Emerging Legal Issues and Challenges In Information Technology and Communication In Nigeria*

Abstract

The paper traces the growth in the Information and Communication Technology (ICT) infrastructure in Nigeria, and how market-forces have pulled the industry to liberalize. It reveals that the Nigerian Communication Act[1] which subsequently provided for the establishment of a regulatory body, the Nigerian Communications Commission (NCC) in 1992 was the first bold act taken in that direction. It shows how liberalization of the telecommunications market in Nigeria (especially with the coming into force of the Communications Act, 2004, has developed the industry with attendant legal challenges that are not explicitly addressed by general common law classifications of contract or tort, and that criminal legislation also lags behind in many respects to tackle criminal actions possibly fostered by ICT. It therefore suggests ways and measures to deal with them.

Introduction

The emergence of communications in Nigeria can be traced to 1851 when the British Post Office established its postal branch in the country. This was followed in 1885 by the establishment of the internal telecommunication arms. However the first direct telegraph services between Lagos and

---

* Emuasiri A. Jonathan, Dept. of Public & International Law Faculty of Law, University of Abuja and Mrs. Ifeola Adesina, Lecturer, Nigerian Law School, Yenagoa Campus, Bayelsa State.

[1] Act No. 75, 1992 as amended by Act No. 30, 1998

London began in September 1886 using submarine cables by the African District Telegraphy Company Limited and Cable and Wireless Company of London. The colonial government moved a step further in 1895 to introduce local telecommunication form of telegraphy using the key and sounder system. It was then run under the Public Work Department (PWD). By 1907, the responsibility was transferred to the Post and Telegraph Department (P & T) which had been formed to operate national postal and communications services. At the time, the operation of Post and Telegraph Department was heavily dominated by colonial masters, with projects which were then at small scale direct executed by the establishment's staff on contract. From 1914, in the wake of the amalgamation of the western and Southern protectorates, up to 1923 the form of transmission system established was limited in scope and needed for linking administrative offices for ease of colonial governance. It was mainly physical and wire system. The Post and Telegraph Department took vital steps at growing a national transmission network when in 1923 the first trunk telephone service was established between Itu and Calabar.[2] In 1946, the post and telegraph begun more purposeful development of the national network in a move that appeared to have had a slight shift of focus and purpose other than that of telecommunication for governance alone. However, it was not until the 1950s that substantial expansion began with the introduction of Very High Frequency (VHF) radio systems, 116 manual and five automatic telephone exchanges. At Independence in 1960, there were less than 20,000 telephone lines.[3] By 1960 the post and telegraph began to run more by indigenous staff, the management of the establishment began to think of the need for a systematic development of telecommunications infrastructure in Nigeria. The indigenous government through Post and Telegraph then conceived periodic development plans. The national telecommunication plans was to be carried out between 1962 and 1991. However the developmental plans were abandoned in its fourth stage in 1985.

In other to enhance the quality of telecommunications services in Nigeria, the telecommunications arm of the Post and Telegraph Department and

---

[2] O.N. Ofulue, Telecommunications Services in Nigeria in the Seventies - An Overview, being paper presented at Nigerian Society of Engineers National Engineering Conference, Enugu, Nigeria, 4-6 December, 1980 Proceedings.

[3] Ernest Ndukwe, An Overview of the Nigerian Telecommunications Environment, being paper presented at International Telecommunication Union (ITU) Telecom Africa, 2004.

the Nigerian External Telecommunications Limited (NITEL) which previously managed the domestic and external services respectively, were merged in 1984 to a single profit-oriented limited liability company called Nigeria Telecommunication Limited. Under the company, the number of automatic switching centres in Nigeria grew to 227 in July 1986. The national telex network grew also to a total capacity of 12,800 lines with only one international exchange having 1,500 trunks.[4] By this time, the transmission media for toll and trunks included terrestrial microwave, coaxial cable, and domestic satellite[5] But it would appear that more attention was paid to communication with the outside world than the development and enhancement of the internal telecommunications system. The Lanlate (Oyo State) Satellite Earth Station, Nigeria's first international satellite telecommunication gateway, became operational in March 1971 with one antenna (Lanlate 1) tracking the Indian Ocean International Telecommunications Satellite Organization (INTELSAT) satellite. A second antenna called Lanlate II was added in December 1975. This one operates with the Atlantic Ocean satellite. By the end of 1986, the two antennas provided a total 417 circuits, namely 248 in the Atlantic Ocean Region and 169 in the Indian Ocean Region. Another international earth station was built at Kujama in Kaduna State. With these facilities, most of Nigeria's external telecommunications, including telephone, telex, facsimile, and television were by satellite. The Nigeria Domestic Satellite System (DOMSAT) was established in 1975 with a network of six 11-metre earth stations operating on a leased International Telecommunications Satellite Organization[6] satellite transponder. The network was subsequently expanded to comprise three leased transponders each of 36 megahertz

---

[4] L.A. Ogunsola & W.A. Aboyade, Information and Communication Technology in Nigeria: Revolution or Evolution, (2005) 11 (1) J. Soc. Sci OAU Ile-Ife 7.

[5] PC Unchidumo, Dedicated Satellite Communications System and Nigeria Seminar on Satellite Communication Systems for Nigeria, 21st-23rd July,1986.

[6] Organisation founded in 1964 by the telecommunication agencies of 18 nations, including the United States, which proposed the organisation. Intelsat owns communications satellites and the ground stations from which they are controlled, but the transmitting and receiving apparatus in each country is owned by the Intelsat member from that country. The consortium contracted with the U.S. National Aeronautics and Space Administration (NASA) to launch its satellites. The first of these was Early Bird, later renamed Intelsat 1, which was placed in a stationary orbit over the Atlantic Ocean at the Equator in 1965. Within a few years, other members of the Intelsat series were orbited over the Pacific and Indian oceans, establishing a commercial telecommunication system accessible from any place on the surface of the Earth

(MHz), 20 earth stations, a network monitor and control station, and backhaul radio links between the Nigeria Domestic Satellite System earth stations and Nigeria Telecommunication as well as stations of Nigerian Television Authority. The first transponder was allocated for television transmission, while the other two were reserved for telecommunication services.

Records suggest that the electronic digital computer made its first appearance in Nigeria in 1963, in connection with the analysis of the 1962/63 national census data.[7] In the 10 years between 1963 and 1973, the total computer population in the country stood at 20-25, with 6 or so of these being associated with the multinational companies. By 1977 the total number of installations had grown to around 70. It was by this time that many universities, government departments, and parastatals, organisations, including the West African Examinations Council (WAEC), the Joint Admissions and Matriculation Board (JAMB), the defunct National Electric Power Authority (NEPA), the Nigerian Ports Authority (NPA), and the Federal Office of Statistics, as well as many banks and commercial firms, began to show interest in computers.

Up to 1977 there were only three computer vendors in Nigeria. They were ICL, International Business Machines (IBM), and National Cash Register Corporation (NCR),[8] and all three were the local subsidiaries of overseas computer manufacturers dealing almost entirely with mainframes and minicomputers. In 1977, the government introduced the indigenisation policy, which set apart some categories of industrial activity exclusively for participation by Nigerian nationals, while stipulating a minimum of Nigerian interest in others. One of the three original vendors, International Business Machines, did not want to comply with the policy, choosing instead to pull out of the country. The policy produced two other important effects. First, there was an influx of indigenous vendors in the computer business. Secondly, the keener competition in the industry led to more aggressive marketing policies. As a result, the number of computer installations in the country rose sharply. Whereas 39 computers were

---

[7] O Longe, Computer Education in Nigeria [1980] 1(1) *Computercope* 38.

[8] American manufacturer of cash registers, computers, and information-processing systems, based in Dayton, Ohio, U.S.

installed in 1975-1977, 1978-1980 witnessed the addition of 197 new installations. There were 149 new installations in 1981-1983, and a further 99 in 1984-1986.[9] Already by the end of 1982, the price of crude oil was beginning to drop sharply in the spot market; and this marked the beginning of the foreign exchange debacle and the attendant import restrictions. The oil industry took the lead in establishing a data network with or without the involvement of Nigeria Telecommunication. Shell Petroleum installed an X-25 packet switched data network between Lagos, Port Harcourt, and Warri using trunk lines leased from Nigeria Telecommunication. On the other hand, the Nigeria National Petroleum Corporation (NNPC) installed a private telecommunication network said to be the largest in Africa[10] The digital network that incorporated 875 km of optical fibre cables, and came under the Integrated Data Services Company, one of the twelve subsidiary limited liability companies established by the Nigeria National Petroleum Corporation in 1988 as part of its new commercialization programme. It is a hybrid network of fibre optic and coaxial cable. The turnkey system interconnects all the vital sites and offices of the Nigeria National Petroleum Corporation, and provides facilities for automatic voice dialling, teleconferencing, and transmission of data, facsimile and telex.

Mobile cellular services (analogue) made their first appearance on the Nigerian market in 1993 with a national service operated by Nigeria telecommunication Limited and a smaller Lagos service operated by Mobile Telecommunications Services (MTS), The two firms, with a joint subscriber base of 12,500, provided voice services over an analogue E-TACS network as well as basic value-added services such as voicemail and paging, from three switches in Lagos, Enugu, and Abuja. However, in 1995, it closed its operations due to failure to pay interconnection charges to Nigeria Telecommunications Limited. M-Tel subsequently emerged as Nigeria Telecommunication Limited's mobile service provider. The Global System for Mobile Communication licensing process was cancelled early in 2000 and the process of auctioning four mobile cellular licenses was reopened in December of that year, after soliciting credible bidders. The winners

---

[9] FO Osuji: Survey of Computer Evolution in Nigeria to Date, 1986, B.Sc., Long Essay Project Report, Department of Computer Science, University of Nigeria, Nsukka.

[10] Tam Fiofori, Lagos Computer and Telecommunications Exhibition, [1988] *Computers in Africa* 2.

who emerged out of this process and settled the agreed licence fees included Econet Wireless Nigeria, Mobile Telephone Networks (MTN) and Communications Nigeria. The new Global System for Mobile Communication licenses were awarded for a period of five years (renewable) and all operators can operate in the 900Mhz and 1800Mhz spectrum bands. Whereas they do provide for a potential upgrading of future networks to general packet radio switching (GPRS), they do not encompass Third Generation (3G) networks, which will probably be auctioned off sometime in the future. Nigeria's digital mobile network has grown significantly since the three companies, awarded the Global System for Mobile Communications license in January 2001, began operating in August 2001.

Another area of development in the communications of information alongside the post and telegraph is the radio and television broadcasting system. Radio broadcasting was introduced into Nigeria as a form of distribution system in 1933. The Post & Telegraph received and re-transmitted via the wire system of British Broadcasting Corporation News, which was later called Radio Diffusion system[11]. In 1939, a station was opened in Ibadan, Kano Station was commissioned in 1944 while between 1945 to 1949 relay stations had been opened in towns like Kaduna, Enugu, Abeokuta, Ijebu-Ode, Jos, Zaria, Calabar and Port-Harcourt.

The Nigerian Broadcasting Services (NBS) which was established on April 1, 1951, later transformed into the Nigerian Broadcasting Corporation (NBC) under the Nigeria Broadcasting Corporation Act No. 39 of 1956. By 1st January, 1962, Voice of Nigeria (VON) was launched as the International Service of Radio Nigeria covering West Africa, East Central & Southern Africa, North Africa & other parts of the world. Voice of Nigeria was later excised from Radio Nigeria on January 5, 1990. The 1st Frequency Modulation (FM) in Nigeria was commissioned on April 22, 1977. It was known then as Radio Nigeria 2 (now Metro FM). A year later when Nigeria Broadcasting Corporation was reorganised, the state stations were handed over to State Governments. Nigeria Broadcasting Corporation was left with only Lagos, Ibadan, Enugu & Kaduna which became Federal Radio Corporation of Nigeria (FRCN). In 2000, the F.R.C.N. was directed by the Federal Government of Nigeria to operate stations at various State capitals.

---

[11] S. Okpanachi: Radio Development: The Case of Radio Nigeria, being a paper presentation at the 2008 Commonwealth Broadcasting Association Conference, Nassau-Bahamas Jan. 23-26, 2008, 3

The partial commercialisation of Federal Radio Corporation of Nigeria (FRCN) was in 1992. Act no. 38 of 1992 gave birth to National Broadcasting Commission, which regulates broadcasting in Nigeria. With the deregulation of broadcasting in Nigeria, Federal Radio Corporation of Nigeria ceased to benefit from the monopoly of radio broadcasting; giving room for quality programming and value for money. At my last count, there are more than 100 Radio Stations now operating in Nigeria. The only challenge is that the commercial radio stations are concentrated in the urban cities with the exception of Federal Radio Corporation Of Nigeria 32 Frequent Module Project which was established as a grass-root/community Radio.

Television broadcasting on the other hand, evolved as a response to nationalism. Following the refusal of Colonial Governor, John McPherson to allow Obafemi Awolowo, the then Premier of Western Region, a right of reply on the government controlled Nigerian Broadcasting Service; the Western Nigeria Broadcasting Corporation (WNBC) was set up in 1959, becoming the first in Africa. This station produced immediate reaction from the Eastern and Northern Regions. Eastern Nigeria Television (ENTV) followed in 1960 while Radio Kaduna Television (RKTV) took off in 1962. The Federal Government in response initiated moves in 1962 to establish the Nigeria Television Service (NTS) with National Broadcasting Company International (NBC) United States of America as managing partners. This followed the enactment of Wireless-Telegraphy Act, No. 31 of 1961. This Act however only authenticated the already established regional stations. With it, both Regions/State and Federal Government could establish and run broadcast station on appropriate licensees from the Federal Ministry of Communication. The ministry was by this act charge with the allocation of wave length, regulating output and station location and ensuring compliance in line with International Telecommunication Convention. The federal government in April 1976 annexed state-owned television systems which were then about 19. This was to stem their proliferation, make for increase central coordination and enhance programme exchange and networking as well as promoting unity. The first network programme was telecasted on April 1, 1976, from Nigeria Broadcasting Corporation television station in Lagos. Nigeria television was later established in 1977 through its enabling Act No. 24 of 1977.

As result of the emerging trends in development of the communication technology over the years, the Federal Government has from time to time taken a stand on some specific Information and Communication Technology

(ICT) issues. In the late 1970s the federal government set up a committee known as the Central Computer Committee, charged with the task of assembling available national data on computing. The committee was expected to develop standards for users, vendors, and consultants on computer projects as well as to develop inputs for a national policy on computing. As this was a period of import restrictions, the committee had the additional function of reviewing all applications for the importation of computers and making recommendations to the Ministry of Finance for the grant of import licenses. The latter function tended to dominate the activities of the committee. But with the advent of import deregulation, the committee went moribund. Even though it has been suggested that the committee succeeded in making recommendations for a computer policy, it appears that its recommendations do not see the light of day, nor were there any apparent policy action stemming therefrom.[12]

In 1986, an advisory panel that was set up by the Minister for Science and Technology to discuss micro-electronics development in Nigeria made a number of far-reaching recommendations, which included:

(i) A programme of short-term activity directed towards the development, design, and fabrication of prototypes of microprocessor-based systems;

(ii) The creation of activity centres for the implementation of the short-term plan;

(iii) The foundation of a Technology Development Centre;

(iv) The formation of a national committee on high-technology microelectronics.

The need to attract investment to develop our national Information and Communication Technology infrastructure led to policy and institutional reforms leading to liberalisation of the telecommunication sector. This reform gave birth to the Nigerian Communication Act.[13] It subsequently provided for the establishment of a regulatory body, the Nigerian Communications Commission (NCC) in 1992.

---

[12] I.K.I Omakwu, Nigeria and Computer Policy, being paper delivered at an international conference on programming, CAN, 1985.

[13] Act No. 75, 1992 as amended by Act No. 30, 1998

Contemporary Issues and Challenges

Unlawful Use of Information and Communications Technology

Unlawful use of information and communications technology is usually manifested through the abuse of its usage which is commonly referred to computer crimes. Computer crime can broadly be defined as criminal activity involving an information technology infrastructure; including illegal access or unauthorised access; illegal interception that involves technical means of non-public transmissions of computer data to, from or within a computer system; data interference that include unauthorised damaging, deletion, deterioration, alteration or suppression of computer data; systems interference that is interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data; misuse of devices, forgery (identity theft), and electronic fraud.[14] The advent of digital technology gave birth to modern communication hard-wares, international network service and powerful computer systems to process data.[15] Hence, cyberspace has provided a safe haven for international network platform, which has created geometric growth and accelerated windows of opportunities for businesses and the removal of economic barriers hitherto faced by nations of the world. People from diverse areas of human endeavour can now freely access and utilise the advantages offered by international network platform. Computer crimes encompass a broad range of potentially illegal activities. Generally it may be categorise into two major groups: (1) crimes that target computer networks or devices directly; (2) crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device.

Privacy and Data Intrusion

About hundred years ago, a reasonable level of privacy existed because the state of technology was such that provided little opportunities for the invasion of privacy. But with the invention of photography in the late 19th century, privacy began to be threatened. It has been suggested that the first publication advocating privacy in

---

[14] Paul Taylor, Hackers: Crime in the Digital Sublime, Routledge, 1999, 200.

[15] RS Hunda, K. Singh & MD Singh (2004), Aspects to Ensure Admissibility of Digital Evidence (2004) 13 Law Journal Guru Nanak dev University Amritsar 1.

the United States written by Samuel Warren and Louis Brandeis,[16] was largely in response to the increase in newspapers and photographs made possible by printing technologies

Prior to the so called information revolution, information and data held on individuals would only be kept in the traditional filing cabinet or their equivalent. Only the holder of the data, or others whom he grants access could see it. But the case with which computer can store and manipulate data has change all of that. Even as rules being formulated and developed to deal with the issues raised, the nature of the threat was undergoing a subtle change as the technology continued to progress. In the 1970s and early 1980s, the focus was on the development of large, centralized database held on mainframe computer. Technological advancement abruptly changed directions and instead of larger machine been developed, the advent of the micro-computer results in computer rapidly becoming a common tool both at work and in the home rather than being confined to large institution. Furthermore, the creation of computer network on a large global scale[17] moved the emphasis form centralized system to increasingly decentralized systems typified by International network and World Wide Web. These gives rise to qualitative different problems. Presently, it is almost impossible to use the international network without being confronted with privacy invading feature which carry out all kinds of processing of operation of personal data that are invisible to the data subject. In other words, the international network user is not aware of the fact that his personal data are collected and processed, may be for purposes unknown to the user. An example of this is called cookie which can be defined as a computer record of information that is sent from a web server to a user's computer for the purpose of future identification of that computer on future visit to the website. As technology advances, the way in which

---

[16] S. Warren & L. Brandeis, The Right to Privacy (1890) 4 Harvard L.R. 193. In their view, privacy is the right to be left alone, a thing instantaneous photograph and newspaper enterprises evades by threatening to make good thing whispered in the closet proclaimed to the roof tops. A similar view was expressed by David Flaherty. See D Flaherty, Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States, Chapel Hill: Univ. of North Carolina Press, 1989.

[17] Computer network actually had their genesis in the 1960s with the creation of the APRANET but it was not until the mid-1980s that the interest began to be used on a regular day to day basis outside the research community.

privacy is protected and violated also changes. The increased ability to share information can lead to new ways in which privacy can be breached either by government or private persons. New technologies can also create new ways to gather private information.

The relationships between data protection and privacy have not always been easy to reconcile. Data protection is often viewed as technical, relating to specific information practices. Thus, it is defined as the legal protection of individuals with regard to automatic processing of information.[18]

In contrast, privacy is more likely to be considered a right.[19] Westin[20] suggested that privacy is the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated. Alan Gotlieb describes privacy as this:

in the privacy domain, there may be found the desire to be left alone, to be left in peace by the rest of the community which means the availability of sufficient space to provide protection from the dictate of one's neighbour, to die alone if he so wished, to rest outside the society, to be non-productive, to be off-beat, to be alone if one desired, to turn off connection. It may involve respect for one's anonymity in a public place, being able to establish intimate relationship.[21]

In Nigeria, the right of privacy is provided in Chapter IV, section 37 of the 1999 Constitution. It declares that, "the privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications is hereby guaranteed and protected."

Even though there does not appear to be an explicit privacy protection in the Constitution of the United States, the Supreme Court of the United States in Griswold v. Connecticut (1965) found that other guarantees have "penumbras" that implicitly grant a right to privacy against government intrusion.[22] The Fourth Amendment explicitly state that the

---

[18] Convention for the Protection of Individual with regard to Automotive Processing of Personal Data, Strasbourg, 28, Jan, 1981

[19] For example, s. 33, 1999 Constitution of the Federal Republic of Nigeria

[20] AF Westin, Privacy and Freedom, London: Bodleyhead, 1967, 14

[21] A Gotlieb, Computers, Privacy And Freedom of Information, Kingston, 1. See also Encyclopaedia of Information Technology Law, London: Sweet & Maxwell, (Vol.2), 1990, 1606.

[22] NAACP v. Alabama 3357 U.S 449 at 469 78, (S.C.T 1958). See also Katz v US 18 USC 2518-1519

right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures. The Fifth Amendment self incrimination clause permits citizens to create a zone of privacy that government may not force a person to surrender his detriment.

The right enjoys further protection by legislation in Nigeria. For example, Section 10(b) Wireless and Telegraphy Act provides that no staff in the course of his duty as a servant of the state either-

(a) Use any wireless telegraphy apparatus with intent to obtain information as to the contents, sender or addressee of any message(whether sent by any means wireless telegraphy or not) which neither the person using the apparatus or any person on whose behalf it is acting is authorized by the commission to receive; or

(b) Except in the course of legal proceeding or for the purpose of any report thereof, disclose any information as to the content sender or addressee of any such message being information which would not have come to his knowledge but for the use of wireless telegraphy apparatus by or by another person.

The above section23 equally adds that any person who contravenes the provision of this subsection shall be guilty of an offence. Section 23, of the Nigeria Communication Commission Act, 2003 on its own part state that state that a person who is or has been an employee of a licensee or authorised carrier shall not:

(c) By means of telecommunication equipment or facilities send or attempt to send any messaging which to his knowledge is false or to his knowledge likely to prejudice the efficiency of any service or endanger the safety of any person except under the authority of a minister or in the course of legal proceedings or for the purpose of a report thereof, disclose any information as it relates to contents, sender or addressee of any such messages, being information which would not have come to his knowledge, but for the use of telecommunications equipment or facilities by him or another person.

---

23 ibid

Cybercrime

Cybercrime is an amorphous field. It refers broadly to any criminal activity that pertains to or is committed through the use of the international network.[24] A wide variety of conduct fits within this capacious definition, Cybercrime is a broad term covering all the ways in which computers and other types of portable electronic devices such as cell phones and portable devices capable of connecting to the international network are used to break laws and cause harm. A slightly more technical definition would be use of computers or other electronic devices via information systems such as organisational networks or the international network to facilitate illegal behaviours.[25]

Threats and Stalking

This is the tracking and the follow-up of individuals especially celebrities and giving update report as to their locations. Unfortunately, the international network makes it much easier to learn about other people, track their activities, and threaten them. Example of this form misuse of Information and Communication Technology is seen in The Nuremberg Files website. The Nuremberg Files website http://www.christiangallery.com/atrocity/ was operated by anti-abortion activists. It displayed the names, home addresses, license-plate numbers, and pictures of individual abortion doctors along with the names of their spouses and children. If the abortion doctors profiled on the Nuremberg Files website were killed by anti-abortionists, the website would put a black line through the name of the doctor; if they were wounded, the website would put a gray line through the name of the doctor. After the abortion doctors brought suit against the anti-abortionist organization which operated the website, the district Court found that the defendants had "acted with specific intent and malice in a blatant and illegal communication of true threats to kill, assault, or do bodily harm to each of the plaintiffs and with the specific intent to interfere with or intimidate the plaintiffs from engaging in legal medical practices and procedures."[26]

---

[24] Zittrain (et al), International Network Laws, Fountain Press, 2009, 1

[25] S McQuade, Understanding and Managing Cybercrime, Boston, MA: Allyn & Bacon, 2006, 16

[26] Planned Parenthood of the Columbia/Willamette, Inc. v. American Coalition of Life Activists, 41 F.Supp.2d 1130, 1154 (D.Or. 1999)

Accordingly, the district Court issued a permanent injunction against the defendants from operating the website and a jury awarded the abortion doctors approximately $107 million in compensatory and punitive damages.

In United States, the primary federal statute used to prosecute international network fraud is the Computer Fraud and Abuse Act of 1986. Section 18 provides that:

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretences, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than five years, or both. If the violation affects a financial institution, such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.

Nigeria is yet to respond with a cyber crime specific legislation. Generally, the Criminal Code and the Economic and Financial Crimes Commission (Establishment) Act have been the main instruments used to fight ICT crimes. This is so because it is easy to pigeonhole most of ICT crimes within the square of economic crimes. Economic crime is defined by the Act as:

> the non-violent criminal and illicit activity committed with the objectives of earning wealth illegally either individually or in a group or organized manner thereby violating existing legislation governing the economic activities of government and its administration to includes any form of fraud, narcotic drug trafficking, money laundering embezzlement, bribery, looting and any form of corrupt malpractices, illegal arms deal, smuggling, human trafficking and child labour, oil bunkering and illegal mining, tax evasion, foreign exchange malpractices including counterfeiting of currency, theft of intellectual property and piracy, open market abuse dumping of toxic wastes and prohibited goods et cetera.[27]

[27] Section 40, Economic and Financial Crimes Commission (Establishment) Act 2004.

Hacking

This pertained to people gaining unauthorized access into information systems including computer networks. Breaking into a computer system or exceeding network permissions is considered a form of computer trespassing. Computer trespassing also extends to individuals who exceed their authorized permissions within a given computer network. Originally, however, beginning in the late 1950s, a "hack" was a slang word first used by students of the Massachusetts Institute of Technology (MIT) to refer to "a clever, benign, and ethical prank or practical joke, which is both challenging for the perpetrators and amusing to the Massachusetts Institute of Technology community". As computer technologies began to be incorporated as part of research programs at Massachusetts Institute of Technology and other universities across the United States, hacking began to include clever and innovative programming. These exploits grew as hackers not only broke into but sometimes took control of government and corporate computer networks. One such criminal was Kevin Mitnick, the first hacker to make the "most wanted list" of the United States Federal Bureau of Investigation (FBI). He allegedly broke into the North American Aerospace Defense Command (NORAD) computer in 1981, when he was 17 years old, a feat that brought to the fore the gravity of the threat posed by such security breaches. Concern with hacking contributed first to an overhaul of federal sentencing in the United States, with the 1984 Comprehensive Crime Control Act and then with the Computer Fraud and Abuse Act of 1986.

A hacker may gain access remotely using a computer in his own home or office connected to a telecom network. The vast majority of hacking activities have been relatively harmless and sometimes, the hacker leave a message publicizing his feat and this reflect the popular image of a hacker. In R V. Gold [1988] 2 All ER 18628 two computer hackers gained access into the British Telecom Prestel Gold computer network without permission and altered data. One of the accused also got into the Duke of Edinburgh's personal computer files and left the message "good afternoon H.R.H Duke of Edinburgh". The two accused were journalist who claimed that they had hacked into the network in order to highlight the deficiencies in its security. The English Court of appeal held that the acts of the accused in gaining access to the telecom gold files do not amount to dishonesty.

---

[28] R V. Gold [1988] 2 All ER 186, 2 WLR 984

Computer viruses and worms

Both worms and viruses are malicious programs which are propagated uncontrollably over the international network. A worm program is designed to invade a computer and replicate itself by sending the worm to other computers on a network or in the user's address book. Worms cause damage by clogging up computer networks, slowing down or even crippling individual computers and shared servers. Unlike worms, which do nothing but replicate themselves, viruses both replicate themselves and carry malicious payload? This malicious payload may be a program which immediately corrupts or deletes data on the infected machine. Virus may unleash a "logic bomb" which lies dormant on the machine and destroys data when the infected computer's clock reaches a certain date. In the past, viruses and worms were spread through floppy disks and infected macro attachments to common files like Microsoft Word documents. Today, many viruses and worms are spread through electronic mail and activated when the user opens an e-mail attachment. A "Trojan horse" is an electronic mail attachment that appears benign. When the user opens the Trojan horse, however, a hidden worm or virus is activated that can damage the user's computer and send itself to other computers on the user's network. The deliberate release of damaging computer viruses is yet another type of computer sabotage.

Conviction under the United States Computer Fraud and Abuse Act of 1986 was first secured under this head. On November 2, 1988, a computer science student at Cornell University named Robert Morris released a software "worm" onto the international network from Massachusetts Institute of Technology. The worm was an experimental self-propagating and replicating computer program that took advantage of flaws in certain electronic mail protocols. Due to a mistake in its programming, rather than just sending copies of itself to other computers, this software kept replicating itself on each infected system, filling all the available computer memory. Before a fix was found, the worm had brought some 6,000 computers (one-tenth of the Internet) to a halt.

Denial of Service Attacks

These are attacks that are aim at crippling a website or network especially the one that provides services. This when occurred when 15-year-old Canadian hacker, orchestrated a series of "denial of service" attacks (DoS) against several e-commerce sites, including Amazon.com and eBay.com. These attacks used computers at multiple locations to overwhelm the

vendors' computers and shut down their World Wide Web sites to legitimate commercial traffic. Under the Computer Misuse Act of United Kingdom, 1990, the offence of computer and network sabotage punishes three categories;
(i) Unauthorised access to computer material (that is, a program or data).
(ii) Unauthorised access to a computer system with intent to commit or facilitate the commission of a serious crime.
(iii) Unauthorised modification of computer material
Let us use the three categories to navigate legal (criminal law) response to ICT crimes as possible pointer to how our law should develop responses.

(i) Unauthorised Access

Unauthorised access is a basic hacking offence. Commission of the offence requires the actus reus of causing a computer to perform any function. Some form of interaction with the computer is required, but actual access does not need to be achieved. This broad formulation means that simply turning on a computer could constitute the necessary act. Under the Act, hacking does not only cover computer but extends to everyday domestic appliances and cars that incorporate computer technology. This position is also adopted in other jurisdiction such as France and Germany. One major exception to this approach is in the United States, where the Computer Fraud and Abuse Act contain the following definition: "An electronic, magnetic, optical, electrochemical or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."[29]

The mens rea of this access comprises of two elements. First, there must be intent to secure access to any program or data held by the computer. Secondly, the person must know at the time that he commits the actus reus that the access he intends to secure is unauthorized. The intent does not have to be direct any particular program

There could be problem in proving that the hacker knew that is access was

---

[29] 18 USC, Section 1030(e)(1) as amended in 1996

unauthorized. In Oxford v Moss[30] it was held that hacking of the examination paper could not be theft because there was no intention to deprive owner of it permanently. For this reason a hacker who simply reads or copies information has not committed theft. However if a hacker goes further and not only make a copy of the information but then immediately after goes on to erase the original from the computer system, this is more likely to be regarded as theft.

But under the US Computer Fraud and Abuse Act,[31] merely accessing and obtaining information from a "protected computer" can lead to liability.

ii. Intent to Commit Further Offences

Some hacking activities could give rise to some nefarious act and also the unauthorized access with intent to commit or facilitate the commission of further offences. In R v. Whiteley[32] the accused gained unauthorised access to the Joint Academic Network (JANET) and gave himself the status of a System Manager. He deleted and added files, changed password and deleted audit files recording his activities. He was very skilled and even made a special program inserted to trap him. In the cases of R v. Strickland and R v Woods,[33] the first classic hackers were jailed six months for conspiracy to commit offences under Sections 1 and 2 of The Computer Misuse Act 1990. The defendant activities were said to have caused damage, valued at £123,000, to computer systems ranging from the Polytechnic of Central London to National Space Agency. In passing the judgment the judge said: "There may be people out there who consider hacking to be harmless, but hacking is not harmless. Computers now from a central role in our lives, containing personal details... It is essential that the integrity of those systems should be protected and hacking puts that integrity into jeopardy."

In *United States v. Ivanov*[34], Ivanov hacked into a Connecticut e-commerce company's computers and obtained credit card numbers of its customers. Ivanov then contacted the company and threatened to damage the

---

[30] (1978) 68 Cr. App R 183

[31] 18 USC 1030(a)(1) which protect national security information

[32] (1991) 93 Cr. App 381,

[33] (1993), the Southwark Crown Court

[34] 175 F.Supp.2d 367, 368-69 (D.Conn 2001).

company's computers unless he was paid $10,000. Prosecutors charged Ivanov for accessing a computer without authorisation with the intent to defraud and for threatening to cause damage to a protected computer with intent to extort something of value. The Court found that Ivanov's access was unauthorised and that he had obtained something of value - the credit card numbers. If Ivanov had merely viewed the information and not taken the credit card numbers, however, he probably would not have obtained something of value and the charge would have been dismissed.

iii. Unauthorised modification

The third substantive offence under the (English) Computer Misuse Act is that of unauthorised modification of computer material. A person is guilty of the offence if he does any act which caused an unauthorised modification of the contents of the computer. In North Tex. Preventive Imaging, L.L.C. v. Eisenberg, M.D.,[35] The software manufacturer sent an "update" floppy disk to the medical company secretly containing a time bomb to disable the software after a certain date, which the company unwittingly installed. When the company found the time bomb, they sued the software manufacturer claiming that the time bomb had accessed their computers without authorisation and damaged their computers. The question of authorisation was contentious because the plaintiff's own employees had installed the defendant's time bomb, so the defendant had not directly accessed the plaintiff's computers without authorisation. But in United States v. Drew[36], Drew was convicted of sending large quantities of electronic mails to his former employer's server in order to damage his employer's computer systems.
Apart from the above categories, computer and network sabotage can occur also occur under the following circumstance.

a. Authorized Access for an Unauthorized Purpose.

An employee may have authorization to use a computer system as a normal part of his duty to his employer. If the employee subsequently uses the system for an unauthorised purpose, for example in Sawyer v. Dept. of Air Force,[37] Sawyer was a government programmer who altered Air Force computer contracts in order to improperly disburse $17,738 to himself. The

---

[35] 1996 WL 1359212 at *1-4 (C.D. Cal. Aug. 19, 1996).

[36] 27 Fed.Appx.164 (4th Cir. 2001), on appeal.

[37] 31 M.S.P.R. 193, 194-195 (Merit Sys. Protection Bd. 1986)

agency fired Sawyer claiming that Sawyer had accessed and altered the accounts payable system without authorization. Rejecting Sawyer's claim that he was trying to point out security deficiencies in the accounts payable system, the Merit Systems Protection Board affirmed, finding that Sawyer's access was unauthorized.

b. Exceeding Authorised Access

In the criminal case United States v. Czubinski38, an Internal Revenue Service employee was found to have exceeded his authorised access to the Service database of taxpayer records. He looked at taxpayer records of people ranging from a woman he had dated a few times to the assistant district attorney who was prosecuting his father on an unrelated charge. In finding that Czubinski had exceeded his authorised access, the court adopted his organisation's internal rules as a benchmark, noting that Czubinski had "knowingly disregarded the Service rules by observing the confidential information he accessed." The charges ultimately failed, however, because the prosecutors could not prove Czubinski had the necessary fraudulent intent or had obtained something of value in merely viewing the records.

Conclusion

From the above analysis, it is trite that there are several novel issues that came with the spiral development in ICT. The challenge now is how to fashion ways of upgrading our laws to meet these novel challenges posed by this development. It is obvious that the traditional tort and contract law are inadequate to cope with the challenges. Apart from crimes in the main, the concept of privacy has grown beyond the traditional conception of the law. There are also regulatory issues and challenges that are unaddressed by the Communications Act of 2004. I suggest that law reform in all of these areas should take clues from reforms in advanced jurisdictions. This will help in maintaining the sanity of the system as well as help to curb crimes.

---

38 106 F.3d 1069, 1072 (1st Cir. 1997)