CRIMINALISATION OF CYBERSQUATTING IN NIGERIA, ENGLAND AND THE UNITED STATES: AN UNUSUAL COEXISTENCE OF CRIMINAL LAW AND INTELLECTUAL PROPERTY RIGHT

Written by ***Abiodun Ashiru***

Lecturer, Faculty of Law, Lagos State University, Ojo, Lagos, Nigeria

ABSTRACT

With the advent development of the internet and the rapid digitisation of the world, almost all forms of human rights are affected and the right to own and acquire intellectual property is not left out. The ease of flow of communications over the internet comes with some disadvantages, one of which is that the internet may expose a company's intellectual property to theft and misuse. Cybersquatting which is the registering, selling or using a domain name with the intent of profiting from the goodwill of someone else's trademark is the latest weapon used by perpetrators of this vice. Cybersquatting is the most crucial type of domain dispute prevalent around the world. It is a practice where individuals buy domain names reflecting the names of existing companies, with an intention to sell the names back to businesses to attain profit when they want to set up their own websites. This paper principally adopts a comparative legal method of analyses to analyse the legal regime of cybersquatting in Nigeria, England and the United States. The paper inquiries into the criminalisation of cybersquatting as a violation of intellectual property which ordinarily falls under the civil law regime. The paper further assesses the adequacy of the laws with a view or providing alternatives legal actions upon which a violation of the property right may be brought to court. The paper concludes that cybersquatters have robbed businesses of their fortune and recommends that there is a need for the Nigerian Government to model its law after the WIPO model.

Keywords: Cybersquatting, Domain Name, Intellectual Property, WIPO, ACPA.

INTRODUCTION

The first time when the cybersquatting term was used was in USA in the early nineties and it was the time when Internet babble exploded. Various individuals and organization could join in common network and share information. The Internet allows many users simultaneously connect and exchange big amount of date- like images, sounds by going to different web pages or web sites. There was and still is huge marketing and sales potential in Internet and unfortunately at this time not everybody could see it from the being. Long before many large companies realized the massive volume of traffic that the Internet could bring to their business, cybersquatters paid for and registered domain names using the trademarks of several prominent businesses. Before 1999, Internet as a tool for success was still being resisted by businesses across the world. Cybersquatters took advantage of growing importance of the internet and the ignorance of the businesses towards it. This gave birth to cybersquatters who registered domain names identical to business trademarks. Since customers and clients try to find businesses online, this became an issue for the companies whose trademarks were already taken by the squatters as they could no longer have their trademarks as domain names. Cybersquatting causes monetary losses and damaged reputation to businesses. In this research work, the meaning, techniques and types of cybersquatting are examined. In addition to this, the research examines the relationship between cybersquatting and intellectual property.

MEANING OF CYBERSQUATTING

Cyber-squatting is a term derived from "squatting". The term squatting is defined as the act of occupying an abandoned or unoccupied space or building that the squatter does not own, rent, or otherwise have permission to use. Cybersquatting on the other hand is defined according to the Anti-cybersquatting Consumer Protection Act of the United States Federal Law as registering, trafficking in, or using an Internet domain name with bad faith, intent to profit from the goodwill of a trademark belonging to someone else.[i] It is simply put the registration of domain names of well-known trademarks by non-trademark holders who then try to sell the names back to the trademark owners.[ii] It is generally defined as the registering, sale or use of a

domain name containing a trademark that the registrant does not have the rights to with the intent to profit from the goodwill of the mark.[iii] Cybersquatting, also known as domain squatting, is the practice of registering domain names, especially well-known company or brand names or trademarks, in the hope of reselling them at a profit. It is used to describe an individual or company who intentionally purchases a domain and holds that domain with the sole intention of selling it at a premium price.[iv] The Black's Law Dictionary states that the "act of reserving a domain name on the internet, especially a name that would be associated with a company's trademark, and then seeking to profit by selling or licensing the name to the company that has an interest in being identified with it" is cybersquatting. [v]

The Nigerian Cybercrimes (Prohibition, Prevention, ETC) Act, 2015 (the Cybercrime Act defines Cybersquatting as to 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.[vi] It is to be noted that persons who cyber squat are regarded as cyber squatters, and they generally depend upon the goodwill associated with someone else's trademark. By buying up domain names that are closely linked with a pre-existing business or person, cyber squatters hope to profit through an association with well-known trademarks or through sale of the domain to the trademark owner. Cyber squatters may also have more nefarious purposes such as capturing personally identifying data from unsuspecting users mistyping the URL. Thankfully, there are legal options to help you recover from a cybersquatting-related offense, including the Anti-Cybersquatting Consumer Protection Act (ACPA) applicable in the United States of America.[vii]

An essential point to note is that there must be an element of bad faith by the cybersquatter. In other words, the cybersquatter intended to interfere with the rightful owner's use of the domain name, or trademark by profiting from it if and when he sells the domain name to the rightful owner. It should be noted that domain names are registered in the registrant's favour on a first come, first-served basis without any recourse to existing trademarks.[viii] There are several variations of cybersquatting; and it could refer to advertisers who mimic domain names that

are similar to popular, highly trafficked websites. The intent of undertaking this action is to profit from an established brand's goodwill among consumers. There are few ways you can tell if you have been the victim of cybersquatting. Generally, you should first check out the domain name that you want to register to see if it leads to a legitimate website. If the address is of a website that looks to be functional and related to the subject of the domain name, then you have most likely just come to the game too late and will have to offer to buy the domain name unless you can make a case for trademark infringement.

For clarity sake, a domain name is a unique internet address which helps internet users to locate or access a particular website. It serves similar functions as a physical public address; it enables its users to easily find persons or computers on the internet. Examples of some popular domain names include: www.facebook.com, www.amazon.com, www.mercedes-benz.com. Domain names are intangible assets and as such falls under the category of intellectual property. Domain names are similar to trademarks; as they assist in identifying a particular brand (in this case an internet address) and to refer users to it. Like a trademark, a domain name indicates a connection in the course of trade between the goods or services and the proprietor as well as enables direct access to the goods or services from anywhere in the world. It is therefore equally essential to protect a domain name from infringement in the same manner as trademarks.[ix]

EXAMPLES OF CYBERSQUATTING

Typo Squatting

More often referred to as a "fake URL," typo squatting takes advantage of typing errors that consumers make while trying to visit websites. This often includes common misspellings of trademarked properties or typos. Infringers who utilize this tactic will often create a fake website to accompany the domain address. This can trick consumers as to the source of products they are purchasing. Cyber squatters may also utilize varying top-level domains in order to compel trademark owners to buy the website.[x]

Name Jacking

Personal names can be trademarked in the United States under certain circumstances. This typically only occurs if they have established secondary meaning in the market (e.g. Madonna, Beyoncé). Name jacking is a complex area of the law, so it may not always fall under the Anti-Cybersquatting Consumer Protection Act. Name jacking can also occur on social media. Even in the absence of a registered domain name, creating a profile representative of a celebrity or famous individual could constitute cybersquatting. This is another murky area considering the number of fan sites currently in existence. If the page starts selling unlicensed merchandise, it may be considered evidence of cybersquatting.[xi]

LEGAL FRAMEWORK FOR THE CRIMINALIZATION OF CYBERSQUATTING IN NIGERIA, ENGLAND AND THE UNITED STATES

Section 25 of the Cybercrime Act Subsection 1 provides that intentional use or interference with a name, business name, trademark, or domain name, registered word or phrase owned by an individual or corporate body or any of the three tiers of government on a computer network or internet is an offence that attracts a fine of five million naira (₦ 5,000,000) or imprisonment for a minimum of 2 (two) years. The Act further provides in subsection 2[xii] that the court's award of penalty is determined by the cybersquatter's refusal upon a formal request, to relinquish to the real owner, the domain name, trademark etc. in question. The court may also give an order directing the offender to relinquish the domain name, trademark, etc to the rightful owner.[xiii] Section 47 vests the power of prosecution of offences stipulated under the Act in "relevant law enforcement agencies" subject to the powers of the Attorney-General. Section 43 provides that the relevant law enforcement, intelligence and security agencies "develop requisite institutional capacity" in order to effectively implement the provisions of the Act. The relevant question is what are the relevant law enforcement agencies? The provision of section 47 may turn out to be a grey area that requires the court's intervention in interpreting. Law enforcement agents referred to in the section could be the Nigerian Police,

State Security Service, the Economic and Financial Crimes Commission, etc. There may be instances of clashes in determination of which agency should be in charge of investigation or even prosecution. The clear intent of the phrase "develop requisite institutional capacity" is also not definite. It might however be inferred that the law enforcement agencies are to be trained in line with modern day enforcement practices in investigation, arrest and prosecution of suspects. Section 49 vests the Federal High Court with the power to order restitution of money or property to a victim of cybercrime. Such an order is to be enforced in the same manner as judgment in a civil matter. The section does not specify restitution of domain name in the case of cybersquatting. From the analysis, it can be deduced that before an action can amount to cybersquatting under the Nigerian Cybercrimes Act 2015 (the Act), such a person must have:

a. acquired the domain name in bad faith,

b. with the intent to make profit, mislead, destroy or prevent others from registering the domain name,

c. the acquired domain name must be similar or identical to an existing registered trademark or the name of a person other than the registrant, in case of a personal name,

d. the domain name was acquired without right or with intellectual Property interests in it.

In other words, for an action against cybersquatting to succeed in Nigeria, the above conditions must be proved. However, it is not expressly clear whether these requirements should be conjunctively or disjunctively proven. Although the Cybercrimes Act (the 'Act') makes provision for the criminalization of cybersquatting and other computer-related offences in Nigeria, the Act does not provide for the establishment of a regulatory agency responsible for implementing the provisions of the Act. Notwithstanding this major loophole in the Act, certain regulatory agencies are indirectly responsible for the regulation of domain name system in Nigeria. One of such agencies is the National Information Technology Development Agency (NITDA) which is established under the NITDA Act to create a framework for the planning, research, development, evaluation and regulation of information technology practices in Nigeria.[xiv]

The Nigeria Internet Registration Association (NIRA), an incorporated trustee, is also one of the regulatory bodies, charged with the management of Nigeria's country code Top Level Doman Name (ccTLD), dotng. Although NIRA lacks any express statutory protection, nevertheless, a domain name applicant would ordinarily be expected to conduct an availability search by taking advantage of the search feature on the domain name registrar's website (on NIRA.org.ng). Upon registration of such domain name, there is protection against the use of identical and similar names as IP addresses by another person, both through NIRA and the Nigerian Courts.

Globally, the Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for overseeing domain name registration. ICANN has implemented thorough standards of acceptance to ensure that the assigning of domain names is done with much more scrutiny. ICANN has also put solid requirements for domain name recovery in place for instances of trademark registration lapses by trademark owners. ICANN adopts the Uniform Domain Name Dispute Resolution Policy (UDRP). The UDRP was by the World Intellectual Property Organisation (WIPO) for the resolution of disputes involving the registration of internet domain names. The UDRP enables trademark owners to bring an action against domain names which infringes on its trademarks. Under the UDRP, ICANN can cancel an improperly registered domain name or order a losing party to transfer the domain name to the winning party. The purpose of UDRP is to provide a cheaper and more efficient mechanism for resolving cybersquatting disputes. It is deemed to be a better alternative to litigation of disputes involving domain names. The procedure, however, does not preclude the filing of a lawsuit, either during or after the proceeding.

Under the Cybercrime Act, where a domain name is used in relation to any good or service which is identical or confusingly similar to an existing trademark and is likely to cause confusion, such use of a domain name can be said to be an infringement of the registered trademark. The Cybercrimes Act also prohibits the registration of a domain name that is similar to an existing trademark registration. The Cybercrimes Act defines the offence of cyber-squatting as including the acquisition of domain names that are, "similar, identical, or confusingly similar to an existing trademark registered with the appropriate government agency at the time of the domain name registration." This definition therefore clearly creates a link

between cybersquatting and trademark infringement. Although Cyber-squatting has been criminalized in Nigeria under the Cybercrimes Act, there are no records of any action taken against cyber-squatters so far. This might be as a result of the inadvertence of the legislature in not establishing an enforcement agency under the Cybercrimes Act. It is therefore suggested that an enforcement agency should be established and empowered to arrest and prosecute cyber-squatters and to also enforce the provisions of the cybercrimes Act in general.

In 1999, the United States Congress passed the Anti-Cybersquatting Consumer Protection Act[xv] (the "ACPA") as an amendment to the Lanham Act. The Act is directed at the practice of cybersquatting, or the acts of cyber squatters.[xvi] While it is admitted that it serves as an avenue in assisting trademark owners in protecting their brands on the internet, the nefarious activities of these cyber squatters have grown in leaps and bounds, with increasing innovation in the way domain names are cyber squatted. However, its significance as an American legislation cannot be overemphasized judging by the plethora of cases in which the legislation has been applied since its enactment. The passage of the legislation was influenced by the fact that the existing avenue for claims in the U.S. court (anti-dilution claims) was becoming increasingly inadequate in curbing the excesses of the cyber squatters.[xvii] The ACPA therefore provides a cause of action for an owner of trademark against any person who has a bad faith intent of profiting from the owner's mark and "registers, traffics in, or uses a domain name"[xviii] which is identical or confusingly similar to the owner's distinctive mark or that is identical, confusingly similar to or dilutive of the owner's famous mark.[xix]

It should be noted that an innocuous registration of a domain by someone who is ignorant of another person's use of the name does not qualify as cybersquatting. Hence, the United States' Senate Report on the ACPA[xx] gave a definition of cyber squatters as those who:

1. "register well-known brand names as Internet domain names in order to extract payment from the rightful owners of the marks;"
2. "register well-known marks as domain names and warehouse those marks with the hope of selling them to the highest bidder;"
3. "register well-known marks to prey on consumer confusion by misusing the do-main name to divert customers from the mark owner's site to the cyber squatter's own site;"

4. "target distinctive marks to defraud consumers, including to engage in counterfeiting activities."

It is therefore pertinent for the element of bad faith intent to be present in a case of cybersquatting. Under the Act, a trademark owner has the right to sue the person or corporate entity that created the "infringing domain name.[xxi] The trademark owner is also permitted to bring an *in-rem* jurisdiction over the actual domain name. In exercising an *in rem* jurisdiction under the Act, however, the trademark owner must show that it was unable to acquire *in personam* jurisdiction over the would-be defendant or the would-be defendant could not be located through due diligence.[xxii] In determining bad faith intent, the circumstances peculiar to each case are adduced to.[xxiii] It should however be pointed out, that the *ACPA* itself provided 9 (nine) factors that should be considered by the courts in ascertaining if the domain name registrant acted in bad faith[xxiv]:

i. the trademark or other intellectual property rights of the person, if any, in the domain name;
ii. 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;
iii. the person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;
iv. the person's bona fide non-commercial or fair use of the mark in a site accessible under the domain name;
v. 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;
vi. the person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct;

vii. the person's provision of material and misleading false contact information when applying for the registration of the domain name, the person's intentional failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct;

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

ix. the extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous within the meaning of subsection (c)(1) of this section.

The last five factors are particularly indicative of bad faith intent while the first four factors are considered as reasons why a defendant registered the domain name in good faith.[xxv] For a plaintiff to prevail, however, he must establish that the defendant has "bad faith intent to profit" from the act of cybersquatting.[xxvi] Under the ACPA, statutory damages ranging from $1,000 to $100,000 per each domain name may be recovered from the cyber squatter by the trademark owner.[xxvii] This is separate from the trademark owner's right to injunctive remedies. A proceeding under the ACPA can only be brought in a federal court. The ACPA has the legal jurisdiction to reverse a URDP based decision if such a result "is called for by application of the Lanham Act."[xxviii] The federal court can also reverse a URDP decision where it is in essence foreign or hostile to American Law.[xxix] In the United States of America, the Anti-Cybersquatting Consumer Protection Act (ACPA) is designed to allow trademark owners to sue an alleged cyber squatter in federal court. If the trademark owner wins, the lawsuits generally result in a court order requiring the cyber squatter to transfer the domain name to the trademark owner and, in some situations, pay monetary damages as well.

For a plaintiff to be successful in such a lawsuit, he or she must be able to prove the following;

a. That the trademark was distinctive at the time the domain name was first registered
b. That the domain name registrant (the alleged cyber squatter) had a bad faith intent to profit from the trademark

c. That the registered domain name is identical or similar enough to cause confusion with the real trademark, and
d. That the trademark is protectable under federal trademark law (meaning that the trademark is distinctive and its owner was the first to use the mark in commerce).

The registrant, in order to defend against the claim must show the judge that he had a reason to register the domain name other than selling it later to the trademark owner or otherwise exploiting the goodwill associated with the trademark.[xxx]

In the UK generally, there isn't a clearly defined internet domain name law since most of the legal framework is based on the law of contract. The United Kingdom like most other counties does not have specific laws to deal with cybersquatting. Nominet is the UK organisation with responsibility for administering the domain name system in the UK and has a well-developed and respected domain name dispute resolution process (DRS). For over 20 years, Nominet has been operating at the heart of the internet infrastructure as proud guardians of the .UK domain name registry. Nominet manages and runs over 10 million .UK domain names, as well as over 70 top level domains, including .wales, .bbc and .london. Nominet's understanding of the Domain Name System (DNS) underpins a sophisticated cyber-security capability. Used by the UK government and global enterprises to secure their networks, it highlights suspicious events at unprecedented speed, enabling real-time threat blocking.

In England, hijacking of domain name is a purely civil matter as the remedies are to be found in law of contract and tort law. This is unlike the Nigerian and America's approach. In Nigeria, cybersquatting is a crime and remedy is found in criminal law unlike in the United States which adopts both civil and criminal sanctions to remedy cybersquatting.

JUDICIAL RESPONSE TO CYBERSQUATTING

Many companies experienced cybersquatting in the early days of the internet. This is because forward-thinking cyber squatters would often purchase domain names before corporations even realized they should by them. Even with knowledge of this importance increasing, though, we're still seeing more cases of cybersquatting. Around 3,500 are filed yearly with World

Intellectual Property Organization (WIPO) alone.[xxxi] In the 2000 case of Morrison & Foerster LLP v. Wick[xxxii], the aggrieved defendant, in a bid to "get even with corporate America"[xxxiii] registered several variations of the name Morrison & Foerster. He then posted disparaging comments targeted at the plaintiff on the domain names. The court held that the defendant's act "strongly suggested bad faith." The court in Toronto Dominion Bank v. Kapachev[xxxiv] found the defendant liable under the fifth and eight factors of the ACPA for opening 16 misspelled domain names and describing the plaintiff as Nazi and Soviet communists. Also, the defendant intent on diverting the bank's customers made him liable.

In the case of Audi AG v. D'Amato[xxxv], a cyber-squatter was sued in a federal district court for registering www.audisport.com, thereby, violating the ACPA. The court recognized the fact that the defendant was not keen on compelling Audi to purchase the domain name from him. However, he was found liable for intending to make profit off Audi's mark. Hence the element of bad faith was established. In the case of Academy of Motion Picture Arts and Sciences v. GoDaddy.com[xxxvi] Inc. a domain marketer bought several URLs with the Oscar trademarks incorporated in them. During the Oscar season, he made a substantial amount of profit from the advertisements placed on the sites. The plaintiff, being the organizers of the Oscar awards then sued the defendant who benefitted from the cyber squatter's act through its paid parking programme.[xxxvii]

The 2008 case of Verizon California Inc. v. Onlinenic Inc.[xxxviii] is one of the landmark cases on cybersquatting. The chief reason for this is the highest award of damages in the history of cybersquatting was made in the case. In June, 2008, the plaintiff who owns multiple trade names and trademarks filed its case against the defendant for violations of the provisions of the *ACPA*[xxxix]. The purpose of this was to attract internet users who sought to visit Verizon's legitimate websites[xl]. The defendant equally failed to desist from such act, thereby establishing bad faith intent. This was further evident in the manner in which it used fictitious business names in order to prevent detection. The federal court in a default judgment in the Northern District of California consequently awarded the sum of $33.15 million. The award was calculated based on $50,000 per each of the 663 domain names.[xli] Default judgment was entered as the defendant failed to show up at the proceedings initiated against him.

In the matter involving the Nigerian Air and Olumayowa Elegbede,[xlii] upon the launching of the National Carrier/Airline for Nigeria by the Federal Government on 18th July 2018, one Olumayowa Elegbede quickly purchased the domain names; NigeriaAir.ng and NigeriaAir.com.ng on the same day and subsequently put them up for sale. Although no legal action was taken against Olumayowa Elegbede, his action amounts to an obvious case of cyber-squatting as defined under section 58 of the Cybercrimes Act. Similarly, in the matter involving Linda Ikeji and Emmanuel Efremov, the latter, the owner of a media outfit called 9jalife, registered the domain name lindaikeji.net. Linda Ikeji is a popular Nigerian blogger who owns and runs a blog named after her (www.lindaikejisblog.com) and averages an estimated $900,000.00 in income each year. Emmanuel was using her name and prestige to earn himself advertisement revenue. Upon revelation of this fact, Emmanuel redirected the site to Linda's blog in an attempt to erase evidence of the cyber-squatting activities. There is no record of any action brought against him by Linda Ikeji. The fact that no action was brough against the possible defendants in these two scenarios goes to reaffirm the fact that Nigerians are not usually litigious.

In Microsoft v. Mikerowesoft, when Rowe demanded $10,000 for the domain, Microsoft sent a cease-and-desist letter accusing him of cybersquatting. After massive public backlash against the company, a settlement was reached outside of court. In Peta v. Doughney,[xliii] the People for the Ethical Treatment of Animals (PETA) has existed since 1980. In 1995, Michael Doughney registered the domain peta.org and titled it "People Eating Tasty Animals." PETA attempted to get Doughney to transfer the domain name willingly, and when he refused to do so, they sued him for trademark infringement, cybersquatting and dilution. The website's content proved without a doubt that it was a parody page, but the court ruled that this was not conveyed in the domain name itself. Doughney also was not facing accusations of cybersquatting until he made statements implying that PETA should pay him money to transfer the domain. Doughney had to surrender the domain, but due to a lack of malicious intent, he was not ordered to pay damages.

CYBERSQUATTING AND INTELLECTUAL PROPERTY LAW

Intellectual property (IP) refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce. Intellectual property is divided into two categories: Industrial Property includes patents for inventions, trademarks, industrial designs and geographical indications. Copyright covers literary works (such as novels, poems and plays), films, music, artistic works (e.g., drawings, paintings, photographs and sculptures) and architectural design. Rights related to copyright include those of performing artists in their performances, producers of phonograms in their recordings, and broadcasters in their radio and television programs.[xliv] Intellectual property law deals with the rules for securing and enforcing legal rights to inventions, designs, and artistic works. Just as the law protects ownership of personal property and real estate, so too does it protect the exclusive control of intangible assets. The purpose of these laws is to give an incentive for people to develop creative works that benefit society, by ensuring they can profit from their works without fear of misappropriation by others.[xlv]

One of the rights that is mostly affected in times of cybersquatting is the intellectual property right of the domain name owner. Intellectual property rights are the rights given to persons over the creations of their minds. They usually give the creator an exclusive right over the use of his/her creation for a certain period of time.[xlvi] When a person registers a domain, that person retains the rights to that domain until he/she sells it or lets the registration expire. Therefore, cybersquatters can severely damage the brand of a trademark owner, simply by preventing them from using the domain name corresponding to their brand. However, this damage can go far beyond just preventing trademark owners from using the domain for their own business endeavors. In some cases, it involves redirecting visitors to obscene web pages, phishing sites, and even competitor's sites. This can tarnish the reputation of the brand quite badly. A cybersquatting claim is related to trademark infringement and trademark dilution but it is a separate legal claim with its own requirements. Cybersquatting has once been defined as when a person other than the owner of a well-known trademark registers that trademark as an Internet domain name and then attempts to profit from it either by ransoming the domain name back to the trademark owner or by using the domain name to divert business from the trademark owner to the owner of the domain name.[xlvii]

No doubt, the act of cybersquatting is a violation of the intellectual property rights of a person which are protected by the laws. However, the approach to adopt in redressing this wrong depends on the jurisdiction in which the parties are. For example, in Nigeria, cybersquatting is a crime punishable with a term of imprisonment or fine or both. In the United States on the other hand, this violation may be redressed either in civil or criminal law. If the domain name is registered, the redress is usually criminal while is usually civil when the domain name is not registered. In England however, the approach is basically civil as there is no law expressly criminalising cybersquatting in the whole of United Kingdom.

CIVIL LAW I.E. PASSING OFF AS AN ALTERNATIVE REMEDY TO CYBERSQUATTING IN CRIMINAL LAW

Prior to 1999, the Federal Trademark Dilution Act (FTDA) was the main avenue for responding to cybersquatting. This changed after the passage of the Anti-Cybersquatting Consumer Protection Act (ACPA). The statute created a cause of action against cyber squatters that allows trademark owners to gain ownership of a domain and potentially receive monetary damages.

Often these types of cases are handled through the Internet Corporation for Assigned Names and Numbers (ICANN). To sue under the ACPA, plaintiffs must prove the following:

i. The alleged cyber squatter intended to profit from bad faith registration.
ii. Defendant registered, used or trafficked in a domain name that is either…
iii. Confusingly similar or identical to an existing distinctive identifier.
iv. Confusingly similar, identical or dilutive of a famous identifier.
v. The trademark belongs to specific organizations mentioned under U.S. Codes 18 and 36.

If these issues are proven in federal court, plaintiffs may receive injunctive relief, attorney's fees and damages that range from $1,000 to $100,000 per domain name. Website owners have many of the same defenses granted to other accused infringers. If someone registered the domain KodakComplaints.com and shared negative reviews of KODAK® products, for instance, they would meet both of the first two prongs. Since their intent is to critique rather

than profit, though, they are not likely to be considered guilty of cybersquatting. If the infringing behavior does not cease after this point, filing trademark litigation under the Anti-Cybersquatting Consumer Protection Act may be appropriate. Doing so will often result in the cyber squatter looking to immediately settle the case or refusing to fight back in court at all which would lead to a default judgment.

Up until 2015, an aggrieved complainant in Nigeria could only resort to the NIRA Dispute Resolution Policy Rules. Another alternative was the UDRP Rules of ICANN. A complainant equally had the option of initiating the tort of passing off against the cyber squatter. The basis of this tort is that "one man has no right to put off his goods as the goods of a rival trader."[xlviii] However, to succeed in bringing this, the claimant needs to show that[xlix]

i. he or she has a goodwill and reputation in the domain name;
ii. and that the third party made false representations which are likely to lead, or have led the public to be confused that his goods and series are those of the owner of the unregistered mark; or
iii. that his goods or services are associated with or somehow connected to the business of the owner of the unregistered mark; and
iv. that damage resulted from such misrepresentations.

Alternatively, a victim of cybersquatting could bring a civil action of passing off against the perpetrator. Passing off is described as an unfair competition by misrepresentation or literally speaking "the cause of confusion or deception". Generally, an action for Passing off arises where the deception is made in the course of trade, which could lead to confusion amongst customers. This applies to both ecommerce businesses and businesses with physical addresses. Another definition of Passing off is the act or an instance of falsely representing one's own product as that of another in an attempt to deceive potential buyers.[l] It is necessary to state that Passing off and trademarks infringement goes hand in hand and is very similar in nature. Whilst, passing off is an action on unregistered marks that have become notoriously attributable to a person or company, a trademark infringement action usually involves a registered mark. This means that a mark, brand, design, name must be registered as a trade mark before one can make a claim on trade mark infringement. An action for Passing off is a common law remedy

and the claimant need not establish title for same but must show that the goods/services have distinctive features. It is arguable to state that Passing off is both a common law and statutory remedy in Nigeria as it is statutorily supported by Section 3 of the Trademarks Act[li] which provides that no person shall be entitled to institute any proceeding to prevent, or to recover damages for, the infringement of an unregistered trade mark; but nothing in this Act shall be taken to affect rights of action against any person for Passing off goods as the goods of another person or the remedies in respect thereof.

In the case of Trebor Nigeria Limited v. Associated Industries Limited,[lii] Trebor Nigeria Limited the makers of Trebor Peppermint brought an action against Associated Industries Limited the makers of Minta Supermint claiming that the wrapper used to package the product by the Defendant was similar to that of the Plaintiff and that they were guilty of Passing off their products like that of the Defendant. The Defendants raised dissimilarities in the two products as a defence to the action, the Judge however found the Defendants liable for Passing off their products as that of the Plaintiff. In this instance Passing off occurred by the use of a package strongly similar with that of another product such as to deceive the public that they are one and the same. In the case of Niger Chemists Limited and Nigeria Chemists,[liii] the Plaintiff had an established chemist business using the name "Niger Chemist" while the Defendants established the same business on the same street with the Plaintiff using the name "Nigeria Chemist". The Plaintiff sued the Defendant claiming the name was too similar and likely to deceive the public that there was a relationship between them. The Court agreed with the Plaintiff and granted an injunction against the Defendant on the use of the name. In this instance passing off occurred by the use of a trade name similar with that of another such as to deceive the public that there exists a business relationship between the two.

CONCLUSION AND RECOMMENDATION

With all the threats that have occurred lately, it is clear that cybercrime touch almost everyone. We can hardly go a week without the mainstream media reporting another major incident or breach. It has become commonplace to hear that millions of private records have been disclosed or a major ransomware attack has occurred as Cybercriminals continue to use malware to wreak

havoc. Envisioning the present conditions existing around the world, cybersquatting is considered to be a menace with no frontiers. Cybersquatters have robbed businesses of their fortune. Cybersquatting is acting as an eye-opener to the government in all countries and requires serious attention. Countries need to protect the spreading of this virus. The active involvement of WIPO in resolving disputes regarding domain names has played a vital role in evolving concrete principles in this field. It provides a streamlined, cost-effective and swift procedure to review the claims before it. Also, the prevention of cybersquatting revolves mainly around two acts, the UDRP and the ACPA.

In England, there is no single criminal law statute on cybersquatting. This may be due to the fact that most of the infringements on intellectual property are redressed by civil actions including passing off and breach of contract. This paper nevertheless recommends an enactment of a comprehensive statute on cybersquatting in the jurisdiction.

Cybercrime has taken a new dimension in Nigeria. One of the justifications for the enactment of the CPPA is that traditional criminal law statutes were not enough to secure conviction for the charge of cybercriminality. Despite the robust legislation, there is a very little report of convictions secured under the Act. This is to a large extent due to the poor implementations of the law. Most of the lawyers employed as public prosecutors are not skilled in the area of technology law. This may result in them not being familiar with computer crimes. This research thereby recommends the establishment of an agency which will be saddled with the responsibility of implementing the Act.

In Nigeria, there is a need to have Judges and Law Enforcement Officers that are technically and technologically sound in understanding cybercrime and its terminologies, appropriately interpreting the law on cybercrimes and keeping up with the trends of cyber environment. Further, it is desirable to have local and international collaboration between private, governmental and civil society in intelligence and data sharing and other international treaties on cyber security. Also, in Nigeria, there should be provision of training and technical assistance in building cyber security skills within the Law Enforcement Agencies to get better understanding of activities of cyber criminals and hands-on with equipment and technologies

that are likely to be found at cybercrime scenes. There should be continuous public awareness on preventive measures against cybercrime.

ENDNOTES

[i] Anti-Cybersquatting Consumer Protection Act 15 U.S.C. 1125(d).
[ii] Sporty's Farm L.L.C. v. Sportsman's Market, Inc., 202 F.3d 489, 493 (2nd Cir. 2000) (citing H.R. Rep. No. 106-412, at 5-7 (1999); S. Rep. No. 106-140, at 4-7 (1999)); Sallen, 273 F.3d at 19.
[iii] Internet Cybersquatting: Definitions and Remedies, available at https://smallbusiness.findlaw.com/business-operations/internet-cybersquatting-definition-and-remedies.html, accessed September 25, 2020.
[iv] Olufunmilayo Mayowa, Cybersquatting And Protection Of Domain Names In Nigeria, available at https://www.mondaq.com/nigeria/trademark/877252/cybersquatting-and-protection-of-domain-names-in-nigeria#:~:text=Cybersquatting%2C%20also%20known%20as%20domain,reselling%20them%20at%20a%20profit, accessed September 25, 2020.
[v] Second Pocket Edition 1996 West Group.
[vi] Cybercrimes (Prohibition, Prevention, ETC) Act 2015, s. 26.
[vii] Internet Cybersquatting, supra note 3.
[viii] Carl C. Butzer & Jason P. Reinsch "Cybersquatting, Typosquatting, and Domaining: Ten Years Under the Anti-Cybersquatting Consumer Protection Act" cited in Adesina-Babalogbon O.A, A Comparative Analysis of Nigeria's Legal Framework on Cybersquatting and America's Anti Cybersquatting Consumer Protection Act (2018) (4) (1) Afe Babalola University Journal of Public and International Law, pp169-186.
[ix] Olufunmilayo Mayowa, supra note 4.
[x] Cybersquatting Examples, available at https://www.mandourlaw.com/cybersquatting/, accessed September 28, 2020.
[xi] World Intellectual Property Organization, Introduction to Trademark Law and Practice, A WIPO Training Manual (Second Edition, Geneva, 1993) 28.
[xii] Cybercrime Act, s.25.
[xiii] Section 25(3)
[xiv] Oluwafunmilayo, Mayowa, Cybersquatting and Protection of Domain Names In Nigeria, available at http://www.spaajibade.com/resources/cybersquatting-and-protection-of-domain-names-in-nigeria-oluwafunmilayo-mayowa/, accessed October 1, 2020.
[xv] U.S.C.§ 1125 (d).
[xvi] Carl C. Butzer & Jason P. Reinsch "Cybersquatting, Typosquatting, and Domaining: Ten Years under the Anti-Cybersquatting Consumer Protection Act" [2009] p.3 <npm.icapps.com>, accessed October 1, 2020.
[xvii] Kenneth B. Germain, TRADEMARKS AND UNFAIR COMPETITION by J. Thomas McCarthy. Rochester, New York: Lawyers Co-Operative Publishing Co., (2d ed. 1984). Pp. 2269, including Index, Table of Cases, Table
of Statutory Citations, Table of Figures, Table of Forms, and Appendices., 34 Cath. U. L. Rev. 595 (1985). Available at: https://scholarship.law.edu/lawreview/vol34/iss2/12
[xviii] Butzer and J. P. Reisch supra note 16 at p.4.
[xix] *Ibid*.
[xx] 15 U.S.C § 1125(d); H.R. No. 106-412 at 9; Lucas Nursery and Landscaping v Grosse, 359 F.3d 806, 810 (6th Cir 2004) (quoted S. Rep No.106-140 (1999) at 5-6).
[xxi] *Ibid*.
[xxii] 15 U.S.C. § 1125(d)(2)(A).
[xxiii] Virtual Works, Inc. v. Volkswagen of Am., Inc., 238 F.3d 264, 269 (4th Cir. 2001).
[xxiv] 15 U.S.C. § 1125(d)(1)(B)(i).
[xxv] Coca-Cola Co., 382 F.3d at 785.
[xxvi] Southern Grouts & Mortars, Inc.,575 F.3d at 1246.

[xxvii] 15 U.S.C.§ 1117(d); see also Kiva Kitchen & Bath, Inc. v. Capital Distrib., Inc., 319 Fed. Appx. 316, 320 (5th Cir. 2009).
[xxviii] Barcelona.com, Inc. v. Excelentisimo Ayuntamiento De Barcelona, 330 F.3d 617, 626 (4th Cir. 2003).
[xxix] Southern Co. 324 Fed Appx 316.
[xxx] Adesina-Babalogbon O.A, A Comparative Analysis of Nigeria's Legal Framework on Cybersquatting and America's Anti Cybersquatting Consumer Protection Act (2018) (4) (1) Afe Babalola University Journal of Public and International Law, pp169-186.
[xxxi] Cybersquatting, available at https://www.mandourlaw.com/cybersquatting/, accessed September 30, 2020.
[xxxii] 94 F. Supp.2d 1125.
[xxxiii] J. Ryan Giloil, 'A judicial Safe Harbor under the Anti-Cybersquatting Consumer Protection Act', (2005) (20) (1) Berkeley Technology Law Journal, p.190.
[xxxiv] 188 F. Supp 2d 110(D. Mass 2002).
[xxxv] 381 F. Supp. 2d 644 (2005).
[xxxvi] No.CV 10-0378 AB (CWx)2015 WL 5311085.
[xxxvii] Cybersquatting case study: Academy of Motion Pictures Arts and Science v. GoDaddy.com Inc. Published on the 20th of May, 2015 <kellywarnerlaw.com> accessed October 12, 2020.
[xxxviii] No C 08-2832 JF (RS), 2009 WL 2706393 (N. D. Cal. 25, 2009)
[xxxix] Rowe v. Reconstrust Company, N.A. (5:09-cv-04844), available at <https://wwwcourtlistener.com> Accessed on October 12, 2020.
[xl] *Ibid*.
[xli] Nick Brown <https://law360.com > Accessed October 12, 2020.
[xlii] Toba Obaniyi, "Nigeria Air Domain Registration Saga. Who Wins?" available at: https://blog.whogohost.com/nigeria-air-domain-name-saga/ accessed October 12, 2020.
[xliii] 113 F.Supp.2d 915 (E.D. Va. 2000).
[xliv] World Intellectual Property Organization, 'What is Intellectual Property?' Available at https://www.wipo.int/edocs/pubdocs/en/intproperty/450/wipo_pub_450.pdf, accessed October 4, 2020.
[xlv] H.org Legal Resources, 'What is Intellectual Property law?' available at https://www.hg.org/intell.html, accessed October 4, 2020.
[xlvi] World Trade Organization, 'What are Intellectual Property Rights?' available at https://www.wto.org/english/tratop_e/trips_e/intel1_e.htm#:~:text=Intellectual%20property%20rights%20are%20the,a%20certain%20period%20of%20time, accessed October 4, 2020.
[xlvii] Cornell Law School, Cybersquatting, available at https://www.law.cornell.edu/wex/cybersquatting, accessed October 4, 2020; see also DaimlerChrysler v. The Net Inc., 388 F.3d 201 (6th Cir. 2004).
[xlviii] Trebor (Nigeria) Ltd. V. Associated Industries Ltd. [1972] N.N.L.R. 60 at p.63. Cited in Kodinliye Gilbert and Aluko Oluwole 1999 Ibadan Spectrum Books Limited
[xlix] Cybersquatting in Nigeria" < www.lawpadi.com> Accessed October 9, 2020.
[l] T&A Legal, An Appraisal of Passing Off Actions Under Nigerian Law, available at https://www.mondaq.com/nigeria/trademark/704160/an-appraisal-of-passing-off-actions-under-nigerian-law, accessed October 9, 2020.
[li] Cap T13 Laws of the Federation of Nigeria, 2004.
[lii] (1972) NNLR 60.
[liii] (1961) ANLR 180.