SIAR-Global Journal of Social Sciences & Legal Review (GJSSLR)
www.siarpublications.org
info@siarpublications.org
Vol. 1 Issue 1 Sept.-Oct. 2025

The Cybercrime Act and Intellectual Property Rights: An Interrogation

Kelvin Bribena PhD

Faculty of Law, Niger Delta University,
Wilberforce Island, Bayelsa State, Nigeria.

Abstract

The paper interrogated the corelates between the Cybercrimes Act 2015 and intellectual property rights in Nigeria. No doubt, the introduction of the anti-cybercrime legislation marked a watershed in the efforts geared towards the promotion of national cyber security policy and strategy in response to increased threat of the phenomenon of cybercrime to national security and economy in Nigeria. As a developing country, the development of policy, technical and legal measures for the promotion and protection of the critical national information infrastructure presents a strong imperative to address the persistent 'digital dilemma' that has plagued developing countries in addressing the challenges of the cyberspace and the development of new digital economy. The Cybercrime Act is the first cybercrime legislation in the country following protracted public debate on the high incidence and negative impact of cybercrime on the economic, socio-cultural and political activities in the country. The black letter research method as in doctrinal style was employed which focused on the analysis of legal rules and principles within primary sources like statutes, case law, and regulations as well as secondary sources like books, journal articles, and online data banks. As such, this paper examined the Intellectual Property Rights (IPR) infringement from the prism of cybercrime and the Cybercrimes Act 2015. In doing so, it considered the definitional and structural approaches involved in the main instruments, which provided major frameworks and strategies for promoting and ensuring cyber security in the global information superhighway. The paper underscored the technological roots and the associated digital connection that has shaped the contours of cybercrime phenomenon and what it has developed into and affirmed the far-reaching implication on the protection of IPRs indicating the connection between cybercrime and IPR crimes in the form of digital piracy and other forms of IPR infringement.

Keywords: Cybercrime, intellectual property rights, infringement, information communication technology, interrogation.

Introduction

A fundamental legal mechanism in mitigating the negative effects in the last half a century of global information revolution has been the development of specially designed cybercrime laws and policy frameworks at both national and international levels. As far back as the 1990s, global efforts have focused on cybercrime framework and have spurred both national and regional initiatives. With the Cybercrime (Prohibition, Prevention etc.) Act 2015 (Cybercrime Act), Nigeria has joined the global community with effective national cybercrime legislation as part of the policy instruments for national regulation of emergent global information system.

The Cybercrime Act is the pre-eminent legislation establishing the legal and institutional regime governing cybercrime in Nigeria. According to the Global Centre for Information and Communication Technologies in Parliament, only five African countries have enacted cybercrime laws.[1] The Act is the first cybercrime legislation in the country following protracted public debate on the high incidence and negative impact of cybercrime on the economic, socio-cultural and political activities in the country. The ambit of the Act has far reaching implication on existing legal and social norms that more recent discourses have continued to examine its ramifications, particularly on the new normative order the Act seeks to establish both in the realm of private and public law. As much as its primary objective established a legal framework for cybercrime properly so called, its effect has serious concern in the area of IPRs.

In large measure, the Act has not only reinforced the discussion of intellectual property rights in the light of the phenomenon of cybercrime but has also introduced, in the ensuing discussion of the relationship between Cybercrime Act and IPRs, an important context for the examination of the emerging legal framework for the protection of IPRs in the digital ecosystem. In that context, two perspectives present the rationale and significance of that relationship. Firstly, the Act brought about an effective legal regulation in Nigeria of information and communication technology (ICT) system, a development that will shape the contours of the three key legal norms in the interaction between ICT and law, namely, privacy, security of data and IPRs. This incipient legal regime covers the major doctrinal areas of cyber law and regulation as they affect both private and public law domains comprising criminal law, privacy, human rights, Internet governance, among others.

Secondly, and with particular reference to IPRs, the Act as an anti-cybercrime legislation and overall regime of promoting cyber security seeks to 'cover the field' including protecting proprietary content which implicates IPR within the networked environment. The legal and commercial dimensions of the impact of the emergent online ecosystem remain one of the most intractable challenges facing the exploitation of IPRs in the information age. In its positive context, ICT and the Internet, with the opportunities it offers, has brought about remarkable changes in cultural and socio-economic development. On the negative side,

[1]These countries include Cameroon's Cybersécurité et la Cybercriminalité au Cameroun (2010), Kenya's Communications (Amendment) Act (2009), Mauritius' Computer Misuse and Cybercrime Act (2003), South Africa's Electronic Communications and Transactions Act (2002), and Zambia's Computer Misuse and Crimes Act (2004).

it has facilitated, in various degrees, rapid and sustained violation of IPRs as well as the norms of privacy and security of information and protection of data that has been captured in the phenomenon of cybercrime.

This work examines the phenomenon of cybercrime and IPRs and the doctrinal basis of the interaction between the two concepts; discusses the technological root of the relationship between IPR and cybercrime; presents an overview of the Cybercrime Act 2015 as the primary legal framework for the regulation of online environment; highlights the basic objectives of the Act and its essential features in promoting cyber security and protecting national information infrastructure and at the same time IPR. In the context of IPR, the chapter examines the Act as the framework for examining the protection of IPR, as one of the most valuable content or features of that environment, and examines whether the Act provides a regime for the protection and enforcement of IPR, particularly as regards digital and online piracy and criminal infringement of IPRs.

The research also suggests that, although, it is not within the remit of the Cybercrime Act, primarily as a cybercrime legislation, to operate as an intellectual property (IP)legislation, it has provided effective and alternative legal mechanism for more serious cases of online criminal IPR infringements, particularly for the protection of valuable proprietary contents such as movies, music and software, thereby providing the much needed instrument for the protection for emerging entertainment and software industries in Nigeria. On a pragmatic and final note, this chapter subscribes to the notion of understanding the complementary role of the new Cybercrime Act to the existing IPR laws, which are not only inadequate but are largely unsuited for the digital environment and in addressing the increasing rate of digital piracy, thereby reinforcing the protection and enforcement of IPRs in the emerging digital economy in Nigeria.

The Concept of Cybercrime

The phenomenon of cybercrime provides one of the justifications for the regulation of technological innovation in its rapid development and impact on human behavior. Advances in ICT, which has produced the Internet as one of the most revolutionary technological system of the 20th Century, have created a new global order and information society. The impact of ICT with its constituent information infrastructure has laid the foundation for the development and use of technology-based services and applications that has grown exponentially with far reaching national and global implications.[2] It provides the foundation for emerging legal and social norms in which to address issues of cyber security and for protecting critical information infrastructure for national security and economic development.

Significantly, anti-cybercrime measures form part of the system for measuring, maintaining and ensuring optimal level of cyber security as the critical objective of national ICT framework and policies. Largely undefined, 'Cybercrime' and 'Cyber security' providing context one for the other, are the two main concepts in the development of national ICT regulation and policies. According to the International Telecommunications Union (ITU), cyber-security is [T]he collection of tools, policies, security concepts,

[2]The ICT systems cover email, various online and web services such as social networking, cloud computing and ICT applications such as e-government, e-commerce, e education, e health and e environment all of which have become important in today's discussion on development.

security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber-environment and organization and user's assets.[3]

The new and increasingly common typology of offences in the neo-liberal technological age is cybercrime. The phenomenon has arisen from clearly defined activities, which threaten the security and privacy of persons and computer systems. First coined in 1982 by science fiction writer William Gibson and subsequently applied in the context of the Internet by Howard Rheingold, cybercrime has evolved as a term of art to describe a variety of offensive or criminalized activities against persons and computer systems and networks and has become associated with the Internet or cyberspace.[4] The term has been broadly used in relation to the world of electronic communications in the commission of illegal activities, which is not limited to the use or misuse of computer but also in the Internet situation as its principal means of commission.[5]

There are at least three perspectives in the structure and function of evolving cybercrime legislation, as the primary tool in promoting the broader objectives as well as an important law and policy framework for cyber security. Firstly, in the last 30 years of evolution of information technology, the development of legal responses to the criminal type of abuses of information technology recognized in the distinction between 'computer crime' and 'cybercrime' properly so called have continued to widen the scope of cybercrime beyond the original context of computer crime.[6] Today, the main structure of legislative framework ranges from providing for criminalization and offences, procedural and enforcement measures, jurisdiction, international co-operation and Internet service provider responsibility and liability. For example, in terms of substantive criminalization, several acts have been commonly recognized as the core of cybercrime with their respective enforcement and procedural measures. These include illegal access to a computer system; and to computer data; illegal data interference or system interference; breach of privacy or data protection measures; computer-related fraud or forgery; computer-related identity offences; computer-related copyright and trademark offences; computer-related acts causing personal harm, or involving racism or xenophobia; computer-related production, distribution or possession of child pornography or solicitation or 'grooming' of children; and computer-related acts in support of terrorism offences. While the definition of cybercrime has remained largely fluid and imprecise, a limited number of acts against the confidentiality, integrity and availability of computer data or systems represent the core of cybercrime with the list or

[3]The definition goes further 'Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunication systems, and the totality of transmitted and/or stored information in the cyber-environment. Cyber-security strives to ensure the attainment and maintenance of the security properties of the organization. And user's assets against relevant security risks in the cyber-environment. The general security objectives comprise the following: Availability; Integrity, which may include authenticity and non-repudiation; Confidentiality' See ITU-T Recommendation X.1205.

[4]See Stephanie Perinn, Cybercrime, available at vecam.org/archives, article 5658.html accessed on 11 January 2023. According to the Oxford English Dictionary (OCD), cyberspace is defined as 'the space of virtual reality, the national environment within which electronic communication (especially via the Internet) occurs'.

[5]See http/blog.oxforddictionaries.com/2015/03/cyborgs-cyberspace-csi-cyber/Accessed 16 February 2023.

[6]For definition and classification of cybercrime, see Cybercrime, Definition and General Information, Australian Institute for Criminology, available at: www.aic.gov.au/topics/cybercrime/definitions.htm; Gordon/Ford, On the Definition and Classification of Cybercrime, Journal of Computer Virology, Vol. 2, No 1, 2006, 13-20; Goodman/Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, International Journal of Law and Information Technology, 2002, Vol 10, No 2, 144.

categories having grown exponentially with the rapid developments and applications of ICT and the Internet.[7]

The second perspective entails the recognition of the inadequacy of conventional and substantive criminal law provisions in addressing digital and online activities ranging from computer fraud, illegal access, data interference, child pornography to copyright violations. With cybercrime as a term of art, which covers a wide variety of culpable conduct, constituting offences in the typical cybercrime legislation, it is difficult to develop a typology or classification system for cybercrime. [8]Evidently, cybercrime has extended the frontiers of classical criminal law as it has come to apply to new types of criminality relating to offences both under statute and common law.

Thirdly, cybercrime framework requires the recognition and provision of necessary tools and instruments to investigate and enforce cybercrime, which are vastly different from those for ordinary crimes. As the critical component of developing adequate cyber security strategy, it is therefore important that effective cybercrime legislation should develop and fit definition and framework into the appropriate context. Some definitions are more precise than others by taking the objectives or intentions into consideration. For example, cybercrime has been defined as "computer-mediated activities which are either illegal or consider illicit by certain parties and which can be conducted through global electronic network."[9] It is evident that the global reach of the information infrastructure and services, which has inexorably powered cybercrime phenomenon have enlarged existing perspectives and conceptualization of the phenomenon.

Notwithstanding the imprecision and diversity of definitions, the common denominator describes cybercrime as any activity or typologies of criminal conduct in which a computer or network are a tool, a target or place of criminal activity.[10] In the international context, at least five different initiatives or clusters are identifiable.[11] For example, one of them, the UN Congress on the Prevention of Crime and Treatment of Offenders provides two definitional frameworks.[12] Firstly, cybercrime is defined in the narrower sense of computer crime, which 'covers any illegal behavior directed by means of electronic operations that target

[7]See Comprehensive Study on Cybercrime, Draft February, 2013, United Nations Office for Drugs and Crime (UNODC), Vienna, United Nations, New York, 2013, 19.

[8]See Understanding Cybercrime, phenomena, challenge and legal response, Telecommunications Development Sector, ITU, September 2012, 11. See Gordon/Ford, on the definition and classification of cybercrime, journal in computer virology, Vol 2, No. 1, 2006, 13-20).

[9]See Hale, Cybercrime, facts and figures concerning this Global Dilemma, (CJ/2002, vol 18, available at www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37 accessed 16 March 2023. See also Hayden, cybercrimes impact on information security, cybercrime and security, 1A-3, p 3.

[10]See the ITU-led Global Cyber security Agenda (GCA) launched at the World Summit on the Information Society (WSIS), referred to as the Tunis Agenda for the Information Society or the Geneva Plan of Action within the framework of International Co-operation in 2007 defined the 'global framework for dialogue and international cooperation to co-ordinate the international response to the growing challenges to cyber security and to enhance confidence and security in the information society." See Art. 108-110 and Annex, WSIS Tunis Agenda for the Information Society. GCA seeks to achieve its strategic goals within five critical work areas, namely, legal measures, technical and procedural measures, organizational structures, capacity building and international co-operation. See also Understanding Cybercrime (n 4) 3.

[11]This covers the following main international instruments, namely (i) the Council of Europe or the European Union, (ii) the Commonwealth of Independent States or the Shanghai Cooperation Organization, (iii) intergovernmental African organizations, (iv) the League of Arab States, and (v) the United Nations.

[12]Crimes related to computer networks, Background paper for the workshop on crimes related to the computer network, 10th UN Congress on the Prevention of crime and the Treatment of Offenders, 2000, A/CONF.187/10,p 5; www.uncjin.org/Documents/congr10/10e.pdf.

the security of computer systems and the data processed by them.'[13] Secondly, in a broader sense of computer-related crimes which covers 'any illegal behavior committed by means of, or in relation to a, computer system or network.'[14] Clearly, internet technology has emerged as the key facilitator for the vast and different forms of criminal conducts.[15]

In a more comprehensive context, the Convention on Cybercrime passed by the Council of Europe in November 2001, following the events of 911, constructs five subject areas in the legal framework for cybercrime. This includes:

i. Offences against the confidentiality, integrity and availability of computer data and systems;
ii. Computer-related offences [forgery and fraud];
iii. Content related offences [pornography];
iv. Offences related to infringements of copyright and related rights; and
v. Ancillary liability and sanctions 'aiding and abetting, corporate liability'[16]

The approach of the Treaty provides a convenient definitional framework or models by distinguishing or classifying four different types or categories of offences, which offer the basis for a better appreciation of the typology and phenomenon of cybercrime under those categories. While the first three categories focus on the object of legal protection, the fourth 'computer- related offences' focuses on the method used to commit the crime. Though some of the criminal acts may overlap into more than one categories, the framework reduces the technical and legal challenges which may involve in the evolution and analysis of the various types of conduct that have become known under the umbrella term cybercrime.

For example, the offences in the first categories relate to any one or more of the three legal principles of confidentiality, integrity and availability in the digital media not covered under the traditional law of crime and tort. This includes (illegal access) hacking, cracking, which refers to unlawful access to a computer system, one of the oldest computer-related crimes including act of circumventing password protection on a computer system.[17] This category also includes illegal interception, data interference, system interference, illegal data acquisition (data espionage)[18] and other related activities, which threatens privacy and security of the system and persons.

[13]See also Kumar, Cyber Law, A View to Social Security, 2009, 29.

[14]See Artilel, Stanford draft International Convention to Enhance Protection from Cybercrime and Terrorism 1999, (the 'Stanford Draft') in creating cybercrime as an offence punishable under the Convention defines it to simply 'mean conduct with respect to cyber system.

[15]See Europol, EU Internet Organised Threat Assessment: iOCTA 2011, File No 2530-274, April 28, 2011, p.6 cited in K Finklea and C A Theohary, Cybercrime: Conceptual Issues for Congress and US Law Enforcement, Congressional Research Service, January 15, 2015, CRS Report, 1 www.crs.gov. accessed 16 February 2023

[16]See http://conventions.coe.int/treaty/e.... One of the objectives of the treaty was to establish a well-coordinated system to combat the new criminal frontiers, hence its comprehensive framework of procedural and international co-operation.

[17]Example of hacking includes breaking the password of password-protected websites, circumventing password protection on a computer system, among other hacking activities, which may also include setting up 'spoofing' websites to make users disclose their passwords.

[18]This includes phishing' which describes attempts to fraudulently acquire sensitive information by masquerading as credible person or business i.e. financial institution,

The second category, which is 'content-related offences,' covers 'content' which are considered offensive or illegal such as child pornography, spam and related threats hate speech, xenophobic, false or defamatory materials, depending on national, cultural and legal approaches or principles relating to fundamental rights. This category of cybercrime has raised robust debate on the tension between Internet and freedom of expression. The third category of 'computer-related offences' covers fraud and computer-related fraud such as online auction or payment fraud, advance fee fraud for which Nigeria is notorious, computer-related forgery, identity theft, misuse or abuse of devices, terrorist use of internet (cyber terrorism or cyber warfare, or cyber laundering), attack against critical infrastructures, phishing and other illegal activities that targets the system for obnoxious purposes. The last category relates to copyright and trademark-related offences, which affects content industries such as the entertainment and media enterprises and other IP based industries, which have developed one of the most valuable global markets using ICT and e commerce.

Notwithstanding the stubborn 'digital divide' which beset African continent, both regional[19] and sub-regional[20]frameworks have developed in addressing cybercrime and the menace it poses to the benefits of ensuring cyber security and its developmental functions.[21] These initiatives mirrors the global objective in the promotion and preservation of legal, institutional, technological and informational assets and resources through the treatment of cybercrime and cyber security and other challenges of the digital environment in meeting the socio-economic needs of Africa.[22]

The ambit of cybercrime therefore effectively captures the widest possible category of activities and interaction in relation to the information system, persons and the content (IPR) in the digital network, which has continued to portend huge loss to the economy and national security interest. For example, one of the estimates has placed the annual cost of cybercrime in 24 countries at $113 billion in 2013 alone.[23] In looking at the ambit, it is important to distil the underlining similarities and difference between it and IPR infringement and explain that comparison not only in its legal or regulatory context but also in its socio-

[19]The main regional instrument is the Draft African Union Convention on Cyber security And Personal Data Protection 2000 adopted in 27 June 2014at Malabo Equatorial Guinea. Originally or tentatively titled 'AU Convention on the establishment of A Legal Framework Conducive to Cyber Security in Africa' 2012. Fifteen countries are required to ratify the Convention before it can enter into force. The Convention, among other provisions, criminalizes attacks on computer system, computerized data breaches, content-related offences and offences relating to electronic security measures. It obligates criminalization of the computerized creation and dissemination of 'writings, messages, photographs, drawings or any other presentation of ideas or theories of racist or xenophobic nature' and embraces important elements of electronic transaction, protection of data and private rights.

[20]In addition, cybercrime initiative has been adopted by some four regional economic communities (RECs). The RECs includes East Africa Communities (EAC) Draft Legal Framework for Cyber laws (2008); Economic Community of West African States (ECOWAS) Draft Directive on Fighting Cybercrime 2009; Common Market for Eastern & Southern Africa (COMESA) Cyber Security Draft Model Bill 2011, and Southern African Development Community (SADC) Model Law on Computer Crime and Cybercrime 2012.

[21]See Comprehensive Study on Cybercrime, Draft February 2013, United Nations Office for Drugs and Crime (UNODC), Vienna, United Nations, New York, 2013, 1.

[22]Still left with the prospects of ratification by Africa countries, the AU Convention on Cyber security addresses a wide range of online activities, including electronic commerce, data protection, cyber security and cybercrime. Unlike other African instruments, AU Convention and ECOWAS Directive are binding measures that create legal obligation on member states. See AU, Convention on Cyber Security and Personal Data Protection, 33, https://www.ccdcoe.org/sites/default/files/documents/AU-270614-CSConvention.pdf. Accessed 16 February 2023

[23]See 2013 Norton Report: Cost per Cybercrime Victim Up 50 Percent, Norton, Symantec Corporation, press release, October 1, 2013.

economic dimension on the benefit of technology to the facilitation of both cybercrime and IPR infringement. The considerable inroads of the subject matter and principles of cybercrime in legal texts into IPR should not be viewed strictly as legal or normative deficit but part of the somewhat befuddling visions of striking the ideal relationship between law and technology in the regulation of human conduct.

Intellectual Property (IP) and IP Crime

In broad terms, IP are the legal rights, which result from intellectual activity in the industrial, scientific, literary and artistic fields.[24] The broad categories of IP covers literary, artistic and scientific works, performances of artistes, phonograms and broadcasts, inventions in all field of human endeavors, scientific discoveries, trademark, service marks and commercial names and designations, industrial designs and protection against unfair competition.[25] IP is divided into two broad categories, namely copyright and industrial property. While literary, artistic and scientific works are covered under copyright, industrial property category covers trademark, inventions and industrial designs. Within these subjects, IPR covers a complex and diverse body of rights over creativity and innovation in various fields of human enterprise in the production and distribution of goods, services and associated technologies.

The entire IP fields have evolved into huge global industries that rely on IPR protection for their survival and sustenance. For example, the global markets for entertainment products such as music, movies, video games, software and other valuable goods and services underscore the role and contribution of IPR in both national and global economy. That role have manifested in the huge record of revenue generation, job creation and wealth distribution across industries as a result of adequate protection. On the other hand, abuse and infringement of IPR have not only mitigated the value of IP but have reflected negatively in its strategic and commercial role in the economy.

IPR infringements describe the broad range of violation of various classes of IPR, including infringements of copyright, patent and trademark. IPR infringement have manifested in various forms depending on the subject matter, magnitude or sector of the infringement.[26] IPR infringement, though cuts across all aspects of IP, the criminalization of infringements is only restricted to a limited number of IP subjects. This is essentially in the area of copyright piracy and bootlegging and in the case of trademarks, counterfeiting. Accordingly, a discussion on IP crime will essentially center on these areas. Piracy is the illegal reproduction and/or duplication of copyright works like phonograms, books, paintings, architectural drawings, photographs, films, broadcasts, videos, computer software etc. for commercial purpose. The distribution, exhibition and/or circulation of illegal reproductions also constitute piracy. In the case of music, pirated recording could be a series of sound recordings compiled from various albums that may not have been released together in one legitimate album, cassette or VCD.

[24]WIPO IP Handbook, WIPO, Geneva, 2004, 3.

[25]WIPO IP Handbook (n.19)

[26]See Adebambo Adewopo, Intellectual Property Rights in Nigeria, Law and Development, Nigerian Institute of Advanced Legal Studies, 2015, 151-177 for a detail analysis of enforcement framework of IPR in Nigeria. [Adewopo IPR Law & Development].

Piracy and counterfeiting have been used in describing particular forms of IPR infringement, which terms are more in tune with the concept of cybercrime when applied in its digital context or to the digital environment. While piracy has been used to describe aspects of copyright infringements, counterfeiting has been used with respect to trademarks. Music piracy or software piracy have been associated with particular IP related industries while digital piracy have entered the lexicon of piracy to describe the type of piracy associated with the particular type of unauthorized use of IP works in the online environment. The two forms of IP most frequently involved in cybercrime are copyright works and trade secrets. In the currently digital and online environment far more incidence of music, movie and software piracy occur in the Internet than elsewhere.

The most prevalent forms of IP crimes include but are not limited to the following activities, unauthorized photocopying of printed materials; illegal reproduction of sound recordings and audio visual works; illegal transmission of broadcast signals; bootlegging (unauthorized recording and commercial distribution of performance), software counterfeiting, and end user copying, illegal peer to peer file sharing of music, illegal streaming of entertainment events; unauthorized use of trademarks; counterfeiting of products; manipulation and tampering with right management information in a creative work, illegal distribution of pirated and counterfeit products, importation of pirated or counterfeit products. The most affected IP products include books, sound recording, film and video, artistic works (paintings and crafts), luxury goods, fashion products, household products and consumables and, automobile and other spare parts, pharmaceutical products, building and other goods.

IP related crime would therefore cover a wide range of illegal activities that facilitates other crimes such as investment fraud (using a trademark of a legitimate company to deceive investors); fraudulent sales (creating a bogus website to deceive customers); money laundering (concealing funds acquired from counterfeit goods sales); identity theft (using personal information acquired from misappropriated database); tax evasion (failing to report income acquired through IP violations); trans-border offences (counterfeiting of currency, travel documents and other administrative documents). Part of the legal responses in the regulation of those activities has been through cybercrime law and regulation due principally to their identification and definition within the domain of cybercrime.

The development of these new types of abuses in the digital and online context has not only reflected in the broader sense of cybercrime but also with negative impact on the polity and economy. These developments have led many countries to fashion new ways of controlling and regulating different kinds of cyber related activities and abuses of IPR. The context of the Internet, which will be discussed later, has provided additional platform through online illegal trading in IP works. Consequently, the role of cybercrime law and regulation is no longer new in the protection and regulation of IPR in the digital environment. Indeed, it provides the conceptual and practical rationale for examining in context the relationship between cybercrime and IPR.[27]

[27]See UK Proceeds of Crime Act 2002. See also Australian Cybercrime Act 2001. Nigeria joined with the Cybercrime Act 2015. See also in the US, Racketeer Influenced and Corrupt Organizations (RICO) Statute.

IPR infringement has been broadly classified into two main types, namely, civil and criminal, which types essentially determine the nature or platform of enforcement available for the IPR holder. While civil infringement offers enforcement measures in the nature of civil remedies such as damages, injunction, seizures and similar reliefs and has remained one of the main features of IP system, criminal infringement creates IPR offences by introducing element of mens rea and criminal liability, thereby providing additional enforcement measures for IPR holders. IP theft or IP crime would appear as a narrower term that applies in the realm of criminal infringement of IPR. The criminal dimension, largely spearheaded by global entertainment industries, have been occasioned by the huge loss to piracy and counterfeiting and more recently due to the advent of ICT and Internet that has led to massive digital distribution of unauthorized copies of IP works and the need for strong deterrence.

The global effort against piracy, counterfeiting and other forms of IP violation have contributed immensely in safeguarding the economic role of IP based industries against IPR infringements. To underscore that development, it is significant to note that TRIPS Agreement requires member states to provide criminal penalties in "cases of willful...copyright piracy on a commercial scale."[28] Effective prosecution of IP crime have become an indispensable part of IP enforcement framework and indeed the entire IP system, such that it has required the attention and action of law enforcement agencies worldwide in the area of intelligence, investigation and prosecution.[29] Consequently, criminal infringement has become a standard feature of IPR particularly copyright legislation in many jurisdictions including Nigeria.

The existing Copyright Act makes provision for criminal infringement and liability.[30] Under the Act, the same acts of infringement create an offence enforceable as a criminal action separate from civil action, which actions may be taken simultaneously by copyright holders as well as the Nigerian Copyright Commission, which is vested with the powers to administer criminal enforcement of copyright.[31]

Cybercrime and Intellectual Property Rights: Technological Narrative

The technological narrative of the relationship between cybercrime and IPR affirms the historic and multidimensional interaction between technology and law on the one hand, and technology and IPR on the other hand. While the former has not only impacted the interaction between man and his invention, machine but more significantly the pervasive effect on existing legal norms and creating new ones, with tremendous

[28]Article 61, Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS).

[29]For example In the U.S, the federal IP enforcement agencies include the Federal Bureau of Investigation (FBI) and the national IPR Co-ordination Center, an inter-agency task force led by the US Immigration and Custom enforcement, Homeland Security Investigation (ICE-HSI). It includes also Internet Crime Complaint Center (IC 3), a partnership between the FBI, National White Collar Crime Center and the Bureau of Justice Assistance of DOJ. IC3 is responsible of managing and referring criminal complaints involving cybercrime including online IP crime. Available at http:/www.ic3.gov There are numerous other state and local enforcement agencies such as Infra Gard, Electronic Crime task forces, Computer Hacking and IP (CHIP) Co-coordinators, Computer Crime and IP section (CCIPS), among others. See the following websites
www.ice.gov/contact/inv/;
www.infragard.net;www.secretservice.gov/ectf.shtml;
www.cybercrime.gov.

[30]Sections 20, 21, 22, 24, 25, 30, 33, Copyright Act C18, Laws of the Federation of Nigeria, 2004 [Copyright Act].

[31]Section 38, Copyright Act.

impact on the mode of dissemination of information with reference to IPR in the new technological milieu. Technology, like law, has always being the fundamental and the most singular instrument in the evolution of human civilization. It is ironic that technology which facilitates a whole range of information communication process for societal benefit, enhance the value of human life, provide the dynamic means for economic activities, cultural exchanges and political engagement, also incrementally delivers the opposite and brings out the worst of human behavior. That realm of normative order is what the regimes of cyber security and cybercrime seeks to regulate: to allow technology deliver on its positive promise; to regulate access and use of technology to promote lawful social and economic relationships, preserve human right and liberty, freedom of expression, privacy and knowledge diffusion. With respect to IPR, the impact should be understood in the context of fulfilling those objectives, as well as balancing the legalistic tension that may be found in the examination of the interaction, which places the burden of protecting valuable knowledge assets in the information communication technology process, which cybercrime regulation seeks to govern.

The legal history of the impact of technological changes on the dissemination of information is central to the technological narrative of IPR infringement or crime as the case may be and cybercrime. This is largely due to the rapid expansion of the disciplines of cybercrime. Technological development, particularly with advances in ICT and the advent of the Internet have rapidly shaped the contours of legal doctrine with the introduction of innovative norms to traditional legal theories, particularly in the disciplines of public and private law. Information technologies, for example, have brought about a variety of cyber related activities within its fold as encapsulated in cybercrime phenomenon, which has continued to redefine traditional principles and architecture of criminal jurisprudence.

Without doubt, the definition of the boundaries between IPR and cybercrime lies squarely in their common technological root. They have both engaged the various and progressive manifestations of technology. On the one hand, cybercrime, which originally evolved as 'computer crimes' with the inception of computer technology in the 1960s and 70s has fully developed with the advent of the Internet. In fact, that accounts for the distinction often made in the literature between ‘computer crime’ and ‘cybercrime’ in the definition of cybercrime. On its own part, IPR's romance with technology has had a long standing tradition that dates as far back in the 17th century origin of copyright law, which may be briefly elucidated upon from the standpoint of legal history and better appreciation of the technological narrative in constructing the relationship between IPR and cybercrime.

In retrospect, IPR has enjoyed a rich history of development in its interaction with technological changes, which has spanned different waves of technological eras more particularly defined in at least four eras. Beginning from the printing technology of the early 18th century, which produced the first copyright legislation and its offspring's,[32]to the second era of reproduction technologies in sound recording, cinematographic images and other analogue technologies and the recent 20th century ICT development, which marked the emergence of computer and Internet era, successive technological changes have not only

[32]The English Copyright Act of 1709 entered into force in 1710 and was commonly referred to 'the statute or act of Anne; named after Queen Anne who reigned between 1702-1714.

redefined the boundaries of human interaction but have also shaped the mode of dissemination of information and IP works and the contours of IP law. With each era, the frontiers of piracy was expanded as new wave of technologies further impaired the efficacy of copyright institution against the new types of uses and users of copyright works. Clearly, the trajectory of technological developments continued to open new vista in the nature and scope of regulatory trends. Currently, in its fourth wave of digital revolution, not only has IP legal norm changed remarkably, its linkage with the phenomenon of cybercrime has become more apparent and intricate, especially as it concerns the way the ICT network, services and content interact and have become susceptible to different forms and character of abuses implicating the relationship between IPR and cybercrime.[33]

It is however instructive to note that while the advent of computer technology marked the genesis of the relationship between IPR and cybercrime resulting from the discussions on the various acts relating to the use of and access to ICT generally and with specific regards to creative and IP related content, the era of the Internet and digital technology marked the high-water mark of that relationship. With respect to IPR, two contexts provide that linkage; first, in terms of infringement. The unprecedented dynamism of the cyberspace has presented immense opportunities, in this respect, for IPR infringement unmatched by previous technologies. With the high speed, volume, seamless and borderless reach, and unprecedented 'digital' capacities, the enormous versatility and innovation of the Internet as the instrument of providing access and use of information relates inexorably to the prospects of human behavior in the new environment. Secondly, infringement presented in the digital context, is radically different from the traditional IPR infringement and has given rise to the phenomenon of digital piracy. The advent of the Internet with the attendant technological revolution has led to the creation of global information society and has singularly redefined the nature of dissemination of information and diffusion of knowledge. With the same force, it has opened new vista of violation of IPR, necessitating renewed protection measures and enforcement strategies.

The development of new technologies and growth of Internet have significantly impacted both IPR and cybercrime norms, and have continued to evolve inexorably as important parts of legal norms of the global information society. While the emerging digital economy and the resulting political economy of the Internet, which has continued to feature new applications including the file sharing technologies or peer to peer networks and players, including the ubiquitous online pirates, opening new vista in copyright jurisprudence, cybercrime regulation has offered a new legal and ethical perspective in defining the boundaries of behavior in the network environment. Whereas digital piracy is specific to IPR, cybercrime captures and criminalizes every identified offensive conduct that threatens the integrity of the network or system or its content, inclusive of IPRs. The digital environment provides the common denominator where

[33]This wave of Internet and digital revolution has occasioned not only the loss of control over dissemination of information by their owners and users alike but also the control of what information to disseminate and to who, bringing about a rethinking of regulatory paradigm for the system itself, its content and persons using the system. That is particularly compelling by its unrestrained evolution both in structure and function, and impact on existing norms. Part of that evolutionary trend is the current technological convergence, which has integrated the features of computing, broadcasting and telecommunication in a single system, thereby blurring traditional regulatory principles otherwise separately applicable to those technological industries.

both categories and activities occur and has been sustained by the exponentially developing features and applications of the global connectivity revolution.

Digital Connection: Cybercrime and 'Digital Piracy'

With the digital revolution in full course, it is no longer in doubt that IPR infringements has assumed new dimension particularly in reflecting the duality of functions in the efficiency of distribution of information and content in the digital environment. While on one hand, it enhances diffusion of content and creative works, on the other hand, it erodes erstwhile control owners have in the distribution of their copyright works. The resultant effect is the ever-growing incidence of digital piracy, the new form of IPR infringement or IP crime properly so called, as earlier described by way of unauthorized distribution of electronic copies of copyright works such as software, movies, music or other content in the digital media.

The term 'internet piracy' or digital piracy covers several different ways in which infringing music is distributed or downloaded illegally. Websites host large amounts of music but do not have permission to copy it or deliver it over the Internet. These sites generally offer music either for free or at very low prices because they do not pay artists or other rights holders for their work, including 'peer to peer' (P2P) networks which facilitate file-sharing directly between individual users allowing distribution of a music file to millions of Internet users. Uploading copyright materials onto P2P networks without the permission of the copyright owner became well-known engines of copyright infringement. Global trends in digital piracy have reflected huge losses in the fortunes of music, software and movie industries in terms of revenue and jobs.[34]

The impact of digital piracy cannot be over economized in every market or industry, for example with downloads still accounting for the major bulk of global digital revenue at 52%.It implies that global music industry revenue from physical format account for less than half.[35] In the United States, which hosts the world largest entertainment and media industries, for example, $2.7 billion in earnings and over 71,066 jobs are lost every year due to online piracy, and in 2014 over $12.15 in economic losses in the music industry alone have been recorded due to online piracy.[36] In the same year, 42% of software are illegally downloaded and over $59 billion of software are illegally downloaded. The figure has been on the increase due largely to the versatility of Internet and inadequate digital information management and enforcement measures.

Available statistics and reports for Nigeria have always shown a high level of IPR violation with increasing Internet penetration and widely embraced digital culture. National Bureau of Statistics, in 2013 reports 1.5% contribution of the film and music industries to the national GDP and according to the report, large scale illegal downloads of music and films is one of the bane of the creative economy that has eroded the

[34]See www.go-gulf.com/blog/online-piracy, accessed more 29 February 2016.

[35]IFPI Digital Music Digital 2015, Charting the Path to Sustainable Growth. The report reveals 46 billion music downloads via Bittorrent alone in 2014, which is outside other channels like cyber locker, linking sites and social networks, mostly infringing, at page 38.

[36]In 2010, Hollywood movie, 'Avatar' was reported as the most pirated movie with more than 17 million downloads.

gains of those film and music industries.[37] By 2015,Nollywood, Nigeria's film industry was reported as $3.3billion industry by volume but largely plagued by digital piracy.[38] The scale of software piracy is perhaps worse with 2010 Business Software Alliance (BSA) figure of 83% level in the use of unlicensed software showing the loss of US$156million to software piracy in 2009 and within top 10 in the global list.[39] Without significant decline from previous years, the 2013 Global Software Survey has fixed the commercial value of unlicensed software in Nigeria to more than $287million showing that software piracy is sustained rather than reduced.[40]

Some statistics reflect varying figures but the visible trends have shown that the Nigerian film and music industries are emerging globally with acclaim and the software industry is rapidly evolving as the next creative frontier market on the continent. Notwithstanding the diversity and dearth of reliable statistics, the incidence and impact of digital piracy of music, movie and software is conspicuously demonstrated in the performance deficit in the local creative industries and indigenous innovation and the relatively low ratings in national GDP. It is therefore remarkable when the new cybercrime framework engenders appreciable inroads into IPR and presents the prospects of strengthening existing IPR protection that would offer alternative mechanism for enhancing administration and enforcement of rights by the rapidly emerging IP industries. The trends and statistics, which reflects the impact of digital piracy on the state of IP industries underscores the importance of its relevance to the realm of anti-cybercrime regulation and control.

The impact has raised evolving and contentious issues bordering on appropriate legal responses, for example, to the creation and distribution of content, peer to peer file sharing software that readily facilitates illegal copying of music and film and the extent of circumvention of digital processes for denying access to copyright material, secondary copyright infringement and ISP liability, patenting of business systems and software, administration of domain names and vital means of promoting and marketing products, service and technologies in the Internet, among other issues that has arisen in its impact on IPR. Consequently, with the strong historical roots in the major technological epochs which has continued to define the nature and character of dissemination of information including IP and associated rights, IP law has been sustained by prevailing technologies and economics of the marketplace, and like technology itself, continues to be relevant in the disparate fields of human enterprise, including the emergent legal field of cybercrime. The relationship between IPR and cybercrime is therefore best defined by the impact of ICT environment on the regulation of aspects of human enterprise implicated in IPRs and covered under relevant cybercrime legislation.

Intellectual Property Rights Analysis of the Cybercrime Act 2015

[37]See Financial Times Report at www.ft.com/cms/s/accessed 26 March 2023

[38]Financial Times Report (n 68).

[39]See vanguardngr.com/2010/05/piracy-rate-in-Nigeria-now-83-percent.

[40]ibid

1. Cybercrime Act in Brief

Before examining IPR protection under the Cybercrime Act, it is necessary to briefly highlight the main provisions and general features of the Act. As Nigeria's first attempt at regulating cybercrime and an important national instrument for cyber security, the Act affirms that imperative in its explanatory note and substantive primary objective that it seeks to provide an effective, unified and comprehensive legal regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria; Ensure the protection of critical national information infrastructure; and promote cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.[41]

Within those objectives, the Act would appear to capture the three critical areas of data security, privacy and IPR, which are implicated in any legal or policy instrument for regulating the provision of information infrastructure and services in the networked environment. The Act contains Seven Parts and Two Schedules. Part I deals with object and application. Part II, Protection of critical National information infrastructure Part III, Offences and Penalties. Part IV, duties of financial institutions. Part V, Administration and enforcement. Part VI, Arrest, search, seizure and Prosecution. Part VII, Jurisdiction and international Co-operation, which describe the main theme of the legislation.

The Act provides the definition of four key terms, namely, 'computer', 'computer data', 'computer program' and 'computer system', which are key features of the information communication system, and in the regulation of access and use of hardware (computers), software and content including IPR connected with the system. These terms are also important in the protection of IPR in that environment. According to section 58,'Computer data' includes every information required by the computer to be able to operate, run programs, store programs and store information that the computer user needs such as text files or other files that are associated with the program the computer user is running.

'Computer system'

a) Refers to any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automated or interactive processing of data;
b) covers any type of device with data processing capabilities including, computers and mobile phones;
c) consists of hardware and software which may include input, output and storage components that may stand alone or be connected in a network or other similar devices; and
d) includes computer data storage devices or media;[42]

[41]Section 1, Cybercrime Act 2015 [Cybercrime Act]

[42]The section also defines 'Computer' as an electronic, magnetic, optical, electrochemical or other high speed data processing device performing logical, arithmetic or storage functions and includes any data storage facility and all communication devices that can directly interface with a computer through communication protocols but it excludes portable hand-held calculator, typesetter or other similar devices;

The same section also defines 'computer program' as 'a set of instructions written to perform or execute a specified task with a computer', a definition, which has acquired considerable notoriety in various types of legislation, including IP and cyber related laws.[43] For example, Copyright Act defines computer programme in a similar way.[44] The more comprehensive definition under the Cybercrime Act, not only helps in identifying its application or uses, it may also help in clarifying and aiding in the interpretation of the definition under the Copyright Act. Under traditional copyright law, although, the question of protection of computer program or software as an eligible literary work is no longer in contention, there has been considerable debate and disharmony on the extent of protection not only under copyright but also under patent law considering its dynamic nature and application within the two frameworks. That however, is a different context of IPR from the cybercrime issue under discourse.

Consistent with most data protection and cybercrime legislation, the Act creates certain computer and content related offences. In addition to the provisions for the protection of the information infrastructure which designate certain computer system or network as critical national information infrastructure and the audit and inspection of same,[45] the Act provides for a wide ranging system or network-related offences which, though constitute the main stay of cybercrime, are not particularly germane to IPR. Thus, these offences, except in so far as are pertinent to the discussion of IPR, are not necessary in the consideration of IPR under the Act.[46]

Furthermore, the Act specifically addresses financial institutions and places a duty on them for retention and protection of data and penalizes interception of electronic communications and failure of service providers to assist in enforcement including the identification and prosecution of offenders, or the tracking or tracing of proceeds of crime.[47] The Act provides for a special enforcement measures including prosecution of various offences created under it. The Act places the function of co-ordination of

[43]While section 1(i), WIPO Model Provisions on the Protection of Computer Software 1978, defines computer program as 'a set of instructions capable, when in a machine-readable medium, of causing a machine having information-processing capabilities to indicate, perform or achieve a particular function, task or result', article 10(1) TRIPS means confirms that 'computer programs, whether in source or object code, shall be protected as literary works under the Berne Convention'.

[44] Section 51, Copyright Act, within the context of literary work as an eligible work of copyright, states that 'computer programme' means a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result.' While the US Copyright Act defines computer program as 'a set of statements or instructions to be used directly or indirectly in a computer to bring about a certain result' (17 USC 101), UK's does not provide a definition but merely includes computer program as a literary work (section 3(1), Copyright, Designs and Patents Act 1988).

[45]Sections 3 and 4, Cybercrime Act.

[46]The list of offences include the following; tampering with critical national infrastructure (sections 5 & 10); unlawful access to a computer (section 6); system interference (section 8); unlawful interception (section 12); unauthorized modification of computer system, network data or system interference (section 16); intercepting electronic messages, emails, electronic money transfers (section 9); willful misdirection of electronic messages (section 11); computer related forgery (section 13); computer related fraud (section 14); theft of electronic devises (section 15); cyber terrorism (section 18); fraudulent issuance of e instructions (section 20);reporting of cyber threats (section 21); identity theft and impersonation (section 22); child pornography and related offences (section 23); cyber stalking (section 24); cybersquatting (section 25); racist and xenophobic offences (section 26); attempt, conspiracy, aiding and abetting (section 27); importation and fabrication of e tools (section 28); breach of confidence by service providers (section 29) manipulation of ATM/POS Terminals (section 30); employees responsibility (section 31); phishing, spamming, spreading of computer virus (section 32); electronic card related fraud (section 33);use of fraudulent device or attached emails and web sites (section 36).

[47]See Part IV, Cybercrime Act.

administration and enforcement of the Act on the Office of National Security Adviser (ONSA) and to some extent the Attorney General of the Federation for prosecution of cybercrime and maintenance of international co-operation in the enforcement of the Act.[48] It established the National Cybercrime Advisory Council (NCyAC) specifically for the purposes of the Act with ONSA as presiding officer.[49] The Act also established the National Cyber Security Fund domiciled in the Central Bank of Nigeria for levies specified under the second schedule and other grants, aids, gifts or other funds accruing to the fund, tax exempt.[50]

From the foregoing, while the Cybercrime Act is the indispensable policy and legal tool in the promotion and regulation of cyber security in which information privacy, security, and protection of IPR are essential subsets and components, it also offers, within the disciplines of cybercrime law, the legal framework for providing effective measures for protection of content (IPR) which presents the perspective from which the IPRs under Cybercrime Act 2015 can be examined.

IP is a long-standing field of law and policy that has established itself as the dominant legal mechanism for the protection of different forms of knowledge assets and the rights over those assets. As indicated in the foregoing, IP law has continued to maintain its characteristic tenacity to the impact of technological changes that has shaped the subsistence of IP categories and IP rights and their enforcement, which has brought into reckoning its relationship with cyber law and the phenomenon of cybercrime. On its part, cyber law, as an emergent framework of regulation of cybercrime, is a relatively new but equally dynamic field at the intersection of private and public law domain.

Consequently, two important contexts provide the rational basis for examining the protection of IPRs under the Cybercrime Act. The first is the application of IP law, which governs IPR and IP infringement particularly as it relates to digital or online piracy and counterfeiting in that environment. The second is the need to address the question whether the Cybercrime Act provides among others, the legal framework for the protection of IPR as claimed. It must be noted that the explanatory note and Section 1 expressly mentions 'protection of...intellectual property' as one of the objectives of the Act.[51]While it is not in doubt that IPRs are generally or conceptually implicated in the phenomenon of cybercrime, the critical inquiry points to the extent or nature of such implication in recent cybercrime legislation as presented in Nigeria's Cybercrime Act. Consequently, the question may arise whether the Act tells a lie about itself with regards to IPR protection under section 1. The main point of emphasis has always been the impact of ICT on IPR, which has led to new forms or medium of exploitation of IPR and the emergence of digital and online piracy of creative works, which has been considered in the analysis of cybercrime.

[48]See Section 41, Cybercrime Act.

[49]See Part V, Cybercrime Act for administration and enforcement including the functions and powers the Cybercrime Advisory Council. The Council has recently been inaugurated by the Federal Government.

[50]See Section 44, Cybercrime Act.

[51]Section 1, Cybercrime Act states that 'The objectives of the Act are to -...(c) promote cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights' [emphasis supplied].

Although, the primary source of legal protection for creative works and technological innovation in the online environment is IP law, the impact or implication of ICT on IPR have effectively brought IP within the rubric of cybercrime law within the overall Internet governance system. As far as IPR is concerned, there would appear to be a consensus both in the concerns and objectives of the two laws in terms of the protection of the economic value of the works, provision for all known forms of exploitation of rights and operating as safeguards against infringement. Indeed, these issues continue to characterize the architecture of IP law in the digital reform and the development of cybercrime legislation. With the nexus established both in terms of the framework and objectives, it can be asserted that IP and cybercrime law now offer the natural legal domain for the regulation of IPR in the network environment. Generally speaking, while IPR in the digital domain falls within that framework and the applicable rules, it may not specifically be governed by that framework.

As indicated, while the ICT interface with law has been manifested in the concept of data privacy, security and IPR, however, with regards to IPR, it is manifested in three contexts; first, in terms of the definition of IP subject matter and constituent rights, second, in terms of the control of dissemination of works and third, in terms of enforcement of IPRs, all of which constitute the basis in which to discuss the relationship between IPR and cybercrime, and more specifically the protection of IPR under the Cybercrime Act in view. Indeed, the IPR related provisions or offences and their enforcement under the Cybercrime Act would provide the premise for examining the question whether that Act complements IP law or fills existing gaps in extant IP law in Nigeria.

Cybercrime and Three Key Copyright Concepts: Legal Implication

Within the general cybercrime framework, it is important to note that one of the central features of the Cybercrime Act, like any other cybercrime legislation, are the offences created under it. The acts, which constitute digital piracy in/relation to IPR related offences aligns with some of the widespread activities classified as 'cybercrime' activities. These offences reflect some of the key IPR concepts and norms and provide the nexus between cybercrime and IPRs and more particularly the premise for the analysis of IPR protection under the Act in question. For example, this specie of offences includes system interference,[52] unlawful interception,[53] computer related forgery,[54] computer related fraud,[55] unauthorized modification of computer systems, network data and system interference,[56] cyber-squatting,[57] attempt, conspiracy, aiding and abetting,[58] among other provisions relating to protection of data and security of system or network. In this analysis, three notable IPR concepts are implicated in relation to or in respect of which

[52]Section 8, Cybercrime Act.
[53]Section 12, Cybercrime Act.
[54]Section 13, Cybercrime Act.
[55]Section 14, Cybercrime Act.
[56]Section 16, Cybercrime Act.
[57]Section 25, Cybercrime Act.
[58]Section 27, Cybercrime Act.

'cybercrime offences' are created under the Act, namely, computer software, circumvention of technological protection measures (TPM) and service provider liability.

1. Computer Software Protection

Computer software protection is not particularly germane to the discussion of cybercrime and therefore does not require elaborate emphasis. Software or computer program and its protection have remained one of the important subjects of technological innovation and one that has engendered unending controversy bordering on the best legal response to its functions in the information ecosystem. Suffice it to say that the protection of software has not been firmly secured under IP law on the combination of juridical, technical and policy grounds that are not particularly relevant in the present context of discussion.[59] Indeed, software protection has engaged the attention of IP for a long time and its dynamics has featured in shifting legal grounds under both national and international copyright and patent law. The ambivalence of IP law on the legal status of software, which has not in any way diminished its central place as a technological innovation that is deserving of protection contrasts with the value neutral position taken by cybercrime law, which probably better assures the protection.

Cybercrime law does not pay particular attention to the consideration of software protection once the act involved in relation to a particular program constitute a crime defined under the cybercrime legislation. This is indicative of the treatment of activities in relation to computer programs under the Cybercrime Act. The criminalization of certain range of computer related activities or dealing in computer system, program or data by the definition of computer related fraud or forgery or unauthorized modification of computer system, network data and system interference under the Cybercrime Act deliberately by passes the complexity and international disharmony in the protection of computer software or program under copyright and patent law.[60]

In effect, software protection, if any, does not matter or count in the creation or actual commission of the offences relating to the computer data, program or the system itself, once the act prohibited in relation thereto is established, it remains an offence under the Cybercrime Act. For example, where 'a person knowingly accesses any computer or network and inputs, alters, deletes or suppresses any data resulting in

[59]See the rich body of Literature and Case Law on Software Protection: Whelan Associates V. Jaslow Dental Laboratories; Copyright Protection For Computer Software Structure- What Is The Purpose [1987] Wis L Rev.859 R Widdison, Software Patent Pending [2000] The Journal Of Information, Law And Technology 3, D W Carsen, Legal Protection Of Computer Software; Patent, Copyright And Trade Secrets [1994] 20 Journal Of Contemporary Law 13,Calvin WValden, Copyright And Patent Protection For Computer Software; How Has The Landscape Changed, Intellectual Property Today, April 2015; E Gratton, Should Patent Protection Be Considered For Computer Software-Related Innovation? [2002] 7, Computer Law Review & Technology Journal 2, 223; S DAUS, Computer Program Claims; The Final Frontier For Software Inventions [1998] 20EIPR 429; Cohen, Loren, Okediji & O'Rourke, Copyright In The Global Information Economy, Aspen, 3rd Ed. 226, H Macqueen, C Waelde & G Laurie, Contemporary Intellectual Property Law And Policy, Oxford, 2008, 516; For Cases See DDR Holdings LLC V. Hotels, Com LLP, 773 F.3d Fed. Cir. 2014; Oracle Am Inc V, Google Inc., 750 G.3d 1339, 1355 (Fed.Cir. 2014). For Statutes See WIPO Model Provision on Protection of Computer Software, General 1978, 5.1 (1), EU Directive on Patentability Of Computer-Implemented Invention 2002,

[60]While wide consensus exists regarding broad areas of criminalization, analysis of various instruments would reveal divergent approaches that are apparent both at national and, in some cases, international level. See Comprehensive Study on Cybercrime UNODC (n 12)111.

unauthentic data with the intention that such inauthentic data will be considered or acted upon as if it were authentic or genuine, regardless of whether or not such data is directly readable or intelligible'[61] or in another context 'where a person 'causes any loss of property to another by altering, erasing, in putting or suppressing any data held in any computer, whether or not for the purpose of conferring any economic benefits on himself or another person'[62] are clearly independent of IP protection of software for the offence to take place. Another good example is the offence of unauthorized modification of computer systems, network data and system interference where the program or data is altered, erased, removed, suppressed or where the normal operation or functioning of computer system according to its intended purposes is impaired.[63] Consequently, under the cybercrime regime, it is not important that the computer program or software in question should be or in fact protected as IP subject matter, which protection, as indicated, is divergent across jurisdictions and largely unsettled globally.

2. Circumvention of Technological Protection Measures (TPM)

Technological protection measures (TPM) provides the second important aspect of the cybercrime framework, which is of particular relevance to some of the standard provisions of copyright law in the digital context. The provisions relating to system interference and unlawful interception would appear to implicate the copyright rule against circumvention of technological protection measures (TPM) and remedies obtainable for tampering with rights management information (RMI) for digital copyright works. The dynamics of this so called copyright's anti-circumvention rule deserves a brief elucidation. Circumvention of technological protection of digital works quickly followed the digital revolution of the 90s and it became expedient that the copyright owners needed additional legal protection against the circumvention of any access or copy-control measures they adopt in the protection of the copyright in their works. Even with the technological protection measures (TPM) and digital rights management (DRM) systems, which allows implementation of protective technologies for digital content, circumvention of these measures were still possible. With digitization and peer-to-peer technology that enables users and consumers to share file and data including music, movies and software, serious concern have been raised on the growth of entertainment and other IP industries as a result of the pervasive effect of the digital environment on creative enterprise. Part of this concern has implicated responses and approaches in criminalizing illegal file sharing and disenabling encryption of protected digital content or password protections of such content, which constitutes 'effective technological measures.'

At the international level, the WIPO Internet treaties of 1996, comprising the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonogram Treaty (WPPT) provide significant model response this development by extending copyright protection to authors of literary and artistic works, computer programs and compilation of data as well as performers in the digital environment. The treaties ushered

[61]See Section 13 Cybercrime for Computer Related Forgery. The provision is impari material with Section II, Article 29 on Specific offences specific to Information and Communications Technologies under the AU Convention on Cyber security.

[62]See Section 14 Cybercrime Act for Computer Related Fraud.

[63]See Section 16, Cybercrime Act.

the global framework for access and use of creative work with a double-edge sword. First, with providing against circumvention of technological measures and sanctioning same,[64] and second, providing remedies for tampering with rights management information (RMI), which ordinarily helps to identify the work and enforce copyright interest, knowing or having reason to know that such tampering will induce, enable or facilitate copyright infringement.[65] In defending technological protection measures, the treaties obligate member to provide for the protection against circumvention of effective technological measures adopted by authors to control access or use of their works and in that regard penalizes any effort to circumvent the technological protections in the exercise of rights in their works.

The treaties offered the initial impetus for this protection measure for the copyright industries that was quickly followed by national copyright legislation.[66] The US opened the floodgate of national copyright legislation with Digital Millennium Copyright Act 1998 (DMCA), which criminalized illegal file exchange of copyright materials and music or movies.[67] Emerging copyright legislative reforms have recognized the desirability of protecting copyright owners who deploy technical protection measures for digital media products or services intended for distribution from clever technologists who build tools to bypass or disable these TPMs in order to render them vulnerable and gain access. In an important context of the IPR protection under cybercrime law, the legal prohibition of these circumvention measures which provides legal and regulatory mechanism for protecting valuable IP was quickly embraced as part of the efforts in waging war against cybercrime. The Cybercrime Act would appear to relate favourably with this innovative measure by the provision against tampering or interfering with the computer system. This cybercrime-based provision, which criminalizes any form of interference with, interception of or access to the computer system, with the requisite intent,[68] is in essence an anti-circumvention prohibition existing under copyright law. However, it applies to unlawful access to computer data as much as to the computer system or network and therefore offers an effective legal tool against infringing or offending activity in the digital media.

By generally creating offences around unlawful access including importation and fabrication of tools,[69] the Act echoes the copyright rule against circumvention of TPM and tampering with RMI, an important effect on the protection of IPR in the digital network. It is instructive to note that 'Access' is defined in section 58 of the Act as 'gaining entry into, instructing or communicating with the logical, arithmetical or memory function resources of a computer system or network'. In the same section, the definition of 'authorized Access' provides a clearer and more helpful context for the protection of IPR under cybercrime framework.

[64]See article 11, WCT.

[65]See article 12, WCT.

[66]Article 11, WIPO Copyright Treaty 1996 provides 'Contracting parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.' See section 1201, Digital Millennium Copyright Act, 1998. (17 USC 1201).

[67] See section 1201, Digital Millennium Copyright Act, 1998. (17 USC 1201).

[68]See section 9, Cybercrime Act relating to 'acts, which causes directly or indirectly the serious hindering of the functioning of a computer system by inputting, transmitting, and damaging, deleting, deteriorating, altering or suppressing computer data'.

[69]Section 28, Cybercrime Act.

'[A]authorized Access' means a person has authorized access to any program or data held in a computer if-

a) the person is entitled to control access to the program or data in question; or
b) the person has consent to access such program or data from a person who is charged with granting such consent

Simply put in IP nuance, acts of circumvention of technological measures for protection of copyright works, an IPR infringement constitutes an unauthorized or unlawful interference or interference and therefore amounts to an offence under the Act, and this effectively fills the gap under the extant Copyright Act in Nigeria, which has no anti-circumvention provision.

In the absence of this protection measures under the Copyright Act, it would appear that the provision under the Cybercrime Act fills that gap or lacuna, specifically for copyright owners who have to implement specially designed technical measures to protect their works in the digital system. In practice, nothing prevents copyright owners from invoking the provision in the Cybercrime Act in enforcement or exercise of their circumvented copyright because the provision is not restrictive but imposes liability on 'any person' with the requisite mens rea and actus reus of the offence. This is a particularly significant innovative approach in the use of cybercrime framework considering the serious impact and continuing linkage of software piracy and other digital piracy as key contributor to organized crimes. Though Nigeria has neither ratified nor implemented WCT, it would appear that with the criminal offence of unauthorized or unlawful access to computer data under the Act as it applies to creative works, she is indirectly implementing WCT with regards to anti-circumvention measures in the digital protection of works through traditional cybercrime strategies contained in the Cybercrime Act.

3. Service Provider Liability

The last aspect borders on the provisions on the duties and obligations of service providers giving rise to their liability, considered under both copyright and cybercrime laws. The digital media have presented copyright law with the dilemma of evaluating the legal implication of the role of intermediaries and technology developers for user infringements against copyright owners for unauthorized distribution or use of copyright works in the digital network. Contributing liability therefore has featured in the resulting secondary copyright liability rules that have formed the basis of determining the liability of these intermediaries in different circumstances under emergent copyright law. Since providers under the Cybercrime Act are under a duty to keep all traffic data and subscriber information as may be prescribed by the 'relevant authority' and obliged to "preserve, hold or retain any traffic data subscriber information, non-content information and content data and to release any information required to do kept, 'subject to the constitutional rights to privacy,[70] failure of which amounts to a breach of that duty in contravention of the provisions of the Act, it clearly implies that service providers are held responsible for the security and sanctity of information or data in their network. Does this obligation extend to a situation where

[70]Section 38, Cybercrime Act.

infringement of copyright and IPR materials takes place? The rule relating to service provider liability applicable under the prevailing digital copyright system would therefore appear to be implicated by that provision.

Online intermediary liability has become increasingly controversial and complex particularly in relation to copyright due principally to the high rate of unauthorized downloading of digital music, movies and videos since the advent of P2P technology, social networking and User Generated Content (UGC) such as eBay, YouTube, Facebook, cloud computing and other Internet phenomena, which has required effective legal framework or approaches. Serious concerns bordered on lack of effective legal or actual control and the adoption of a policy of imposing liability on mere intermediaries or conduit for the multiple types of unwanted content of third parties covering the category of harmful materials such as pornography, hate speech, defamatory content on one hand and copyright infringing materials on the other hand. Two approaches have emerged in the model legal frameworks for Internet intermediaries. The first is "horizontal" regulation, which deals with the wider intermediary liability across all types of content.[71] The second is "vertical" regulation, which provides rules for special or more specific cases such as copyright, protection of children, personal data, counterfeiting or domain names.[72]

Like the anti-circumvention measures, the obligation as of service provider may have conveniently crept into the universe of Cybercrime Act considering the provisions relating to service providers. In spite of overlapping features, both copyright and cybercrime frameworks are distinguishable; the question which may arise is whether the scope of the duty and associated liability precisely fits into the elaborate framework of service provider liability under copyright law and jurisprudence. The Cybercrime Act defines 'service provider' as

1. any public or private entity that provides to users of its services the ability to communicate by means of a computer system, electronic communication devices, mobile networks; and
2. Any other entity that processes or stores computer data on behalf of such communication services or user of such service.[73]

Two main global models emerged in the EC Electronic Commerce Directive (ECD) and US DMCA to provide rules for exemptions for ISPs, which rules have been applied with a fair level of consistency in different jurisdictions.[74] The flexible rule constructs a framework that provides immunities or limited liability known as 'safe harbor' for the different functions carried out by intermediaries. The safe harbor under the DMCA provides immunity for infringement liability for service provider under specified

[71]EC E Commerce Directive is a horizontal model.

[72]US DCMA, UK Defamation Act 1996 or the French Code monetaire et financier, for online fraud with payment card adopts the vertical model.

[73]The definition extends to a wide range of 'service' providers like hosting services including also those who provide 'access' and telecommunication operators.

[74]For example, in the US, two separate regimes of immunities were created for ISPs and hosts; one relating to all types of liability materials, and the other relating to liability for infringing copyright materials.

circumstances.[75] The safe harbor, for example, effectively apply and exempt only if the service provider establishes, publishes and implements both a Notice and take Down (NTD) system for removing content when copyright owners complain and a system for identifying 'repeat infringers' and removing them from the system. The framework adopted under the ECD for safe harbor transmission, caching and hosting services are similar to those in the DMCA.[76] The two regimes provides a model legal framework for many developing countries including those who have no rules for determining liability of intermediaries whether of a general or specific nature and further indicate the context in which to provide the ramification of the service provider duty under the Cybercrime Act in its application to IPR. The role and obligation of the service provider as contemplated under that Act can be placed within the rubric of copyright infringement as much as within the wider liability for other types of illegal or reprehensible activity under the purview of cybercrime.

As a matter of general rule, copyright is a strict liability because knowledge is not primarily required for primary infringement. However, secondary infringements of copyright are distinguished from primary or direct infringement because the defendant is not generally liable unless he knew or had no reason to believe that he was handling infringing materials or that the use would infringe copyright. It is also necessary to distinguish the secondary liability in civil arena from criminal. Under the Nigerian copyright law, knowledge is not a prerequisite for secondary liability.[77] In effect, the application or nature of secondary infringement would not appear to insulate service providers and intermediaries from infringement solely on the ground of absence of knowledge that the content they are dealing with is an infringement of copyright.

However, in criminal infringement, the position is different. Copyright Act specifically provides for knowledge as a defense, which requires the accused "to prove to the satisfaction of the court that he did not know and had no reason to believe that any such copy was an infringing copy," and once that burden of proof on the accused (unlike in the general criminal matter where the prosecutor always carry the burden), it operates as a complete defense and a bar to conviction.[78] In effect, unlike in civil infringement, knowledge and bad motive or intent is required for criminal infringement. Similarly, with respect to Cybercrime Act, absence of knowledge on the part of the service providers also operates as defense and in addition he most proves that 'the offence was committed without his knowledge or that he exercised all due diligence in preventing the commission of the offence',[79] which are essential components or ingredients of the immunity or exemptions afforded them under other copyright law.

[75]17 USC 512. Under the provision, immunity is afforded an ISP who engages in any of the following activities, namely, 1) transitory digital network communications, 2) system caching, 3) storing information on its systems at the direction of users, 4) providing at the direction of users, 4) providing location tools like hypertext links.

[76]See Directive 2000/31/ec of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, 2000 O. J (L 178) 1, arts. 12-15.

[77]Except in the specific instance expressly provided for under S.16 (3) where it must be shown that at the time of the infringement the defendant was not aware and copyright subsisted in the work and that if any, its effect mitigates relief to account of profit only.

[78]Section 20 (2) Copyright Act.

[79]Section 29(5) Cybercrime Act.

Consequently, both the Copyright and Cybercrime Acts provide complementary legal frameworks for secondary infringements of service providers and intermediaries, particularly from the perspective of criminal liability. The requirement for service providers to provide assistance in the identification, tracking, tracing, freezing, removal and prosecution is consistent with the obligation of 'due diligence' required in preventing or avoiding the commission of the offence as justification of the immunity. It also correlates with the requirement for service providers to take active steps in ensuring no infringement take place, prevent or identify repeat infringement or administer notice and take down upon knowledge of infringement under copyright situation. To a large extent, the scope and/or extent of the duties and liabilities of service providers under the Cybercrime are and distinguishable from that under the Copyright Act. First, they are broader and more comprehensively defined. Cybercrime Act would appear more 'horizontal' in approach as it defines the role and responsibility of service providers for all types of liability materials or content inclusive of copyright and IP. That is understandable because Cybercrime Act is not copyright or IP legislation. Secondly, they are also applicable to online environment, a gap, which Cybercrime Act would appear to fill with specific regards to the role and responsibilities of Internet intermediaries and service providers in the administration and enforcement of copyright and related rights.

Interestingly, the enforcement mechanisms under the two Acts are different. In one instance, the Nigerian Copyright Commission (NCC) is the enforcing authority for criminal infringement of copyright,[80] and in another instance, 'law enforcement agency', though not defined under the Cybercrime Act, includes, 'all law enforcement security and intelligence agencies', the ONSA including the Attorney General of the Federation (AGF) in collaboration with ONSA for 'effective prosecution of cybercrime and cyber security matters' within the framework of administration and enforcement of the Act.[81] While service providers can take advantage of the two Acts depending on the subject matter of liability, the streams of enforcement, to all intent and purposes, remain separate. Clearly, from the foregoing, Cybercrime Act has implication for IPR. That Act though does not directly or expressly mention piracy, its reference to IPR shows a legislative intent to cover activities touching upon IPR and IP infringements particularly piracy and counterfeiting. That raises the question whether it is indeed the remit of cybercrime law to protect IPR. The answer would depend largely on the express provisions of the Act as highlighted in this paper. Strictly speaking, content, as opposed to the network or computer related offences, provide the limits for examining IPR protection under the Act. As already indicated, the Act has made tremendous inroads into the rules guiding circumvention of TPM and secondary liability of intermediaries, which are some of the significant developments in copyright policies and jurisprudence in the era of cybercrime regulation. For example, prohibiting circumventing measures, blocking user's access to copyright infringing content or site, placing responsibility on ISPs to secure content, prevent infringement and sanctioning neglect or refusal to do so in the cybercriminal dimension complements prevailing strategies at curbing online violations and reinforces existing IPR framework for digital piracy and ISP liability provisions. It addresses the functional relationship between cybercrime and IPR law.

[80]Section 38, Copyright Act.

[81]See Part V, Administration and Enforcement, Cybercrime Act.

The provision of duties of financial institutions with respect of data and information management effectively brings them within the ambit of service providers together with the legal responsibility and liability attaching thereto. Specifically, the duty of financial institution 'to keep all traffic data and subscriber information'[82] including relevant creative works, trademark in form of commercial information or inventions, patented or otherwise, places corresponding liability on such institution as 'service provider' so defined for any breach of that duty within the framework of cybercrime when any of the indicated IPRs is violated. This is important because of the current effort in recalibrating the architecture of Internet intermediaries, who are no longer limited to technological or traditional access providers but extend to a range of service providers including advertising companies, financial institutions and payment providers or platforms and mobile app platforms, who in appropriated circumstances, should not be exempted from taking responsibility for their actions or security of their respective platforms within the existing secondary liability norms. Recent copyright reform in Nigeria have reflected the long overdue legal response to the development through the current draft Copyright Act which makes provision relating to circumvention of technological protection measures and online content.[83]

From the foregoing, although the objective of the Cybercrime Act is not to establish another legal framework for IPR protection, there is no doubt that it has far reaching implication on the protection and enforcement of IPR in Nigeria, particularly in the field of copyright and trademark in the digital and online environment. Copyright owners and relevant enforcement agencies, including intermediaries and service providers many begin to consider how to use the Act to enforce digital and online infringements of creative works and content, particularly music, Nollywood movies, software or domain names in order to protect the industries and technologies from the nefarious activities of hackers, cybersquaters, pirates, counterfeiters and illegal users. In view of the fact that the digital frontier offers the emerging entertainment industry the benefit of the global market, Cybercrime Act may have unwittingly provided a valuable mechanism, which they should rely on for the protection and enforcement of IPR in the digital media.

Conclusion

This paper has examined IPR and IPR infringement from the prism of cybercrime and the Cybercrime Act 2015. In doing so, it considers the definitional and structural approaches involved in the main instruments, which have provided major frameworks and strategies for promoting and ensuring cyber security in the global information superhighway. While the distinction with computer crime has featured in available definitions, the precise scope of cybercrime is both dynamic and all-encompassing in the description of activities relating to the system and network. The paper underscores the technological roots and the associated digital connection that has shaped the contours of cybercrime phenomenon into what it has developed into and affirms it's far-reaching implication on the protection of IPRs indicating the connection between cybercrime and IPR crimes in the form of digital piracy and other forms of IPR infringement.

[82]PART IV, section 38, Cybercrime Act.

[83]See Part VI on Anti-Piracy & other measures and part VII on provisions relating to online content, Draft Copyright Bill 2015.

The paper further identifies three key copyright-related frameworks that make it possible to relate cybercrime with emergent IPR policy in the digital environment. Notably, computer software protection, circumvention of technological protection and service provider liability measures has been identified to provide important linkages for examination of the relationship. While the fact of IP protection or non-protection for computer program or software offers no exemption to the commission of cybercrime with respect to the computer program, offences relating to modification of computer systems, network data and system interference, identity theft as well as service provider responsibility under Cybercrime Act provides important and complementary regulatory frameworks and fills the gap for anti-circumvention of technological protection and service provider liability rules in the synergy of objectives and frameworks for ensuring effective IPR protection and promoting emerging cyber security strategies. Notwithstanding that Cybercrime Act is not, strictly speaking, an IP legislation, the paper suggests that the Act represent an important instrument for combating serious cases of digital piracy. It concludes that the Cybercrime Act indeed offers an additional framework and perspective in which to examine the emerging IPR infringement and enforcement in the current information economy in Nigeria.