Journal of Law, Policy and Globalization
ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online) DOI: 10.7176/JLPG
Vol.84, 2019

Legislating Against Cybersquatting in Nigeria: Moving Beyond Penal Law Into Protective and Compensational Remedies

Dr. Bernard Oluwafemi Jemilohun
Faculty of Law, Ekiti State University, PMB 5363, Ado-Ekiti
Ekiti State, Nigeria

"It appears almost to be the case that an incident of cybersquatting is an integral consequence of commercial success" – Ian J. Lloyd (2011)

Abstract
This paper analyses the menace of cybersquatting on the cyberian frontier in Nigeria with a look to offer real protection to owners of real trademarks and domain names. It examines the provisions of the United States Anticybersquatting Consumer Protection Act of 1999 and the practice adopted in the UK to protect real trademark owners. It examines Nigeria's recent effort at legislating to combat cybercrime via the Cybercrime (Prohibition, Prevention Etc.) Act, 2015 especially the provisions of Section 25 dealing with cybersquatting and points out the various inadequacies of the legislation. It suggests the need to move beyond a criminal viewpoint and penal sanctions and allow for remedies in the laws of tort that secures private rights. It concludes by challenging law-making authorities in Nigeria to make laws that accord with global trends in the light of the inter-territoriality of cyberspace.

Keywords: Cybersquatting, domain names, Infringement, Internet,
DOI: 10.7176/JLPG/84-10
Publication date: April 30th 2019

1. Introduction

One of the greatest benefits of a law-governed society or organisation is the protection of personal and business interests and the availability of remedies where there are grievances due to abuse. An example is the law of passing off, which is an arm of the law of torts that protects the rights of a business owner from attempts by another person to present his own business as that of the original owner and thus enjoy the patronage due to another without authorisation. In the case of *Erven Warnink v Townend* (The Advocaat case), Lord Diplock described the tort of passing off as the misrepresentation made by a trader in the course of trade, to prospective customers of his or ultimate consumers of goods and services supplied by him, which is calculated to injure the business or goodwill of another trader and which causes actual damage or will probably do so. The essence of this is to prevent unlawful gain accruing to the offending party and also injury to the rightful owner by the wrongful appropriation of his business identity and the provision of remedies for the same.

In the age of technology, business names and identities have also acquired some sort of digital nomenclature and form. The widespread use of the Internet has opened the doors for businesses to have online presence and expand their trading capabilities beyond the brick and mortar platform. Thus, the domain name system grants to businesses and other organisations some sort of digital name by which they are identifiable and known in cyberspace and also by which they can be traced. The gains and benefits derivable from e-commerce today will not be that profitable and enjoyable if businesses trading on the web do not have a means by which those digital identities are recognisable and protected.

The problem that arises sometimes is that another person who is not in the least connected with the digital identity of a business or rights emanating from it may desire to appropriate the same and claim the benefits arising there from. When another person without the permission or the authorization of the real owner of the domain name attempts to present the name or identity as his own either to derive financial gain or secure some other interests, legal rights are violated and the law must rise to secure the interests of the genuine owner, punish the offender and compensate the owner for losses sustained in the course of the infringement while preventing further acts of infringement from the offender or any other party with similar intention. The case of *British Telecommunications Plc & Ors v One in a Million* is very instructive here.

In the online world, the advances in digital technology make infringement of intellectual property and violation of private rights much easier than before. (Oyewumi, 2015) Businesses now deserve to use the Internet in furtherance of their objectives and a trade mark owner should have exclusive rights to register his mark and own the same on his domain. Where a business has been known to do business or engage in transactions in a particular name or with a particular trademark, using the trademark or name as a domain name on the Internet should be the exclusive preserve of such a business.

But some unscrupulous individuals or entities have learned the wisdom of registering domain names ahead of the persons who should have rights to the domain name either with the intent to divert the business interest to themselves or with the aim of selling the registered domain name to the right owner for a fee. This act of registering

a domain name without right is what is known as cybersquatting. And it is also referred to as domain-name hijacking

2. The Significance of Domain Names in Nigeria

As the commercial usage of the Internet has increased over the years globally, the benefits of obtaining a domain name which is identifiable with the business of the owner has also become more recognized. (Lloyd, 2011)

That Nigeria is expanding its frontiers in cyberspace is not news. The rate of Internet penetration in Nigeria is rising by the day and the present rate of Internet users testify to this. With a 2018 population estimate of 195,875,237, Internet users as at December 2017 are 98,391,456 which presently amount to a 50.2% Internet penetration. With this level of awareness one can be sure the level of e-commerce will be comparative. There are presently several businesses with online presence in Nigeria and the rate of trading via the Internet is growing consistently.

The present force moving e-commerce expansion in Nigeria is largely driving by private initiatives. Up till now, there is no legislation that is specifically targeted at enhancing electronic transactions within the Nigerian statute books. Several bills have been prepared in the past with some sort of relevance to electronic transactions but none of them has seen the light of day. Examples of such Bills include the Computer Security and Critical Information Infrastructure Protection Bill 2005, the Cyber Security and Data Protection Agency (Establishment, etc.) Bill 2008 the Electronic Fraud Prohibition Bill 2008, the Nigeria Computer Security and Protection Agency Bill 2009, the Computer Misuse Bill 2009, and the Economic and Financial Crimes Commission Act (Amendment) Bill 2010. However, several institutions, organizations and companies in the country have registered their corporate and business names as domain names thus making them easily identifiable in cyberspace.

The Nigerian business landscape is one that is taking more and more advantages of internet access and the possibilities in cyberspace. The present number of Nigerian businesses that have registered domain names on the internet may not be easy to find out. A search on the website of the Nigeria Internet Registry Association reveal that there are 134, 320 active .ng domains as at February 2019. One may not know about other businesses operating within the Nigerian cyberspace but using a generic TLD (Top Level Domain) or even another country code TLD yet having customers and clients in the country.

Nigeria currently has 61 domain name registrars, all operating under the authority and accreditation of the Nigerian Internet Registration Association. If there is anytime the legislative framework for domain name disputes and methods of resolution should be clearly stated in Nigeria, it should be now.

3. The Phenomenon of Cybersquatting

The word "cybersquatting" is simply a combination of two words: "cyber" and "squat". In simple language it should refer to illegal or wrongful dwelling in cyberspace. According to the United States' Anticybersquatting Consumer Protection Act, cybersquatting is registering, trafficking in or using an internet domain name with bad faith intent to profit from the goodwill of a trademark belonging to somebody else. The cybersquatter then offers to sell the domain name to the person or company identified by the name or who owns a trademark contained within the registered domain name at a higher price.

The Nigerian Cybercrimes (Prohibition, Prevention Etc.,) Act (2015) defines cybersquatting as "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
(iii) Acquired without right or with intellectual property interests in it."

While it is possible that the scope of cybersquatting varies depending on the legal context, it may be generally characterised as the abusive registration of domain names which are regarded as bad faith registrations *vis a vis* certain pre-existing rights owned by others. (Wilson, 2009). A variant of cybersquatting is known as *typosquatting* which is the abusive registration by a third party of the misspelled version of an existing domain name (or registered or unregistered trademark) (Wilson, 2009). Another similar act of cybertheft is called *cyberpiracy,* which is defined as "the practice of registering domain names that incorporate variations on famous trademarks for the purpose of taking unfair advantage.

Cybersquatting came into prominence in the United States in 1990s before most businesses became active on the internet. People bought domain names of businesses with plans to sell the domains to those businesses for profit. But as businesses realised that the internet was a developing market place and having a website was important, they tried to buy the domain names only to be faced with large fees from the cybersquatters.

Finding that cybersquatting results in consumer fraud and public confusion, impairs e-commerce, deprives legitimate trademarks owners of revenue and goodwill, and places burdens on trademark owners, the American

legislature moved against the menace by a direct legislation that amended the Lanham Act to protect American consumers and businesses, to promote the growth of online commerce and to provide clarity in Trademark law by prohibiting the deliberate, bad faith and abusive registration of distinctive marks as internet domain names with the intent to profit from the trademark's goodwill. (Mota, 2003)

Presently in Nigeria, there have not been too many cases on cybersquatting or its various shades. But the dynamic nature of the internet and the speed of technological advancements should cause every right thinking and forward looking nation to prepare by appropriate legislation and regulatory framework. It appears the only two cases that emerged in recent times were settled outside the judicial process. The first case is that of *Konga v Jumia* wherein Rocket Internet, owners of Jumia.com registered the domain of Konga in about 11 African countries. The facts show that the domains were registered in June 2012 whereas Konga launched in July 2012. The other case was that of *Linda Ikeji v Emmanuel Efremov* where one Emmanuel Efremov knowing that Linda Ikeji blogs on Lindaikejisblog.com went ahead and registered Lindaikeji.net and used the reputation of the blogger to earn advertising revenue. Upon the exposing of his cyberquatting activity, he redirected the infringing site to Linda Ikeji's blog.

4. The Nigerian Cybercrime Act in Perspective

The Nigerian Cybercrimes (Prohibition, Prevention, Etc.,) Act is explained to be an Act that provides an effective, unified and comprehensive, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. It is also aimed at ensuring the protection of critical national information infrastructure, while promoting cybersecurity and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.

Section 25 of the Act is a direct enactment against cybersquatting. It provides as follows:

(1) "Any 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 any individual, body corporate or belonging to either the Federal, State or Local Governments in Nigeria, on the Internet or any other computer network, without authority or right, and for the purpose of interfering with their use by the owner, registrant or legitimate prior user, commits an offence under this Act and shall be liable on conviction to imprisonment for a term of not more than two years or a fine of not more than N5million or to both fine and imprisonment.

(2) In awarding any penalty against an offender under this section, a court shall have regard to the following:

(a) A refusal by the offender to relinquish, upon formal request by the rightful owner of the 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 Government of Nigeria.

(b) An attempt by the offender to obtain compensation in any form for the release to the rightful owner for use of the 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 Government of Nigeria

(3) In addition to the penalty specified under this section, the court may make an order directing an offender to relinquish such registered name, mark, trademark, domain name, or other word or phrase to the rightful owner."

In the framework of the Cybercrime Act, cybersquatting is seen more from the perspective of a criminal act than a civil wrong necessitating that certain remedies should accrue to the wronged party as a matter of priority. For example, the definition accorded cybersquatting in the Act seems to concern itself with registered trademarks. In the language of the statute, it should be "an existing trademark registered with the appropriate government agency at the time of the domain registration". It seems on the face of it that an unregistered trademark may not be afforded similar protection to a registered one where same is being deprived the rightful owner. This may be compared with the WIPO dispute resolution panel case of *Jeanette Winterson v Mark Hogarth* where the Panel found and ruled that "The Rules do not require that the Complainant's trademark be registered by a government authority or agency for such a right to exist."

Secondly, the operative word that deals with wrongdoing in section 25 is the word "penalty". This is indicative of the mind-set of the lawmaker who sees cybersquatting more as a wrong against the state deserving of punishment and not really a civil wrong against an individual deserving of restitution and the award of damages. The payment of the stipulated penalty of N5,000,000 or less may be deterrent to potential cybersquatters, but it affords no real remedy to the wronged party.

On the third level, the Act appears to make no separation between private interests belonging to individuals and public interests belonging to government. The language of the Act is about "a name, business name, trademark, domain name or other word or phrase registered, owned or in use by any individual, corporate body or belonging to either the federal, State or Local Governments in Nigeria". One would have thought that in an age where private and personal interests are clearly distinguished from public and government interests, the Act will state this dichotomy.

It is also worth noting that while the enactment states that in addition to the penalty specified as payable by the offender, the court *may* make an order directing the offender to relinquish such name to the rightful owner. It

is worrisome that the operative word is "may" and not shall. It seems the lawmaker is more concerned with the penalty than the need to preserve the interests of commerce and remedy wrongs done to private businesses.

Unlike the United States Anticybersquatting Consumer Protection Act, the Nigerian legal framework does not have provisions affording any protection to administrators of domain names within the region. This may largely be because only the powers of the courts are recognised in the Act despite the fact that a proper institutional framework ought to be in place. The focus of the law is so penal that no other parties are considered apart from the offender and the state.

Some writers (Davies, 1997; Mercer, 2000) have argued that cybersquatting should be treated as blackmail because it is the using of the goodwill of another to extort money from him or her. In the opinion of Mercer (2000), although cybersquatting can fit into the general criminal law framework for blackmail, (after all it is the law that says what is a crime or not) the criminal punishment corresponding to blackmail should not be made applicable to cybersquatting. Criminal punishment has at least two major purposes: to act as a deterrent and to provide retribution.

Of course, criminal punishment of cybersquatters would probably be effective as a general deterrent, because other will be less inclined due to criminal sanctions. It may also provide a specific deterrent because it would severely limit the cybersquatter's access to money and to the internet both of which are necessary to register a domain name. Mercer (2000) however opines that the main problem with applying criminal sanctions to cybersquatters is that the punishment is too harsh. Although cybersquatting is a crime against society, the real and directly injured is probably the trademark owner and trademark infringement being an aspect of unfair competition should not be a crime but a tort. He concludes that sanctions against cybersquatters should be handled through civil and not criminal sanctions.

5. The United States and the United Kingdom

It is important at this point to examine the legislative approach to combatting cybersquatting in more advanced democracies like the United States and the United Kingdom. Comparative law is an instrument for development and since the challenges arising from the ubiquitous nature of the internet are not peculiar to any nation, it becomes important to see how other nations have approached the problem. I choose to consider these two nations because our government is patterned after the model of the United States while United Kingdom laws have strongly influenced Nigerian laws.

5.1 The United States

The legal framework for the prohibition of cybersquatting in the United States is largely contained in the Anticybersquatting Consumer Protection Act (ACPA 1999) which is a federal legislation and an expansion of the Trademark Act (1946) and is intended to provide protection against cybersquatting for individuals as well as owners of distinctive trademarked names and promote electronic commerce generally. Prior to the enactment of the ACPA, there was no clear deterrent to cybersquatting. While the Federal Trademark Dilution Act was used successfully against cybersquatters, Congress still believed that a specific legislation was necessary. (Senate Report, 1999)

In the United States, it is possible to bring an action against the domain name under the Anticybersquatting Act. *Kremen v Kohen* is an example of this. Trademark holders now have a cause of action against anyone who, with a bad faith intent to profit from the goodwill of another's trademark, registers, traffics in, or uses a domain name that is identical to, or confusingly similar to a distinctive mark, or dilutive of a famous mark, without regard to the goods or services of the parties.

The law also establishes *in rem* jurisdiction under Section 3 of the ACPA which allows the trademark owner to file an action against the domain name itself in some cases, such as where the domain name violates any right of the registrant of a mark registered in the Patent and Trademark Office and where after due diligence, the owner was not able to find the person who would have been a defendant in a civil action under the earlier paragraph. This makes it more appealing to claimants who have the resources to file claims relating to .com, .net in the United States. The remedies of an *in rem* action under Section 3 (2) (b) of the ACPA is however limited to a court order for the forfeiture or cancellation of the domain name to the owner of the mark.

In determining bad faith, the law states the factors that are to be considered. The first four will count against a determination of bad faith while the remainder would weigh in favour of a bad faith determination:

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 legitimate non-commercial 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 substantial consideration without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services.
7. The person's intentional provision of material and misleading false contact information when applying for the registration of the domain name.
8. the person's registration or acquisition of multiple domain names which are identical or confusingly similar to trademarks or service marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous trademarks or service marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of such persons.

It is worth noting that while the legislation specifically provides that bad faith intent shall not be found in any case in which the court determines that the person believed, and had reasonable grounds to believe, that the use of the domain name was a fair use or otherwise lawful, the legislation fails to address whether knowledge of the existence of an unrelated business using the same or similar mark will constitute bad faith.

The legislation provides some general remedies in cases of domain name piracy, namely, injunctions and damages and goes further to create what is known as statutory damages by providing that in addition to traditional trademark remedies, plaintiffs may elect at any time before final judgment is delivered by the trial court to recover instead of actual damages and profits, statutory damages in an amount ranging from $1,000 to $100,000 per domain name.

Another important aspect of the legislation is that, the factors for determining bad faith can be applied by the domain name registrar. Thus, in an effort to provide less expensive and timely legal remedies, the legislation allows the registrar to fill the shoes of a court in determining bad faith and exempts them from liability if they do so. If the registrar decides against the domain name holder, the domain name holder will have no recourse against the registrar.

Further, in a small effort to prevent reverse domain name hijacking, the Act makes a trademark owner who knowingly misrepresents a domain name to be infringing, liable to the domain name holder for damages and attorneys' fees resulting from cancellation.

A case that came up for determination shortly before the ACPA was enacted but which appeal met the ACPA is the case of *Sporty's Farm L.L.C. v. Sportsman's Market Inc.* The matter was instituted under the Federal Trademark Dilution Act wherein the plaintiff brought an action to continue the use of the name "Sportys.com" and the defendant counterclaimed for trademark infringement and trademark dilution. The appeal court ruled in favour of the defendant/counterclaimant finding the domain name confusingly similar and further ruling that there was bad faith intent to profit on the part of the plaintiff. Thus the first appellate court upheld an injunction against the company registering another's trademark as a domain name.

Apart from the adversarial procedure of righting domain name wrongs, there is also the Uniform Domain Name Dispute Resolution Policy which allows parties to come before panels to resolve their domain names disputes without the necessity of going before a court. Thus, instead of suing in federal court under the ACPA, a trademark owner can choose to pursue an administrative proceeding under the UDRP. This allows a trademark owner to challenge domain name registrations in expedited administrative proceedings.

A UDRP proceeding can be faster and cheaper for trademark owners than an ACPA lawsuit. Also, UDRP outcomes tend to be pro-plaintiff because many UDRP arbitrators are trademark lawyers. However, some trademark owners prefer to bring ACPA claims because they offer more remedies than the cancellation or transfer of the domain name (the only remedies available under UDRP proceedings) and a court ruling can lead to a final resolution of the matter. Also, a suit under the ACPA may deter future cybersquatters more effectively than a UDRP proceeding.

5.2 The United Kingdom

Registration of domain names in the United Kingdom is relatively easy and straightforward being online and automatic. (Wilson, 2009). As a matter of fact, it is only domain names that are identical to existing .uk domain names that are rejected. The registry of the .uk domain name is Nominet under which other domain name registrars function to serve applicants/registrants. It is the duty of the applicant/registrant to maintain the accuracy of the contact details, having asserted the right to use personal details relevant to the domain name registration. The registrant also undertakes that the registration does not infringe third party intellectual property rights, including trademarks, and confirms that the registrant has the right to register the domain name.

There is no specific legislation in the United Kingdom dealing with domain name disputes similar to the situation in the United States. It is the Trade Marks Act of 1994 that governs where a trademark has been infringed

or where the aggrieved party may bring an action on the basis of fraud. (See for example, Section 10) Thus, the legitimate owners of the domain names who feel they have a better right to it may only bring actions for infringement of trademark or the tort of passing off. *British Telecoms & Ors v. One in a Million*

In the United Kingdom, it is not yet possible to bring an action against a domain name as a proceeding in rem as it is in the US. This is because English courts have adopted a very narrow interpretation of when such jurisdiction is available. Under the terms and conditions of the .uk registry, "a domain name is not an item of property and has no 'owner'. It is an entry on our register database reflected by our nameservers which we provide as part of this contract".

However, despite the absence of a single legislative framework to combat cybersquatting, there is the operation of the Uniform Domain Name Dispute Resolution Policy. Ian J. Lloyd posits that one of the early domain name disputes in the United Kingdom was about attempts by domain name registries such as Network Solutions and Nominet to devise policies designed to render them immune from legal action. (Lloyd, 2011) This was because in many situations, the agencies were put in difficult legal positions like it happened in the case of *Pitman Training Ltd v Nominet United Kingdom* where the domain name registry (Nominet) was threatened with legal action by one party unless the name was reassigned and with action by the other in the event that it was reassigned.

The emergence of the Internet Corporation for Assigned Names and Numbers (ICANN) as the coordinating body for the domain names system, a new approach was introduced to resolve domain name disputes. The Uniform Domain Name Dispute Resolution Policy was introduced and any organisation interested in acting as a registry had to conduct business according to the UDRP. Thus applicants had to submit to mandatory dispute resolution procedures before approved dispute resolution providers in the event of issues that may arise.

Of the four organisations namely the Asian Domain Name Dispute Resolution Centre, CPR Institute for Dispute Resolution, the National Arbitration Forum and the World Intellectual Property Organization that were initially recognised as capable to offer dispute resolution services under the ICANN rules, only the World Intellectual Property Organisation has been the major player and sustained activity in the field.

6. The Need for New Laws

While one cannot overlook the fact that criminality has moved into cyberspace, one may also freely observe that it is not in all instances that regulating interactions in cyberspace would be by the instrumentality of criminal laws and penal sanctions. The basic problem with cybersquatting is that it robs others of the reward of their innovation and sometimes their means of livelihood. The menace of cybersquatting has more debilitating effect on businesses and private intellectual productivity than on the government directly.

The present Nigerian legislative framework is rooted in the law of crime. The sole aim of the Cybercrime Act is punishment for offenders and deterrence to intending offenders. There is really nothing in the law that takes the need to adequately compensate the victim into serious consideration. There is need to amend the law as it stands, separating remedies and restitution provisions from penalties. The sections dealing with cybersquatting can be either incorporated into other laws governing trademarks or made into a whole new enactment in the light of developments in cyberspace.

Nigeria needs to take a cue from the American legislation on Cybersquatting. The Anti-cybersquatting Consumer Protection Act is an amendment to the Trademark Act of 1946 which was 'an Act to provide for the registration and protection of trademarks used in commerce, to carry out the provisions of certain international conventions, and for other purposes' It is noteworthy that the United States Congress did not consider it important to amend a penal statute while providing for the protection of consumers against cybersquatting, rather it amended a civil legislation that related to the issues at stake.

The main purpose of the American legislation is to protect consumers and not really to punish offenders alone. While punishment of offenders is necessary to maintain personal rights in society, that should not be the main aim of a legislation. The courts in the United States do not have any dilemma knowing what interests to secure in cases of cybersquatting. And more than the courts, wronged parties do not have to bother about whether a court will uphold their rights by restoring their domain names to them as well ordering the infringer to pay damages or simply penalise the offender and leave them in the cold.

7. Conclusions and Recommendations

Recognising the role of the law as an instrument of regulating human interactions compels us to see the need to regulate this all important area of protecting intellectual property, business interests, the development of electronic commerce and minimising confusion in our cyberspace.

It is true that criminal conduct in the Nigerian "cyberian" frontier may demand very tough legislation to serve as deterrents to would be cyber criminals. But one strongly feels the challenges cannot be handled by a singular all-in-one enactment no matter how broad the scope is. The consciousness of criminal activities and deviant behaviour in cyberspace should not becloud legislative sense to prevent lawmakers seeing the need for remedies and restitutions where desirable and applicable.

This writer suggests that the Nigerian legislature take a cue from the United States Congress which found that "the registration, trafficking in, or use of a domain name that is identical or confusingly similar to a trademark or service mark of another that is distinctive at the time of the registration of the domain name, or dilutive of a famous trademark or service mark of another that is famous at the time of the 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''cyberpiracy'' and ''cybersquatting'')—
(a) results in consumer fraud and public confusion as to the true source or sponsorship of goods and services;
(b) impairs electronic commerce, which is important to interstate commerce and the United States economy;
(c) deprives legitimate trademark owners of substantial revenues and consumer goodwill; and
(d) places unreasonable, intolerable, and overwhelming burdens on trademark owners in protecting their valuable trademarks."

And by their findings made necessary amendments to the Trademark Act which clarified the rights of a trademark owner and provided for adequate remedies while deterring cybersquatting in all ramifications.

References

Davies, G. G. (1997) Internet Domain Namesand Trademarks: A Growing Area of Dispute, in PLI's Third Annual Institute for Intellectual Propoerty Law, at 649, 656

Friedman, N. J. & Siebert, K. (1997) *The Name Is Not Always The Same*, 20, Seattle U. L. Rev 631, 635-636

Lloyd, I. J. (2011) Information Technology Law, (6th ed. Oxford University Press,) 426

Mercer, J. D. (2000) Cybersquatting: Blackmail on the Information Superhighway 6 B. U. J. Sci & Tech . L. 290

Mota, S. A. (2003) The Anticybersquatting Consumer Protection Act: An Analysis of the Decisions from the Courts of Appeals 21 J. Marshall J. Computer & Info. L. 355

Oyewumi, A. O. (2015) *Nigerian Law of Intellectual Property*. Lagos: Unilag Press

Wilson, C. (2009) Domain Names and Trademarks in Edwards, L. & Waelde, C. (Eds) *Law and the Internet* (pp. 311-334)Hart Publishing, Oregon

nigerianlawtoday.com/squashing-the-squatter-on-cyberspace/ accessed on 25th March 2019

Nominet, 'Terms and Conditions of Domain Name Registration' Clause 10, available at http://www.nominet.org.uk/registrants/aboutdomainnames/legal/terms

United States Senate Report 106 – 1410 (1999)

www.internetworldstats.com/top20.htm accessed on 23rd March 2019

www.nira.org.ng accessed on 25th March 2019

http://arbiter.wipo.int/domains/

Cases

Erven Warnink v Townend (The Advocaat case) [1979] A.C. 731

British Telecommunications Plc, Virgin Enterprises Ltd, J Sainsbury Plc, Marks & Spencer Plc and Ladbroke Group Plc v One in a Million [1998] FSR 265, (High Court) [1999] FSR 1

Sporty's Farm L.L.C. v. Sportsman's Market Inc 202 F.3d at 489

Pitman Training Ltd v Nominet United Kingdom [1997] FSR 797