Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Version 21 August 2009
[Reformat in April 2011]

Cybercrime legislation – country profile

NIGERIA

This profile has been prepared within the framework of the Council of Europe's capacity building projects on cybercrime in view of sharing information and assessing the current state of implementation of the Convention on Cybercrime under domestic legislation. It does not necessarily reflect official positions of the country covered or of the Council of Europe.

Comments may be sent to:

Economic Crime Division
Directorate General of Human Rights and Legal Affairs
Council of Europe, Strasbourg, France

Tel: *+33-3-9021-4506*
Fax: *+33-3-9021-5650*
Email: *alexander.seger@coe.int*
www.coe.int/cybercrime

Country:	**Nigeria**
Signature of Convention:	No
Ratification/accession:	No
Provisions of the Convention	***Corresponding provisions/solutions in national legislation*** *(pls quote or summarise briefly; pls attach relevant extracts as an appendix)*
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs	**The Advance Fee Fraud and other Fraud Related Offences Act(2006)** While there is no definition section in this law, **Part 2 (sections 12 and 13) of the Act** make provisions for Electronic and Telecommunications Offences uses terms like "electronic communication service" or "remote computing service either by e-mail" or any other form.

automatic processing of data; b “computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function*;* c “service provider” means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d “traffic data” means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service	And mentions ‘Service Provider’ as “any person or entity who in the normal course of business provides telecommunications or internet services or is the owner or person in the management of any premises being used as a telephone or internet cafe or by whatever name called.” Also, the Act describes as a Service Provider any person whose normal course of business involves the provision of non-fixed line or Global System of Mobile Communications (GSM) services or is in the management of any such services. **<u>Cybersecurity bill 2008</u>** 38. In this Bill, **“Access”** includes to gain entry to, instruct, make use of any resources of a computer, computer system or network. **“Agency”** means Cyber Security and Data Protection Agency. **“Authorized officer”** means a person authorized by law to exercise a power this Bill **“Authority”** means express or implied consent to access a computer network, program, data or database, software. **“Computer”** includes any electronic device or computational machinery programmed instruction which has the capabilities of storage, retrieval memory, logic, arithmetic or communication and includes all input, output, processing, storage, communication facilities which are connected or related to such a device in a system or network or control of functions by the manipulation of signals whether electronic, magnetic or optical. **“computer network”** includes the interconnection of computers or computer system **“Computer program”** means data or a set of instructions or statements that when executed in a computer causes computer to perform function.

“damage” means an impairment to the integrity or availability of data, program or network.

“data” includes a representation of information, knowledge, facts, concepts or instructions intended to be processed, being processed or has been processed in a network.

“database name” includes any designation or name registered with the domain registrar as part of an electronic address.

“intellectual property rights” include any right conferred or granted under any of the following laws or treaties to which Nigeria is a signatory:
(a) Copyright Act, CAP 68. LFN (as amended);
(b) Patents and Designs Act CAP 344, LFN;
(c) Trade Marks Act, CAP LFN;
(d) Berne Connection;
(e) World Intellectual Property Organization (WIPO) Treaty;
(f) Trade-Related Aspects of Intellectual Property Rights (TRIPs);
(g) Universal Copyright Convention (UCC); and
(h) Paria Convention (Lisbon Text).

“internet” means global information system linked by a unique address space base on the internet protocol or its subsequent extensions.

“intercept” includes the aural or acquisition of the contents of any wire, electronic or oral communication through the use of technical means so as to make some or all the contents of a communication available to a person other than whom it was intended, and includes;
(a) monitoring of such communication by any device;
(b)viewing, examination or inspection of the contents of any communication; and
(c) diversion of any communication from its intended destination.

“Law enforcement” agency means any institution created by law and charged with the responsibility of enforcing obedience to our written law.

“loss” means any reasonable lost to a victim, including the cost of responding

	to an offence, conducting a damage assessment and restoring the data, program, system or information to its condition prior to the offences and any revenue lost, cost incurred and other consequential damages incurred because of the interruption of service. **“Minor”** means a person under 18 years. **“Modification”** means (a)alteration or erasure of the content of any program, data and data base; (b) any event which occurs to impair the normal operation of a computer (c) modification is unauthorized if: (i) the person that causes the act is not himself entitled to determine whether the modification should be made; and (ii) he does not have consent from anybody to modify. **“Service provider”** includes but not limited to; (a) internet service provider; (b) communications service provide; and (c) application service provider. **“Software”** includes any program, data, database, procedure and associated documentation concerned with the operation of a computer system. **“Spamming”** means unsolicited electronic mail message having false headers, address and lines. **“Minister”** means minister of information and communication.
Chapter II – Measures to be taken at the national level ***Section 1 – Substantive criminal law***	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or	**<u>Cybersecurity bill 2008</u>** 7. (1) Any person who without authority or in excess of his authority accesses any computer for the purpose of: (a) securing access to any program; or (b) data held in that computer; or

other dishonest intent, or in relation to a computer system that is connected to another computer system.	(c) committing any act which constitute an offence under any law for time being in force in Nigeria, commits an offence and shall be liable on conviction: (i) in the case of offence in paragraph (a) of this subsection, to a fine of not less than N10,000 or imprisonment for a term of not less than 6 months or to both such fine and imprisonment. (ii) For the offence in paragraph (b), to a fine of not less N100,000 or a term of not less than 1 year or to both such fine and imprisonment. (2) Where damage or loss is caused to any computer as a result of the commission of an offence under subsection (1) of this section, the offender shall be liable to a fine of not less than N1,000,000 or imprisonment for a term of not less than 5 years or to both such fine and imprisonment. (3) In pronouncing sentence under this section, the court shall have regard to the extent of damage or loss occasioned by the unlawful act. 14. Any person who with the intent to deceive or defraud, accesses any computer or network and uses or assumes the identity of another person, commits an offence and shall be liable on conviction to a fine of not less than N500,000 or imprisonment for a term of not less than 3 years or to both such fine and imprisonment.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	**Cybersecurity bill 2008** 16.(1) A person who intentionally, without authority or in excess of authority intercepts any communication originated, terminated or directed from, at or to any equipment, facilities or services in Nigeria, commits an offence and shall be liable on conviction to; - a fine of not less than N500,000; - imprisonment for a term of not less than 10 years; or - both such fine and imprisonment. (2) Notwithstanding the provision of subsection (1) of this section, any service provider, its employee or duly authorized agent may, in the normal course of work, carryout the activity mentioned in section 16 of this Bill.

Article 4 – Data interference 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**<u>Cybersecurity bill 2008</u>** 11. (1) Any person who without authority or in excess of authority interferes with any computer network in such a manner as to cause any data or program or software held in any computer within the network to be modified, damaged, suppressed, destroyed, deteriorated or otherwise rendered ineffective, commits an offence and shall be liable on conviction to a fine of not less than N1,000,000 or imprisonment for a term of not less than 5 years or to both such fine and imprisonment.
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	**<u>Cybersecurity bill 2008</u>** 13. Any person who without authority or in excess of authority intentionally interferes with access to any computer or network so as prevent any: (a) part of the computer from functioning; or (b) denying or partially denying any legitimate user of any service of such computer or network; commits an offence and shall be liable on conviction to a fine of not less than N2,000,000 or imprisonment for a term of not less than 7 years or to both such fine and imprisonment. 9. (3) Any person spamming electronic mail messages to receipts with whom he has no previous commercial or transactional relationship commits an offence and shall be liable on conviction to a fine not less than N500,000 or imprisonment for a term of not less than 3 years or to both such fine and imprisonment. (4) Any person who with intent to commit any offence under this Bill; (a) uses any automated means, device; or (b) any computer program, software; to collect or store electronic mail addresses from any sources whatsoever, commits an offence and shall be liable on conviction to a fine not less than N1,000,000 or to imprisonment for a term not below 5 years or both such fine and imprisonment.
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:	**<u>Cybersecurity bill 2008</u>** 12. Any person who unlawfully produces, adapts or procures for use, distributes, offers for sale, possesses or uses any devices, including a computer program or

a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	a component or performs any of those acts relating to a password, access code or any other similar kind of data, which is designed primarily to overcome security measures with the intent that the devices be utilized for the purpose of violating any provision of this Bill, commits an offence and is liable to a fine of not less than N1,000,000 or imprisonment for a term of not less than 5 years or to both such fine and imprisonment. 8. (1) Any person who, knowingly and without authority or in excess of authority, disclose any: (a) password; (b) access code; or (c) any other means of gaining access to any program data or database held in any computer for any unlawful purpose or gain, commits an offence and shall be liable on conviction to a fine of not less than N500,000 or to imprisonment for a term of not less than 3 years or to both such find and imprisonment, and in the case of a second or subsequent conviction, to a fine not exceeding N1,000,000 or to imprisonment for a term of not less than 5 years or both such fine and imprisonment. (2) Where the offence under subsection (1) results in damage or loss, the offender shall be liable to a fine of not less than N1,000,000 or imprisonment for a term of not less than 5years or both such fine and imprisonment. (3) Any person who with intent to commit any offence under this Act uses any automated means or device or any computer program or software to: (a) retrieve; (b) collect; and (c) store password, access code; or any means of gaining access to any program, date or database held in any computer, commits an offence and shall be liable on conviction to a fine of N1,000,000 or to imprisonment for a term of 5 years or to both such fine and imprisonment.
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be	**Cybersecurity bill 2008**

necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	10. (2) Any person who knowingly accesses any computer and inputs, alters, deletes or suppresses any data resulting in unauthentic data with the intention that such inauthentic data be considered or acted upon as if it were authentic or genuine, whether or not such data is readable or intelligible, commits an offence and shall be liable on conviction to a fine of not less than N500,000 or imprisonment for a term of not less than 3 years or both such fine and imprisonment.
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**Cybersecurity bill 2008** 9. (1) Any person who with intent to defraud send electronic mail message to a recipient, where such electronic mail message materially misrepresents any fact or set of facts upon which reliance the recipient or another person is caused to suffer any damage or loss, commits an offence and shall be liable on conviction to a fine of not less than 5 years or to both such fine and imprisonments. (2) It shall not operate as a defense for any person charged with an offence under subsection (1) of this section to claim that: (a) he could not have carried out his intended act; or (b) it is impossible to execute the ultimate purpose of his intention; or (c) the object of his deceit is non-existent. 10. (3) Any person who knowingly and without right causes any loss of property to another by altering, erasing, inputting or suppressing any data held in any computer for the purpose of conferring any benefits whether for himself or another person, commits an offence and shall be liable on conviction to a fine of not less than N500,000 or imprisonment for a term of not less than 3 years or both such fine and imprisonment.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution	**Cybersecurity bill 2008** 22. Any person who use any computer to: (a) engage or solicits or entices or compels any minor in any sexual or related act; or

through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 3 For the purpose of paragraph 2 above, the term “minor” shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	(b) engage in, or facilitates any indecent exposure of a minor or creates, possesses or distributes child pornography; or (c) facilitates the commission of a sexual or related act which constitutes an offence under any law for the time being in force in Nigeria, commits an offence and shall be liable on conviction: (i) in case of paragraph (a), to a time of not less than N3,000,000 or imprisonment for a term of not less than 7 years or to both such fine and imprisonment. (ii) in case of paragraph (b, and (c), to a fine of not less than N1,000,000 or imprisonment for a term of not less than 5 years or both such fine and imprisonment. **Child Rights Act** **Structure and Content of the Child’s Right Act** The structure of the ***Child’s Rights Act 2003*** **(CRA)** has been informed by the mandate to provide a legislation which incorporates all the rights and responsibilities of children, and which consolidates all laws relating to children into one single legislation, as well as specifying the duties and obligations of government, parents and other authorities, organizations and bodies. **Definition of a Child** The Act defines a child as one who is below the age of eighteen years. It categorically provides that such a child’s best interests shall remain paramount in all considerations. A child shall be given such protection and care as is necessary for its well being, retaining the right to survival and development and to a name and registration at birth. **Basic Provisions of the CRA** • Provisions of freedom from discrimination on the grounds of belonging to a particular community or ethnic group, place of origin, sex, religion, the circumstances of birth, disability, deprivation or political opinion; and it is stated categorically that the dignity of the child shall be respected at all times.

	• No Nigerian child shall be subjected to physical, mental or emotional injury, abuse or neglect, maltreatment, torture, inhuman or degrading punishment, attacks on his/her honor or reputation. • Betrothal and marriage of children are prohibited. • Causing tattoos or marks, and female genital mutilation are made punishable offences under the Act; and so also is the exposure to pornographic materials, trafficking of children, their use of narcotic drugs, or the use of children in any criminal activities, abduction and unlawful removal or transfer from lawful custody, and employment of children as domestic helps outside their own home or family environment. . • Buying, selling, hiring or otherwise dealing in children for purpose of begging, hawking, prostitution or for unlawful immoral purposes are made punishable by long terms of imprisonment. Other offences considered grave include sexual abuse, general exploitation which is prejudicial to the welfare of the child, recruitment into the armed forces and the importation/ exposure of children to harmful publications.
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party,	**Section 20 of the Copyright Act states** "any person who makes or causes to be made for sale, hire, or for the purposes of trade or business any infringing copy of work in which copyright subsists, or imports or causes to be imported into Nigeria a copy of any work which if made in Nigeria would be an infringing copy, commits a crime." It also criminalizes the acts of selling, letting for hire, distribution, and possession of "infringing copies" of copyright protected works - Section 20(2) See also, Section 21(2): which states that "Any person who sells, rents, hires or offers for sale, rent or hire, any anti piracy device or imports such device into Nigeria without permission from the Copyright Commission commits an offence." **Cybersecurity bill 2008**

pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	21. Any person who uses any computer to violate any intellectual property rights protected under any law or treaty applicable in Nigeria, commits an offence under this Bill and shall be liable on conviction to a fine of not less than N1,000,000 or imprisonment for a term of not less than 5 years or to both such fine and imprisonment, in addition to any penalty or relief provided under laws.
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	**S.4 of the Criminal Code Act** provides that "When a person, intending to commit an offence, begins to put his intention into execution by means adapted to its fulfilment and manifests his intention by some overt act... constitutes an offence and it is immaterial that the offender has not done all that is material in completing the commission of the offence." Aiding/Abetting: criminalized in the same law at Sections 7-10 of the Criminal Code with varying degrees of punishment.

Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	Several laws exist in Nigeria that imposes civil and criminal liabilities on corporations. For instance, where copyright offences are committed by a body corporate, the body corporate and every person who at the time of the offence was in charge of or responsible to the body corporate for the conduct of its business is deemed to be guilty of the offence and liable to be proceeded against and punished accordingly. **Cybersecurity bill 2008** 23. Any person who: (a) attempts to commit any offence under this Bill; or (b) does any act preparatory to or in furtherance of the commission of an offence under this Bill; and (c) abets or engages in a conspiracy to commit any offence, commits an offence and shall be liable on conviction to the punishment provided for such an offence, under this Bill.
Article 13 – Sanctions and measures 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	Persons found guilty and convicted of crimes in Nigeria are usually subjected to either penal incarceration or fines, or both forms of punishments. For instance, "Any person found guilty of infringing Section 20(1) of the Copyright Act is liable on conviction to a fine of an amount not exceeding N1,000 for every copy dealt with in contravention of the section or to a term of imprisonment not exceeding five years, or to both such fine and imprisonment. There are no probations in the legal system in Nigeria.
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article	**Cybersecurity bill 2008** 31.Notwithstanding anything contained in any enactment or law in Nigeria, an information contained in any computer which is printed out on paper, stored, recorded or copied on any media, shall be deemed to be primary evidence under this Bill.

to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of	**The Constitution of Nigeria is the supreme law of the land. See Section 1(1) of The 1999 Constitution of Nigeria.** **Also in its Chapter Four, it outlines Fundamental Human rights which are safeguarded under the Constitution**. Also, **Section 37 of the Constitution provides for the Fundamental Right to Private and Family Life** stating that 'the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is guaranteed and protected.'

proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	As seen above, under the Constitution no man can be convicted of a crime unless the conduct against which he was prosecuted was prohibited in a written law in which a punishment was also prescribed. Section 37(13) **Cybersecurity bill 2008** 15. (4) Any data retained, processed or retrieved by the service provider for the law enforcement agency under this Bill, shall not be utilized except for legitimate purposes either with the consent of individuals to whom the data applies or if authorized by a court of competent jurisdiction. (5) A person exercising any function under this section shall have due regard to the individual right to privacy under the constitution of the Federal Republic of Nigeria 1999 and shall take appropriate technological and organizational measure to safeguard the confidentiality of the data retained, processed or retrieved for the purpose of law enforcement. (6) A person or service provider, body corporate who willfully contravenes the provisions of this section commits an offence and shall be liable on conviction to a fine of not less than N500,000 or imprisonment for a term not less than 3 years or both fine and imprisonment.
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently	**Cybersecurity bill 2008** 15. (1) Every service provider shall keep all traffic, subscriber information or any specific content on its computer or network for such period of time as the Agency may require. (2) Every service provider shall, at the request of any law enforcement agency: (a) provide the law enforcement agency with any traffic of subscriber information required to be kept under subsection (1) of this section; or (b) preserve, hold or retain any related content.

renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party’s competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Cybersecurity bill 2008** 15. (1) Every service provider shall keep all traffic, subscriber information or any specific content on its computer or network for such period of time as the Agency may require. (2) Every service provider shall, at the request of any law enforcement agency: (a) provide the law enforcement agency with any traffic of subscriber information required to be kept under subsection (1) of this section; or (b) preserve, hold or retain any related content.
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person’s possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider’s possession or control. 2 The powers and procedures referred to in this article shall be subject to	**Cybersecurity bill 2008** 15. (3) Any law enforcement agency may with warrant issued by a court of competent jurisdiction, request for the release of any information in respect of subsection (2) (b) of this section and it shall be the duty of the service provider to comply.

Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data;	**Cybersecurity bill 2008** 29. (1) Pursuant Section (2) of this section, any authorized officer entitled to enforce any provision of this Bill shall have the power to search any premises or computer or network and arrest any person in connection with the offence. (2) Subject to National Security Agency Act, an authorized officer of any law enforcement agency, upon a reasonable suspicion that an offence has been committed or likely to be committed by any person or body corporate, shall have power to: (a) access and inspect or check the operation of any computer to which this act applies; or (b) use or cause to use a computer or any device to search any data contained in or available to any computer or network; or (c) use any technology to re-transform or decrypt any encrypted data contained in a computer into readable text or comprehensible format; or (d) seize or take possession of any computer used in connection with an offence under this Bill, or (e) require any person having charge of or otherwise concerned with the operation of any computer in connection with an offence to produce such computer; or (f) require any person in possession of encrypted data to provide access to any information necessary to decrypt such data;

c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	(g) require any person in authority to release any subscriber or traffic information or any related content; and (h) relate with any international law enforcement agencies for the purpose of giving or receiving on information or exchanging any data or database for the purpose or investigation and prosecution under this Bill. (i) The Agency shall have power to cause or direct investigation by any law enforcement agency. **30. Any person who:** (a) willfully obstructs any law enforcement agency in the exercise of any power under this Bill; or (b) fails to comply with any lawful inquiry or request made by any authorized officer in accordance with the provisions of this Bill, commits an offence and shall be liable on conviction to a fine of not less than N500,000 or imprisonment for a term of not less than 3 years or to both such fine and imprisonment.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.	**Cybersecurity bill 2008** 17. Every service provider shall ensure that any of its equipment, facilities or services that provides a communication is capable of: (a) enabling a law enforcement agency to intercept all communications on its network for the purpose of investigation and prosecution; (b) accessing call data or traffic record; (c) delivering intercepted communications and call data or traffic record in such a format that they may be transmitted by means of equipment, facility or service procured by any law enforcement agency to a location other than the premises of the service provider; and (d) facilitating authorized communications interceptions and access to call data or traffic records unobtrusively with minimum interference with any subscriber's communication service and in

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	a manner that protects: (i) the privacy and security of communications and call data or traffic records not authorized to be intercepted. (ii) information regarding the interception. (2) A service provider who contravenes the provision of subsection (1) of this section, commits an offence and shall be liable on conviction, in case of; (a) service provider, a fine of not less than N100,000; and (b) director, manager or officer of the service provider, a fine of not less than N500,000 or imprisonment for a term of not less than 3 years or to both such fine and imprisonment.
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information	**Cybersecurity bill 2008** 17. Every service provider shall ensure that any of its equipment, facilities or services that provides a communication is capable of: (a) enabling a law enforcement agency to intercept all communications on its network for the purpose of investigation and prosecution; (b) accessing call data or traffic record; (c) delivering intercepted communications and call data or traffic record in such a format that they may be transmitted by means of equipment, facility or service procured by any law enforcement agency to a location other than the premises of the service provider; and (d) facilitating authorized communications interceptions and access to call data or traffic records unobtrusively with minimum interference with any subscriber's communication service and in

relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	a manner that protects: (i) the privacy and security of communications and call data or traffic records not authorized to be intercepted. (ii) information regarding the interception. (2) A service provider who contravenes the provision of subsection (1) of this section, commits an offence and shall be liable on conviction, in case of; (a) service provider, a fine of not less than N100,000; and (b) director, manager or officer of the service provider, a fine of not less than N500,000 or imprisonment for a term of not less than 3 years or to both such fine and imprisonment.
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.	**Courts: The courts vested with criminal jurisdiction in Nigeria are the High Courts and the Magistrate Courts. (section 56 of the Criminal procedure Act)** **Jurisdiction:** The High Court can try any criminal case (on Information) and impose any degree of punishment. (section 77) The Magistrate Court ordinarily tries non-indictable offences (Summary Trial) however it can try an indictable offence upon submission to its jurisdiction by the accused person(s) or by fiat of a prosecuting law officer other than a policeman. With respect to magistrate courts however, there is no power to impose the penalty of capital punishment. This is provided for in section 304. NOTE: 'Indictable offence' is defined in section 2 of the Act. Both the State and Federal High Courts have jurisdiction over offences under the EFCC Act, because the Agency enforces several financial services related laws as

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	well as laws affecting terrorism and intellectual property crimes. **Cybersecurity bill 2008** 28. (1) The Federal High Court or state High Court shall have jurisdiction to try offender under this Bill. (2) Notwithstanding anything to the contrary, the court shall ensure that all matter brought before it under this Bill against any person or body corporate are conducted with dispatch and given accelerated hearing. (3) for the purposes of this Bill, a person shall be subject to prosecution in Nigeria for an offence committed while the offender is physically located either within or outside, if by the conduct of the offender or that of another acting for him; (a) the offence is committed either wholly or partly within Nigeria; (b) the act of the offender committed wholly outside Nigeria constitutes a conspiracy to commit an offence under this Bill within Nigeria; and an act in furtherance of the conspiracy was committed within Nigeria, either directly by the offender or at his instigation; or (c) the act of the offender committed wholly or partly within Nigeria constitutes an attempt, solicitation or conspiracy to commit offence in another jurisdiction under the laws of both Nigeria and such other jurisdiction. (4) For the purpose of this section: (a) an offence or element of the offence is presumed to have been committed in Nigeria if the offence or any of its elements substantially affects person of interest in Nigeria; (b) where any other country claims jurisdiction over an alleged offence which is subject to prosecution in Nigeria as established by this section, the Attorney General of the Federation may consult with such other country with a view to determine the most appropriate jurisdiction for prosecution.
Chapter III – International co-operation	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal	The provisions of the Extradition Act would apply to a country where an Extradition Treaty exists with Nigeria, as well as to every country within the

offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate	Commonwealth, whether specific bilateral Extradition commitment exists or not.

to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of	

whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses	

of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.	

b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	

Article 29 – Expedited preservation of stored computer data

1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2 A request for preservation made under paragraph 1 shall specify:

a the authority seeking the preservation;

b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c the stored computer data to be preserved and its relationship to the offence;

d any available information identifying the custodian of the stored computer data or the location of the computer system;

e the necessity of the preservation; and

f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential

interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where:	

a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning	Nigeria is a member of the G8 24/7 Network. It is represented by the EFCC

criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	
Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	