25] and it provides a wide scope of cyber offences.
The Act defined Cybersquatting as[26]:

> *The acquisition of a domain name over the internet 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 Acquired without right or with intellectual property interests in it.*

Section 25 of the Cybercrime Act aims to stop cybersquatting and protect the intellectual property rights of legitimate domain name owners. It criminalizes the intentional use of "name, business name, trademark, domain name, or other word or phrase registered, owned, or in use by any individual, body corporate or belonging to either the Federal, State or Local Governments in Nigeria, on the internet or any computer network" without authorization and

[25]<https://www.mfwa.org/ecowas-court-orders-nigeria-to-align-its-cybercrime-law-with-its-international-obligations/> accessed on 8 May 2024
[26]Cybercrimes (Prohibition, Prevention etc.) Act, 2015, s. 58

with the intent to interfere with the rightful owner's use. Offenders face imprisonment for up to two years, a fine of up to N5,000,000.00, or both upon conviction.

A perusal of Section 25 reveals that:

i) There must first be a name, business name, mark, trademark, domain name, or other registered word or phrase that must be owned and be in use by an owner.
ii) An offender's act must interfere with the owner's name, business name, mark, trademark, or domain name.
iii) This interference must have occurred over any computer network, including but not limited to the internet.
iv) This act must also have been unauthorized.

Scholars have noted that although Section 25 is labelled 'cybersquatting,' it covers not only cybersquatting but also other offences such as username squatting and brand jacking.[27] This stems from the use of words such as "a name, business name, trademark, domain name, or other word or phrase registered, owned or in use…".

Additionally, it can be argued that registration or trademarking of the complainant's name is not necessary. It suffices if the name is owned by the complainant, meaning it is how they are known and/or actively used at the relevant time. However, this argument may not be sustainable in a case concerning trademark infringement because the courts lack jurisdiction to determine an infringement of trademark action when the trademark in question is not registered.[28] More so, the argument may be countered given the definition of cybersquatting under Section 58 which provides that it should be "...an existing trademark registered with the appropriate government agency at the time of the domain name registration...". Therefore, it appears that an unregistered trademark may not receive equivalent protection to a registered one when the rightful owner is deprived of it. Given that domain names do not inherently include trademarks, a victim of cybersquatting might assert that the domain name has become associated with their business through long-term and active use.[29]

3.1.3 Criminal Code Act

Section 419 of the Act provides that:

> *Any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony and is liable to imprisonment for three years. If the thing is of the value of one thousand naira or upwards, he is liable to imprisonment for seven years. It is immaterial that the thing is obtained, or its delivery is induced through the medium of a contract induced by the false pretence.*

What can be gleaned from the above is that cyber squatters can potentially be penalized under laws related to obtaining goods by false pretences, depending on the circumstances of the case and the specific laws in the jurisdiction. If a cyber squatter engages in fraudulent behaviour, such as misrepresenting themselves as the rightful owner of a domain name to

[27]BusaInem, 'Nigerian Law on Cybersquatting' (2016) <https://www.academia.edu/resource/work/42164084> accessed on 8 May 2024

[28] MT Elebute and anor v. Dr. Olugbenga Ogunkua (1990) F.H.C.L 201; Trade Marks Act, s.3.

[29]J DLipton 'Celebrity in Cyberspace: A Personality Rights Paradigm for Personal Domain Name Disputes'(2008) *Wash. & Lee L. Rev.*.;65:1445.

obtain goods or services, they may be subject to legal consequences under the Criminal Code Act related to fraud, false pretences, or deceptive trade practices.

3.2 Reviewing Cybersquatting Through the Lens of Civil Wrong

Common law principles, including trademark laws and the concept of passing off, frequently serve as the foundation for resolving domain name disputes.[30]

3.2.1 Trademark Act

Section 67(1) of the Act defines a trademark as a mark used or proposed to be used in relation to goods for the purpose of indicating, or so as to indicate, a connection in the course of trade between the goods and some person having the right, either as proprietor or as registered user, to use the mark, whether with or without any indication of the identity of that person.[31]
Section 5(2) of the Trademarks Act makes provision for what constitutes an infringement of a trademark. In describing an infringement, it states:

> *"…that right shall be deemed to be infringed by any person who, not being the proprietor of the trade mark or a registered user thereof …, uses a mark identical with it or so nearly resembling it as to be likely to deceive or cause confusion, in the course of trade, in relation to any goods in respect of which it is registered, and in such manner as to render the use of the mark likely to be taken either –*
> *a) As being use as a trademark; or*
> b) *In a case in which the use is use upon the goods or in physical relation thereto or in an advertising circular or other advertisement issued to the public, as importing a reference to some person having the right either as proprietor or as registered user to use the trademark or to goods with which such a person as aforesaid is connected in the course of trade*."

Therefore, where a domain name is used in relation to any good or service which is identical or confusingly similar to an existing trademark, such use of a domain name can be said to be an infringement of the registered trademark. This has been observed in a plethora of cases, some of which are examined here:

- *Sporty's Farm LLC v. Sportsman's Market, Inc.*[32]*:*In a legal case involving Sportsman's, a well-known mail-order catalogue company, and Omega, a scientific instrument catalogue company, Sportsman's trademark "sporty's" was registered as the domain name "sportys.com" by Omega. Sportsman's sued for trademark infringement, dilution, and unfair competition. The Court found in favour of Sportsman's on the dilution claim but rejected the infringement claim due to the unrelated nature of the businesses.[33] The Court issued an injunction requiring Omega to relinquish the domain name.
- ***Panavision Intern., LP v. Toeppen***[34]*:* Panavision, known for its motion picture camera equipment, holds trademarks for "Panavision" and "Panaflex." When

[30] Bhutia, T. C. 'Domain Name Disputes and Unfair Trade Practices: An Analytical Legal Study' (2018) *Doctoral dissertation.*
[31] Trademarks Act cap T13 Laws of the Federation of Nigeria, 2004 s.67(1)
[32]Sporty's Farm LLC v. Sportsman's Market, Inc., 202 F.3d 489 (2d Cir. 2000).
[33] Trademark dilution involves the unauthorized use of a famous trademark in a manner that weakens the distinctiveness or reputation of the mark, even if there is no likelihood of confusion among consumers about the source of goods or services. In contrast, trademark infringement occurs when someone uses a trademark in a way that is likely to cause such confusion. While infringement focuses on consumer confusion, dilution centres on harm to the value or distinctiveness of the mark itself.
[34]Panavision Intern., LP v. Toeppen, 141 F.3d 1316 (9th Cir. 1998).

Panavision tried to register "Panavision.com" as a website domain in 1995, Dennis Toeppen had already registered it and offered to sell it to Panavision for $13,000. After Panavision refused, Toeppen registered "Panaflex.com" as well. He has done this with other companies' trademarks too. Panavision sued Toeppen for diluting its trademark, alleging he registered them as domain names and attempted to sell them back. The Court found personal jurisdiction over Toeppen and ruled in favour of Panavision on both federal and state dilution claims.

- ***Union des Associations Europeennes de Football (UEFA) V. Funzi Furniture***[35]*:*the defendant registered a domain name,www.championsleague.com. The claimants who were the organizers of the world famous "UEFA Champions League," a football championship, instituted an action against the defendants who had requested that $1,450,000 be paid to for the site. The Court held that there was a trademark infringement by the defendant.
- ***Konga Online Shopping Limited v. Rocket Internet GmbH, ArntJeschke***[36]*:* The complainant, Konga Online Shopping Limited, based in Nigeria, filed a complaint against Rocket Internet GmbH of Germany concerning the domain name <konga.sc>. The domain was registered with INTERNETX GMBH. The complainant, a company operating an online retail business through the website www.konga.com, applied for trademarks for "KONGA LOGO" and "KONGA" with the Nigerian Trademarks Registry. These applications have not yet been granted. The complaint, filed on May 30, 2014, alleged that the respondent had no legitimate interests in the domain, which was registered and used in bad faith. The respondent contested the complaint, arguing that the complainant lacked trademark rights and failed to demonstrate bad faith. The panellist found that the complainant's trademark applications were insufficient to establish rights, and thus, the complaint was denied.

From the case involving Konga, it is established that in trademark infringement cases related to cybersquatting, the success of a claim often hinges on whether the mark is registered. The landmark case of *Sanofi S.A. v Sanofi Integrated Services Ltd and ors*[37]reiterates the fact that trademarks are central to a company's identity. In most cases of trademark infringement, the courts firmly sided with the rights of trademark holders.[38] They held that a registered trademark grants its owner exclusive rights, and any unsanctioned use is, without doubt, an infringement.

3.2.2 Cybersquatting and Passing Off

Passing off occurs when a defendant, in the course of their trade or business, makes a misrepresentation to potential customers that is intended to harm another's business or goodwill, resulting in actual or potential damage. Cyber squatters can also engage in passing off by falsely presenting their goods or services as those of another[39], often through practices like "typo squatting," where they use a name similar to that of the plaintiff to deceive the public. The legal principles governing passing off can be applied to protect individuals who

[35] Case No: D2000-0710 This can further be seen in www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0710.html accessed on 1st May 2024.

[36] Case No: DSC2014-0001 www.wipo.int/amc/en/domains/decisions/text/2014/dsc2014-0001.html accessed on 1st May 2024.

[37]Suit No: FHC/ABJ/CS/188/2020 Coram J.K. Omotosho J.

[38] Alliance Intl Ltd v. SaamKolo Intl Enterprises Ltd (2022) LPELR-57984(SC); Morison Industries Plc v. CPL Industries Ltd (2021) LPELR-52981(CA)

[39]S Deo, S Deo, 'Cybersquatting: Threat to domain name' (2019) *International Journal of Innovative Technology and Exploring Engineering*; 8(6):1432-

fall victim to cybersquatting, provided the circumstances meet the criteria for passing off. Moreover, unlike in cases involving trademark infringement, a proprietor of an unregistered trademark can sue a third party for passing off his mark.

3.3 Who Oversees Domain Name Protection in Nigeria?

3.3.1 Nigeria Internet Registration Association (NIRA)

Despite domain names being registered on a first-come, first-served basis[40],NIRA has established policies that impose limitations on the registration of certain domain names. According to NIRA's general rules, they reserve the right to verify the applicant's compliance with their policies, and they will only approve applications that adhere to these policies. Additionally, registrants must agree to a contract with NIRA stipulating that the latter reserves the right to cancel or suspend the registration of a domain name if the registrant violates any of the rules.[41]

Further, NIRA retains the authority to maintain a list of domain names that cannot be registered or, if already registered, will be revoked. This list includes:[42]

- **Offensive names**: This list shall contain words as determined by NIRA Executive Board of Directors to be offensive first to the Nigerian community and then to the global community. All requests for domains under this list would be rejected.
- **Restricted names**: This entails domains that, if used, could potentially create misleading impressions, particularly those containing terms associated with the military, government, or similar entities. Applications for these domains will likely face rejection.
- **GeoNames**: This covers domains consisting of geographical location and places, these as determined by the NiRA Executive Board of Directors.
- **Premium Names**: This deals with domains featuring generic words of high value. These premium domains are made available through competitive bidding and auction processes.
- **Existing Nigerian trademarks**: These domains are prohibited unless the registrant obtains consent from the trademark owner.

Regarding the last restriction, it can be argued that it falls short in addressing all potential issues. The issue arises because not all contested domain names align with registered trademarks. For instance, personal names may or may not be trademarked, depending on various factors. However, in the case of *Fiona Roberts v Russell Boyd*[43], wherein the renowned Oscar-winning actress Julia Roberts sought legal action to gain control of the domain name <juliaroberts.com>, it was determined that Julia Roberts possessed unregistered trademark rights in her personal name. This case bears resemblance to the situations seen in *Linda Ikeji v. Emmanuel Efremov* and *Linda Ikeji v. Jonathan Santos,* where both defendants sought to leverage the reputation associated with the name "Linda Ikeji" by incorporating it into their domain names. As there is no recorded judicial decision on these cases, it is presumed that they were resolved through out-of-court settlements. Furthermore, uncertainty lingers regarding whether "Linda Ikeji" is a trademarked name. If indeed it holds trademark status, it raises questions about the adequacy of NIRA's *Julia* measures to restrict the registration of such names.

[40]'NIRA Domain naje policy' (2021) <https://nira.org.ng/pdf/NIRA-Domain-Names-Policy.pdf> accessed on 8 May 2024
[41]*Ibid*
[42]*Ibid*
[43] Roberts v Boyd (2000) WIPO Case No D2000-0210.

Furthermore, NIRA offers a Dispute Resolution Policy (NDRP) to resolve domain name disputes under the .ng domain.[44] The NDRP outlines the procedures for filing complaints, responding to complaints, and resolving disputes in a timely and cost-effective manner. It can also help parties find equitable solutions and avoid protracted legal battles. Under the NDRP policy, most trademark-based domain-name disputes must be settled through agreement, court action, or arbitration before a registrar will take action on a domain name. The NDRP serves as a resolution mechanism for parties not bound by a NIRA Agreement, allowing complainants the choice to either use this process or seek other legal remedies, such as litigation. Initiating a case under the NDRP does not preclude parties from later pursuing court proceedings. Decisions made by the expert panel can be appealed to a three-member panel and may be further challenged in regular court.

3.3.2 The National Information Technology Development Agency (NITDA)

NITDA is a regulatory body established under the NITDA Act to oversee the planning, research, development, evaluation, and regulation of information technology practices in Nigeria. While NIRA handles the registration and administration of domain names, NITDA plays a supervisory role.[45] NIRA does not directly handle domain name registrations; instead, it operates through accredited registrars. When an application is submitted, an authorization letter is sent to the Chief Operating Officer of NIRA. The authorization letter is typically sent to NITDA for verification and approval.

Upon successful verification and approval, NITDA sends confirmation to the registrar via NIRA, allowing the registrar to create the domain while NIRA activates it.

3.3.3 Corporate Affairs Commission

The extent to which the Corporate Affairs Commission (CAC) actively promotes domain name protection may be subject to debate. However, from an impartial standpoint, it can be argued that CAC indirectly influences domain name regulation through its regulations governing the registration of distinct business names by business owners.[46] The reason is not farfetched because business owners often prefer to register their business names as domain names. By ensuring that businesses do not share similar names, CAC indirectly impacts domain name regulation by reducing the likelihood of conflicts arising from similar names being used for both business registration and domain registration.

3.3.4 The Economic and Financial Crimes Commission (EFCC)

The EFCC Act establishes the Economic and Financial Crimes Commission, tasked with enforcing all laws related to economic and financial crimes, among its various responsibilities. By virtue of Section 46 of the Act, economic and financial crimes include, but are not limited to, the theft of intellectual property and piracy. This means that the EFCC contributes to the protection of domain names in Nigeria, safeguarding them from misuse that aligns with financial crimes such as fraud, money laundering, and other forms of corruption that could involve or affect the digital economy and digital assets.

While there may not be specific cases where the EFCC has directly regulated domain names, it is possible that they have been involved in investigations or prosecutions related to

[44]<https://nira.org.ng/pdf/NIRA_DISPUTE_RESOLUTION_POLICY.pdf> accessed on 8 May 2024
[45]NITDA, Act 2007, second schedule, section 6(M).
[46]Companies and Allied Matters Act, 2020, s. 852.

cybercrimes that involve domain names. These could include cases of phishing scams, fraudulent websites, or online piracy, where domain names play a significant role.

4.0. The Challenges and Deficit

4.1. Navigating Challenges in Domain Name Regulation: Insights into NIRA's Operational Hurdles

As the steward of Nigeria's online presence, the Nigerian Internet Registration Association (NIRA) faces a lot of challenges in its mission to regulate and maintain the integrity of the .ng domain space. This section will explore some of the obstacles encountered by NIRA in fulfilling its mandate effectively.

1. **Jurisdictional Limitations**: NIRA's authority is restricted to matters concerning .ng domain names. Other domain extensions, like .com and .org are not overseen by NIRA and are not specifically designated to Nigeria by the Internet Assigned Numbers Authority (IANA).[47]This means they cannot handle complaints about domains outside of the .ng space, or breaches of Nigerian trademark laws, unless they relate directly to .ng domains. Excluding generic domain names from NIRA's jurisdiction poses several challenges to domain name protection. Malicious actors could potentially exploit this gap by registering generic domains to engage in fraudulent activities, knowing that NIRA's jurisdiction doesn't cover them. Additionally, many online activities involve interactions across different domain spaces. This means that NIRA may struggle to address issues that involve both .ng and generic domains. For example, if a scam involves a website with both a .ng and a .com domain, NIRA may only be able to address the .ng aspect, leaving the rest unresolved. Further, users may not fully understand the jurisdictional boundaries between .ng and generic domains. This could lead to confusion regarding where to report domain related problems.
2. **Lack of express statutory authority**: Despite its important role in the management of the .ng domain space in Nigeria, NIRA operates without express statutory authority or legal backing. While some argue that Section 6(m) of the NITDA Act combined with its second schedule provides NIRA with authority, this interpretation may not be solid. Section 6(m) merely provides one of the functions of NITDA. The second schedule, primarily establishes NITDA's regulatory oversight over organizations managing Nigeria's country code top-level domain, rather than directly granting statutory authority to NIRA.
3. **Lack of Legislative Powers**: The challenge associated with NIRA not having express statutory authority may be connected to its inability to wield direct legal power. NIRA does not possess the authority to impose fines or penalties on registrars or registrants. This means they cannot directly punish those who violate domain policies but can only request corrective actions or terminate accreditations in extreme cases. Thus, while NIRA can establish policies and procedures for domain name management within its jurisdiction, it may face difficulties in compelling compliance or imposing consequences on registrars or registrants who violate these policies. As a result, NIRA's effectiveness in regulating the .ng domain space may be limited, as it relies more on cooperation and voluntary compliance than enforceable legal measures. While many agencies may lack legislative powers, an organisation tasked with overseeing domain names, like NIRA, holds a unique position. Given its crucial

[47]IANA- Report on the Redelegation of the .NG Top-level Domain <https://www.iana.org/reports/2009/ng-report-07apr2009.html> accessed on 8 May 2024.

role in domain name protection and combating cybersquatting, it is imperative that NIRA possess the authority to administer punishments for offenders.

4. **Challenges in Dispute Resolution Effectiveness:** The initial phase of the NDRP mandates that an expert handle the resolution or informal mediation, but it's unclear who qualifies as the expert—is it an IT expert, a legal practitioner, or someone from NITDA? None of these professionals might possess the full range of necessary qualifications since the process ideally requires knowledge from both IT and legal perspectives. Additionally, the remedies available under the NDRP may be insufficient. There is also the issue that the parties involved might disregard the NDRP proceedings, as nothing prevents them from initiating litigation or other legal actions simultaneously. For instance, a party penalized by NIRA could challenge the legality of the sanction or even accuse NIRA of contributory infringement, leading to further legal complications**.**
5. **Subjectivity in Complaint Evaluation**: NIRA's discretion in investigating complaints based on subjective criteria like frivolity or bad faith poses a challenge to domain name protection. Differentiating between legitimate complaints and those deemed frivolous or brought in bad faith may be open to interpretation, leading to potential inconsistencies in complaint handling. This may also lead to dismissing valid complaints and allowing abusive practices to continue unchecked. Ensuring fair evaluation of complaints while preventing abuse of the complaint process presents a challenge to maintaining effective domain name protection.

4.2. Identifying Deficiencies in Current Legal Provisions

Some current legal provisions, although well-intentioned, have weaknesses that hinder their effectiveness in protecting domain names. This section will examine some of the challenges. As mentioned earlier, protecting a trademark under the Trademarks Act can also safeguard a brand's domain name from cyber squatting. However, a closer examination of the provisions of sections 67 and 5 of the Trademark Act reveals some significant limitations to this protection, which must be carefully considered. One potential challenge in the provisions is the requirement for a trademark to be used or proposed to be used in relation to goods. Traditionally, trademarks have been associated with physical goods or products. However, in the digital age, trademarks are also used to identify and distinguish services, including those provided online. This means that while the Trademarks Act may cover trademarks used in relation to physical goods, it may not fully address the protection of trademarks used in the context of domain names and online services.

Additionally, the requirement that infringement occurs "in the course of trade" may pose challenges in the context of cybersquatting. Cyber squatters often engage in their malicious acts outside of traditional commercial transactions, making it difficult to establish infringement under the provisions outlined in the Trademarks Act.[48]

Furthermore, the language used in the Act, such as "identical with" or "so nearly resembling it as to be likely to deceive or cause confusion," may not fully capture the details of domain name disputes. In the context of domain names, slight variations or misspellings of

[48] For instance, a cybersquatter may register a domain name solely to sell it to the rightful trademark owner at an inflated price, or to disrupt the owner's online presence. In such cases, it may be hard to prove that the infringement occurred "in the course of trade."

trademarks are often used to deceive or cause confusion among internet users.[49] However, the Act's language may not be sufficient to address these subtle variations, potentially leaving trademark owners without adequate protection.

Similarly, the definition of cybersquatting under the Cybercrimes Act poses challenges to effective domain name protection. For instance, the Act's requirement that the domain name be acquired "in bad faith" introduces a subjective element, making it potentially difficult to prove, especially in cases where the cyber squatter's intentions are unclear or obscure. Moreover, the Act's requirement for registration with a government agency may create vulnerabilities for trademark holders whose marks are not registered or whose registration processes are delayed, leaving them exposed to cybersquatting.

Furthermore, there can be challenges to personal name protection. While the Act addresses domain names that are "identical or similar to the names of persons other than the registrant," protecting personal names can be challenging, especially if the names are common or if there are multiple individuals with the same name.

Additionally, the requirement of existing intellectual property interests introduces complexities in establishing ownership or rights to a domain name. This requirement may complicate legal proceedings and enforcement actions related to cybersquatting. Another challenge with the Cybercrimes Act is that it does not designate a specific agency or entity responsible for enforcing its provisions, leaving a gap in accountability, and potentially hindering the effective implementation of the Act's measures against cybersquatting. Having examined the limitations of domestic laws in addressing cybersquatting, we now turn to an international perspective, exploring how other countries and global frameworks approach domain name protection and cybersquatting issues.

5.0 International Perspective.

5.1 United States

Domain name protection and cybersquatting are significant concerns in the United States, where the internet and e-commerce play a vital role in the economy. The US legal framework for domain name protection and cybersquatting includes:

1. Lanham Act (Trademark Act)
2. Anti-Cybersquatting Consumer Protection Act (ACPA)
3. Uniform Domain-Name Dispute-Resolution Policy (UDRP)

5.1.1 Lanham Act

The Lanham Act, also known as the Trademark Act, established in 1946, serves as the main federal law governing trademarks in the United States. It forbids various actions such as trademark infringement, dilution, and false advertising. Before the Lanham Act, trademarks depended on state common law for protection, resulting in confusion and insufficient safeguarding. The Act addressed these issues by providing comprehensive regulation of trademark creation and use, ensuring protection for both owners and consumers. Since its inception, the Act has undergone multiple amendments. Its influence was notably strengthened by the Trademark Counterfeiting Act of 1984. This Act criminalized intentional or unauthorized use of counterfeit trademarks.

[49]For instance, a domain name that is one letter off from a trademarked name may still cause confusion among consumers but may not meet the Act's threshold of being "identical with" or "so nearly resembling" the trademark.

It is true that cyber squatters don't always engage in their malicious acts to misrepresent their products as those of the real owners of the trademark, they also do so to achieve trade dilution. There are two types of trade dilution:

1. **Dilution by blurring**: When a similar mark is used on unrelated products, it reduces the distinctive quality of the original mark.
2. **Dilution by tarnishment**: When a similar mark is used on inferior or unwholesome products, it tarnishes the reputation of the original mark.

This can lead to a loss of brand value, reputation, and customer loyalty. Section 43(c) of the Lanham Act, generally outlines the broader law against the dilution of famous trademarks, providing protection against both blurring and tarnishment that might occur without regard to competition or likelihood of confusion. This was observed in *Sporty's Farm LLC v Sportsman's Market, Inc.* However, Section 43(c)(4) of the Act provides that the non-commercial use of a trademark does not constitute trademark dilution. This was observed in *Bosley Medical Institute, Inc. v Kremer*.[50] Michael Kremer, a dissatisfied patient of Bosley Medical Institute, Inc., created a website under the domain name www.BosleyMedical.com to criticize the company, using their registered trademark "Bosley Medical." Bosley sued Kremer for trademark infringement and related claims. The District Court ruled in favour of Kremer, finding that his use of the trademark in a non-commercial, critical context did not constitute infringement under the Lanham Act. However, the Court did not resolve a cybersquatting claim due to incomplete discovery and incorrectly granted summary judgment on this point.[51]

In *Avery Dennison Corp. v Sumpton*[52], the Court found that despite the early registration and continuous use of the marks "Avery" and "Dennison," the plaintiff had not provided sufficient evidence to demonstrate that the marks were famous and distinctive enough to support a claim for trademark dilution in relation to cybersquatting. This highlights the strict requirements for proving trademark dilution under both the ACPA and other U.S. laws. It also suggests that the outcome might have been different if the case had involved trademark infringement, as the legal standards and evidence required for each type of claim can vary.

Section 67(1) of the Nigerian Trademark Act[53] defines a trademark as a mark used or proposed to be used in relation to goods to indicate a connection between the goods and the rightful owner in the course of trade. While the phrase "in the course of trade" typically implies commercial activity, the law does not explicitly require commercial use of the trademark for it to be considered infringement. In other words, unlike Section 43(c), which requires commercial use to constitute trademark dilution, Section 67 has a broader scope and may consider non-commercial use as trademark infringement if it meets the definition of a trademark and is used in relation to goods in the course of trade.

The section under the Lanham Act that directly deals with domain name protection is Section 43(d). It addresses cybersquatting. It prohibits registering, trafficking in, or using a domain name with bad-faith intent to profit from the trademark of another. Specifically, it provides

[50]Bosley Medical Institute, Inc. V. Kremer, 403 F.3d 672 (9th Cir. 2005) <https://scholar.google.com/scholar_case?case=6777991169490441191&q=Bosley+Medical+Institute,+Inc.+V.+Kremer.&hl=en&as_sdt=2006>

[51]*Ibid*

[52]Avery Dennison Corp. V. Sumpton, 189 F.3d 868 (9th Cir. 1999)

[53] Cap T13 Laws of Federation of Nigeria 2004

remedies for trademark owners whose marks are being used in bad faith within domain names. Moreover, Section 45 of the Act defines a domain name "as any alphanumeric designation which is registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority as part of an electronic address on the Internet." These provisions of the Lanham Act offer comprehensive protection for trademark owners against misuse of their marks in domain names. Its application has been demonstrated in various instances of cybersquatting.[54]

5.1.2 Anti-cybersquatting Consumer Protection Act (ACPA)

The Anti-cybersquatting Consumer Protection Act (ACPA) is a United States law that was enacted in 1999.It is an amendment to the Lanham Act, specifically designed to address the issue of cybersquatting. It provides a framework under U.S. law for registering trademarks and addressing trademark disputes, including those that involve domain names used in bad faith.

The ACPA defines cybersquatting as:
"The registration, trafficking in, or use of a domain name that is identical to, confusingly similar to, or dilutive of a trademark or service mark of another that is distinctive at the time of registration of the domain name, without regard to the goods or services of the parties, with the bad-faith intent to profit from the goodwill of another's mark (commonly referred to as ''cyber piracy'' and ''cybersquatting'') —

1. results in consumer fraud and public confusion as to the true source or sponsorship of goods and services;
2. impairs electronic commerce, which is important to interstate commerce and the United States economy;
3. deprives legitimate trademark owners of substantial revenues and consumer goodwill; and
4. places unreasonable, intolerable, and overwhelming burdens on trademark owners in protecting their valuable trademarks."

The Act holds individuals liable for registering, using, or profiting from a domain name that is identical or similar to a distinctive trademark; dilutes a famous trademark; a protected trademark, word, or name (including certain organizations' names). This liability applies to the domain name registrant or their authorized licensee, if they act with bad faith intent to profit from the trademark.[55]A trademark is famous if the owner can prove that the mark "is widely recognized by the general consuming public of the United States as a designation of the source of the goods or services of the mark's owner."[56] To determine bad faith intent, courts consider various factors, including the registrant's trademark rights, prior use of the domain name, intent to divert customers, and offering to sell the domain name for financial gain.[57] However, the court cannot make a finding of bad faith if the defendant had reasonable grounds to believe that their use of the domain name was fair or lawful.[58]

---

[54]T. Belcyzk, 'Domain Names: The Special Case of Personal Names' (2002) BUL *Rev..;82:485.*

[55]The ACPA provides a list of nine non-exclusive factors that a court may consider in determining whether a bad faith intent to profit is established– 15 U.S.C. § 1125(d)(1)(B)(i); also see, DaimlerChrysler v. The Net Inc., (2004) 388 F. 3d 201.

[56]P. Marquez 'Trademark: A Comparative Look at China and the United States'(2010) *Touro Int'l L. Rev..;14:334*.

[57]Enrico Schaefer, 'What is 'Bad faith' Intent to Profit Under the Anti cybersquatting Consumer Protection Act?' (2014) <https://www.traverselegal.com/blog/what-is-bad-faith-intent-to-profit-under-the-anticybersquatting-consumer-protection-act/> accessed on 8 May 2024.

[58]Harrods Ltd. V. Sixty Internet Domain Names, 302 F.3d 214 (4th Cir. 2002).

Unlike the Nigerian trademark laws, a trademark need not be registered to be entitled to protection under the ACPA.[59]Section 43(a) of the Lanham Act "protects qualifying unregistered trademarks, and the general principles qualifying a mark for registration under Section 2 of the Lanham Act are for the most part applicable in determining whether an unregistered mark is entitled to protection under Section 43(a)."[60]

Section 1125(d)(1)(C) of the Lanham Act, which is part of the ACPA, provides a cause of action for trademark owners who believe their mark is being infringed upon or diluted by a domain name that is confusingly similar to their trademark. If the court finds in favour of the trademark owner, it may order injunctive relief, including the forfeiture or cancellation of the domain name or its transfer to the trademark owner. This was observed in *DaimlerChrysler v The Net Inc*. (supra). On the issue of whether the short duration of infringement can be considered to mitigate damages, in *Shields v Zuccarini*[61], the Court found no requirement in the ACPA to consider the duration of infringement when awarding damages.

The ACPA has been instrumental in addressing cybersquatting and establishing clear guidelines for trademark owners to protect their rights.

5.1.3 Uniform Domain-Name Dispute-Resolution Policy (UDRP)

The World Intellectual Property Organization (WIPO) has played a significant role in domain name protection through its administration of the Uniform Domain Name Dispute Resolution Policy (UDRP). The UDRP is a mechanism established by the Internet Corporation for Assigned Names and Numbers (ICANN) to resolve disputes related to domain names.[62]It provides a cost-effective way for trademark owners to resolve related disputes, and it offers an alternative to traditional litigation, which can be time consuming and costly.[63] It might seem contradictory to say that UDRP provides a cost-effective way to resolve disputes while also acknowledging that it can be costly.

However, the cost-effectiveness of UDRP is relative to traditional litigation. UDRP proceedings are typically faster and less expensive than going to court. Traditional litigation can involve much higher legal fees, court costs, and expert witness fees, which can add up quickly. Additionally, UDRP proceedings are often resolved within a few months, whereas litigation can take years. So, while UDRP can still be costly, it is generally a more efficient and cost-effective option compared to traditional litigation.

Any individual or organisation worldwide can submit a domain name complaint through the UDRP Administrative Procedure. Similarly, for disputes involving country-code top-level domain names (ccTLDs), the UDRP process can be utilized if the relevant ccTLD registry has voluntarily adopted the UDRP policy.[64]The UDRP policy sets out the rules and procedures for resolving disputes related to domain names, including the criteria for

[59]Wal-Mart Stores, Inc. V. Samara Bros., (2000) 529 U.S. 205, 209, 120 S.Ct. 1339; Two Pesos, Inc. V. Taco Cabana, Inc., (1992) 505 U.S. 763, 768, 112 S.Ct. 2753.
[60]A. J. Canfield Co. V. Honickman (1986) 808 F. 2d 291.
[61] Shields v. Zuccarini, 254 F.3d 476 (3d Cir. 2001).
[62]A. Christie, 'The ICANN Domain-Name Dispute Resolution System as a model for resolving other intellectual property disputes on the internet', (2002) J. World Intell. Prop.; 5:105.
[63]E. G. Thornburg, 'Fast, cheap, and out of control: Lessons from the ICANN dispute resolution process', (2002) *J. Small & Emerging Bus. L. 6:191.*
[64]HP. Singh, 'Domain Name Disputes and Their Resolution under UDRP Route: A Review.', (2018) *Archives of Business Research. Dec 25;6(12):147-56.*

determining whether a domain name registration constitutes abusive or unlawful behaviour, the process for filing complaints and responses, the appointment of impartial panellists to adjudicate disputes, and the available remedies, such as the transfer or cancellation of the disputed domain name.

The case of *Sallen v Corinthians Licenciamentos*[65]raises important issues about the relationship between the ACPA and the WIPO's dispute resolution procedures under the UDRP. In this case, Jay D. Sallen lost a WIPO dispute over his use of the domain name corinthians.com and subsequently filed a complaint in a U.S. federal court against Corinthians Licenciamentos LTDA (CL). Sallen sought a declaration that his registration and use of the domain name did not violate the ACPA, relying on specific sections of the Act that allow a domain name registrant to challenge an adverse decision under the UDRP. He argued that federal courts have the authority to override the WIPO panel's decision and potentially order the domain name to be returned to him. Section 1114(2)(D)(v) offers a remedy for a registrant who has lost a domain name under the UDRP, allowing them to seek an injunction to regain the domain name if they can demonstrate compliance with the ACPA. Thus, a declaration of Sallen's compliance with the ACPA would redress his loss of corinthians.com in the UDRP proceeding. Even an agreement by the defendant to waive his right under the ACPA does not necessarily negate the court's decision. Section 1114(2)(D)(v) provides disappointed administrative dispute resolution participants with a chance to have any unfavorable UDRP decision reviewed in a U.S. court.

In essence, under certain circumstances, a court's decision under the ACPA can override or supplant an administrative panel's decision under the UDRP.

5.2 Kenya

The first cybersquatting case in Africa was *UEFA v Funzi Furniture in Kenya*.[66] UEFA[67], the European football governing body, took action against Funzi Furniture, a Mombasa-based company, for registering the domain name 'championsleague.com' in bad faith. Despite Funzi registering the domain name first, the company attempted to sell it to UEFA for $1.45 million. UEFA filed a complaint with the Arbitration and Mediation Centre, which ruled in their favour. The panellists found that the domain name was identical to UEFA's trademark, Funzi had no legitimate interest in the name, and the company had registered and used the domain name in bad faith. Funzi's intention was to profit from the domain name by reselling it at a high price and attracting visitors to its furniture business.

Kenya has a growing online presence, and as a result, domain name registration and cybersquatting laws are becoming increasingly important. Kenya has its own country-code top-level domain (ccTLD) .ke, managed by the Kenya Network Information Centre (KENIC).[68]KENIC implements policies to prevent and resolve domain name disputes, ensuring a fair domain name space management. KENIC has developed a Domain Name Dispute Resolution Policy (DRP) based on the principles of the Uniform Domain Name Dispute Resolution Policy (UDRP) established by ICANN. This policy provides a fast and cost-effective process for resolving domain name disputes, it offers a more efficient and

[65]Sallen v. Corinthians Licenciamentos LTDA, 273 F.3d 14 (1st Cir. 2001).

[66] UEFA and Funzi Furniture (2000) WIPO Case No. D2000-0710, <https://www.wipo.int/amc/en/domains/decisions /html/2000/d2000-0710.html> accessed on 8 May, 2024.

[67] Union des Associations Europeennes de Football (UEFA).

[68]M.M. Gatune, Competitive *Strategies Adopted By Kenya Network Information Centre (KeNIC)* (Doctoral dissertation, University Of Nairobi 2012).

affordable solution compared to traditional legal proceedings. To initiate proceedings under the DRP, a complainant must prove that the domain name is similar and confusingly similar to their trademark, the registrant has no legitimate right to the domain name, and the domain name was registered and used in bad faith. The domain name disputes under the DRP are typically settled through alternative dispute resolution methods, either arbitration or mediation. Several organizations offer these services, including the Arbitration and Mediation Centre (AMC) and the WIPO Arbitration and Mediation Centre, which are accredited to help resolve domain name disputes.

While there aren't many reported cases specifically on domain name disputes and cybersquatting in Kenya, there have been instances where companies and individuals have sought legal recourse for such matters. One notable case involves the dispute between Kenya Airways and a domain name registrant, Caroline Kariemu.[69] In this case, Kenya Airways Limited filed a complaint against Caroline regarding the domain name 'kenyaairways.com'. Kenya Airways argued that the domain name was identical to its name and trademark and that the respondent had no legal right to use it. Despite Kenya Airways' request for the transfer of the domain name, the respondent did not respond. The UDRP regulated the procedure. According to the policy, Kenya Airways had to establish three elements: the domain name's identity or similarity to its trademark, the respondent's lack of legitimate interests in the domain name, and the domain name's registration and use in bad faith. The panel found that the domain name was indeed identical to Kenya Airways' trademark. Additionally, the respondent had no legitimate rights or interests in the domain name, as they had not been licensed to use the trademark. The panel also concluded that the domain name was registered and used in bad faith, as the respondent had prevented Kenya Airways from using its own name and trademark and had failed to respond to Kenya Airways' correspondence. Therefore, the panel ordered the transfer of 'kenyaairways.com' to Kenya Airways Limited.

The Kenyan laws which regulate domain name protection and cybersquatting includes:

1. The Computer Misuse and Cybercrimes Act, 2018
2. The Kenyan Trademarks Act, 2009

The Computer Misuse and Cybercrimes Act enacted in 2018 is Kenya's primary legislation on cybercrime, providing a legal framework for the investigation, prosecution, and punishment of cybercrimes, including cybersquatting, online fraud, hacking, and other related offenses. Section 28 of the Act makes provision for cybersquatting. It stipulates that:

> *A person who, intentionally takes or makes use of a name, business name, trademark, domain name or other word or phrase registered, owned or in use by another person on the internet or any other computer network, without authority or right, commits an offence and is liable on conviction to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years or both*.

This provision aims to protect individuals and organizations from cybercriminals who seek to profit from their reputation, goodwill, or brand identity. The Act's provisions on cybersquatting are crucial in preventing online identity theft, fraud, and consumer deception, and ensuring that individuals and businesses can safely conduct online transactions and

[69]Kenya Airways v. Caroline Kariemu, AF-0313 (UDRP, 2000) <https://www.disputes.org/decisions/0313.htm#:~:text=Complainant%20is%20the%20holder%20of,a%20period%20of%2014%20years> accessed on 10 May 2024

maintain their online presence. It seems to have similar wording to Section 25 of the Nigerian Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, highlighting the shared concern and approach to addressing cybercrimes across jurisdictions.

The Kenyan Trademarks Act provides legal protection for registered trademarks, enabling trademark holders to pursue legal action against infringement, including cases of cybersquatting involving domain names. According to Section 5 of the Act, "No person shall be entitled to institute any proceeding to prevent, or to recover damages for, the infringement of an unregistered trademark," but the person can seek an action for passing off. Thus, it is essential to register a trademark in Kenya to enjoy full legal protection, as is also the case in Nigeria.

Kenya's efforts in regulating domain name protection and cybersquatting reflect its commitment to fostering a secure online environment. The resolution of notable cases like UEFA v Funzi Furniture and Kenya Airways v Caroline Kariemu demonstrates the judiciary's dedication to upholding the rights of trademark holders and deterring bad faith practices in cyberspace. By aligning its policies with international standards and leveraging alternative dispute resolution mechanisms, such as the UDRP, Kenya aims to build trust and confidence in its digital economy, safeguarding the interests of individuals and businesses.

6.0 Conclusion and Recommendations

6.1 Conclusion

This critical appraisal has examined the concept of domain name protection and cybersquatting in the Nigerian legal system, highlighting the challenges and gaps in its application. The existing legal framework, including the Cybercrimes Act and the Trade Marks Act, provides some protection against cybersquatting, but there are limitations and inconsistencies in their application. While Nigeria has enacted specific legislation on cybersquatting, the effective implementation and enforcement of these laws remain a challenge. Moreover, the absence of reported court cases on cybersquatting in Nigeria makes it difficult to determine the effectiveness of the existing laws and regulations.

To enhance the efficacy of domain name protection and combat cybersquatting in Nigeria, recommendations have been proposed, including increasing awareness and education on domain name protection and cybersquatting, and international cooperation and collaboration. Additionally, further clarification and guidance on specific aspects of domain name protection and cybersquatting may be necessary to address the existing gaps and inconsistencies in the legal framework. The legislation should be amended to streamline NIRA's authority for clarity. There also ought to be clear guide line for addressing complaints. This guideline must be objective and pragmatic.