

DIGITAL RIGHTS AND FREEDOM BILL, 2016

ARRANGEMENT OF SECTIONS

Clause:

PART I - PRELIMINARY

1. Objectives
2. Application

PART II - FUNDAMENTAL RIGHTS AND FREEDOMS

3. Right to Digital Privacy
4. Anonymity
5. Data and Information Privacy
6. Data in the Cloud
7. Meta Data
8. Data Ownership
9. Phishing
10. Surveillance and Lawful Interception
11. Personal Data Protection
12. Freedom of Opinion Online
13. Freedom of Expression Online
14. Freedom of Information Online
15. Freedom of Assembly and Association Online
16. Right to Education Online
17. eGovernance

PART III - OFFENCES AND PENALTIES

18. General Offences and Penalties
 - (1) Offences related to Data Ownership
 - (2) Offences related to phishing
 - (3) Offences related to personal data
 - (4) Offences relating to expression of Hate Speech online
 - (5) Offences related to Child Pornography online
19. Special Defenses and Exemptions

ARRANGEMENT OF SECTIONS

Clause:

PART I - PRELIMINARY

C 1382

Digital Rights and Freedom Bill, 2016

2016

PART IV - ADMINISTRATION AND ENFORCEMENT

20. National Human Rights Commission as the Administrative Agency.

PART V - JURISDICTION AND INTERNATIONAL CO-OPERATION

21. Jurisdiction

PART VI - SEARCH, ARREST AND PROSECUTION

20. Search, Arrest and Prosecution

PART VII - MISCELLANEOUS

22. Regulations
23. Schedules
24. Interpretation
25. Short Title/Citation

A BILL

FOR

AN ACT TO PROVIDE FOR THE PROTECTION OF HUMAN RIGHTS ONLINE, TO PROTECT INTERNET USERS IN NIGERIA FROM INFRINGEMENT OF THEIR FUNDAMENTAL FREEDOMS AND TO GUARANTEE APPLICATION OF HUMAN RIGHTS FOR USERS OF DIGITAL PLATFORMS AND/OR DIGITAL MEDIA AND FOR RELATED MATTERS

Sponsored by Hon. Chukwuemeka Ujam

[] Commencement

ENACTED by the National Assembly of the Federal Republic of Nigeria as follows-

PART I - PRELIMINARY

1. The Objectives of this Bill are to: (a) promote the freedoms of expression assembly and association online; (b) guarantee the fundamental privacy rights of citizens and define the legal framework regarding surveillance; (c) clearly outline provisions for lawful and authorized interception of communications within the digital environment and online without sacrificing the freedom of citizens or their constitutional right to communicate freely; (d) accord data privacy more priority and thus safeguarding sensitive citizen data currently being held by numerous government and private institutions; (e) guarantee application of the human rights which apply offline within the digital environment and online; (f) provide sufficient safeguards against abuse and provide opportunities for redress where infringement occurs; (g) safeguard the digital liberty of Nigerians, now and in the future; (h) seek to guarantee the inviolability of communications, except by order of Court obtained in accordance with the due process of Law; and

	1	(i) equip the judiciary with the necessary legal framework to protect
	2	human rights online.
Application	3	2. The provisions of this Act shall apply throughout the Federal
	4	Republic of Nigeria Application.
	5	PART II - FUNDAMENTAL RIGHTS AND FREEDOMS
Rights to Digital Privacy	6	3.-(1) Unlawful, unauthorised and undue interference with the online
	7	privacy of any person, is prohibited under this Act.
	8	(2) Except the context otherwise provides, the Rule of Confidentiality
	9	shall apply to the entire provisions of this Act.
Anonymity	10	4.-(1) Every person shall have the right to communicate anonymously
	11	online without fear of interference with correspondence.
	12	(2) Every person shall have the right to express themselves
	13	anonymously online and shall not be compelled to adopt real name registration
	14	systems.
	15	(3) Internet Service Providers shall uphold and respect the human
	16	rights of customers by supporting the exercise of anonymous speech.
Data and Information Privacy	17	6.-(1) Every person is guaranteed the confidentiality of his personal
	18	data.
	19	(2) The integrity and confidentiality of personal data and information
	20	of citizens is inviolable and therefore guaranteed.
	21	(3) There shall be clarity on the means by which the private data of
	22	individuals, stored by intermediaries, can be accessed.
	23	(4) Requests for private data shall follow legally stipulated
	24	procedures and Court warrants shall be necessary in order for an intermediary
	25	to honour a request for private data, which request shall be reported to the
	26	concerned individual.
	27	(5) Every private entity in Nigeria holding citizen data – personal
	28	details of private individuals – shall publish in two National Newspapers bi-
	29	annual periodic reports detailing the nature and frequency of government
	30	requests.

1 (6) All entities that collect, store and/or process personal data in the
2 course of their activities shall have data privacy policies that are readily and
3 easily accessible to the public.

4 Under certain exceptional situations where the State may limit the right to
5 privacy for the purposes of administration of criminal justice or prevention
6 of crime, such measures shall be in compliance with the international human
7 rights framework, with adequate safeguards against abuse. This includes
8 ensuring that any measure to limit the right to privacy is taken on the basis of
9 a specific decision by a State Authority expressly empowered by law to do
10 so, and shall respect the principles of necessity and proportionality.

11 7.-(1) Every data owner is entitled to the ownership of his or her Data in the Cloud
12 data stored in the cloud regardless of where it is stored.

13 (2) Every cloud storage provider offering services in Nigeria shall
14 be responsible for keeping the data available and accessible, and the
15 physical environment protected and running on behalf of the data owner.

16 (3) Every data owner shall have the ability to access personal data
17 and transfer it in the event that the cloud provider goes bankrupt.

18 (4) A cloud provider shall give a data owner a seven-day warning
19 before declaring bankruptcy to afford data subjects ample time to get their
20 data off of that server.

21 (5) A data owner reserves the right to be informed about the success
22 or liability in the event that such provider is bought out by another company.

23 (6) A data owner shall be notified by the host whenever his data is
24 subpoenaed, in order to file a response in court where the need arises.

25 (7) A Provider shall make backup of data and guarantee uptime,
26 and where the Provider loses data belonging to the owner, such a Provider
27 shall be liable for damages commensurate to the value of the data lost, plus
28 interest at the prevailing rate.

29 (8) A Provider shall give a data Owner guarantees as to the constant
30 availability of his account on the cloud at all times.

	1	(9) A data Owner shall have the right to know the status of Cyber Risk
	2	insurance and certification of the Provider.
Data Ownership	3	8.-(1) Every person shall be entitled to the ownership of online
	4	content created by themselves or their agents, and shall be responsible for
	5	them.
	6	(2) The digital assets or data sets of an owner such as passwords,
	7	instructive memos, digital contracts, digital receipts, pictures, medical
	8	information, bank accounts, writings, social interactions or anything else that a
	9	user has access to primarily in the digital space is inheritable to be managed and
	10	owned by his heirs or next of kin.
	11	(3) Service providers shall strictly protect the privacy rights of owners
	12	against violation by third parties and by the service providers themselves or
	13	their agents howsoever; the occurrence of which shall give rise to
	14	compensation as shall be determined by the court having due regard to the
	15	extent of damage.
Phishing	16	9. No person, masquerading as a legal entity or otherwise, is entitled
	17	to hold and own sensitive information on the internet such as usernames,
	18	passwords, credit card or bank information, and similar information of an
	19	individual without authorised access.
Surveillance and lawful interception	20	10.-(1) Notwithstanding the provisions of Section 5 of this Act, the
	21	right to privacy shall be derogated only in the following conditions-
	22	(a) Any interference with privacy rights shall be properly published in
	23	a Gazette and available to the general public. Any person who is the subject of
	24	such lawful interference shall be duly notified within seven days upon the
	25	completion of such lawful interference;
	26	(b) Where interference is unavoidable, the collection, interception
	27	and retention of communications data, shall only be lawfully carried out with
	28	an appropriate Court Order having been sought and obtained, and a period
	29	specified;
	30	(c) Any measure to undertake lawful interference shall not be applied

1 in a manner that discriminates on the basis of ethnicity, sex, religion,
2 political or other opinion, national, property, or other status;

3 (d) Communications Surveillance shall be strictly based on the
4 principle of necessity and as a last resort; it shall only be conducted when it is
5 the only means of achieving a legitimate aim, or, when there are multiple
6 means, it is the means least likely to infringe upon human rights. The onus of
7 establishing this justification shall always be on the Government, and/or the
8 entity seeking to carry out the surveillance;

9 (e) Any instance of Communications Surveillance authorised by
10 the court shall be appropriate, proportionate and adequate to fulfil the
11 specific legitimate aim identified;

12 (f) Government decisions and policies about Communications
13 Surveillance shall consider the sensitivity of the information accessed and
14 the severity of the infringement on human rights and other competing
15 interests;

16 (g) User notification shall be issued to anyone whose
17 communications are being under surveillance with enough time and
18 information as appropriate in the circumstance to enable him challenge the
19 decision or seek other remedies and shall have access to the materials
20 presented in support of the application for authorization;

21 (h) Any delay in notification as stipulated in sub-section (a) of this
22 Section 13 (a) above shall only be justified in the following circumstances
23 enumerated hereunder-

24 (i) Notification would seriously jeopardize the purpose for which
25 the Communications Surveillance is authorized, or there is an imminent risk
26 of danger to human life;

27 (ii) Authorization to delay notification is granted by a court of
28 competent jurisdiction; and

29 (iii) The User affected is notified as soon as the risk is lifted as
30 determined by a Competent Judicial Authority in Sub-paragraph (ii);

1 (iv) The obligation to give notice rests with the State; however
2 communications service providers may notify individuals of the
3 Communications Surveillance, voluntarily or upon request.

4 (2) Citizens and lawful residents of Nigeria shall be at liberty to send
5 electronic communications to one another free from the fear of surveillance,
6 monitoring, interception or any other violation of privacy.

7 (3) Mass or indiscriminate surveillance of the people and the
8 monitoring of their communications shall not be carried out.

9 (4) The State shall apply transparency in its use and scope of
10 Communications Surveillance policies, regulations, activities, powers, or
11 authorities; It shall publish, at a minimum, aggregate information on the
12 specific number of requests approved and rejected, a disaggregation of the
13 requests by service provider and by investigation authority, type, and purpose,
14 and the specific number of individuals affected by each.

15 (5) The State shall provide individuals with sufficient information to
16 enable them to fully comprehend the scope, nature, and application of the laws
17 permitting Communications Surveillance. States should not interfere with
18 service providers in their efforts to publish the procedures they apply when
19 assessing and complying with State requests for Communications
20 Surveillance, adhere to those procedures, and publish records of State requests
21 for Communications Surveillance.

22 (6) The State shall establish independent public oversight
23 mechanisms in addition to any oversight already provided through another
24 branch of government, to ensure transparency and accountability of
25 Communications Surveillance.

26 (7) Government agencies shall obtain a search warrant based on
27 probable cause before it can compel any service provider to disclose a user's
28 private communications or documents stored online.

29 (8) Government agencies shall obtain a search warrant based on
30 probable cause before they can track, prospectively or retrospectively, the

however

of the

send

ance,

the

of

or

the

the

se,

to

is

th

in

is

is

it

1 location of a cell phone or other mobile communications devices. (9) Before
2 obtaining transactional data in real time about when and with whom an
3 individual communicates using email, instant messaging, text messaging,
4 the telephone or any other communications technology, government
5 agencies shall demonstrate to a court that such data is relevant to an
6 authorized criminal investigation.

7 (10) Monitoring of communications made over the Internet or
8 telephone, and in particular, the data at issue or information on who
9 individuals email with, share instant messages with, send text messages to,
10 and the Internet Protocol addresses of the Internet sites individuals visit shall
11 not be lawful without a court order.

12 (11) Before obtaining transactional data about multiple
13 unidentified users of communications or other online services when trying
14 to track down a suspect, government agencies shall first demonstrate to a
15 court that the data is needed for its criminal investigation and obtain a Court
16 Order.

17 (12) Government agencies shall not arbitrarily employ the use of
18 subpoenas to get information in bulk about broad categories of telephone or
19 Internet users.

20 (13) Government agencies shall seek, with the leave of court, the
21 records of specific individuals that are relevant to an investigation.

22 (14) Government agencies shall not compel service providers or
23 hardware or software vendors to build surveillance or monitoring capability
24 into their systems, or to collect or retain particular information purely for
25 State Communications Surveillance purposes.

26 (15) Any information obtained in a manner that is inconsistent with
27 these principles shall be inadmissible as evidence or otherwise not
28 considered in any proceeding, as is any evidence derivative of such
29 information.

30 (16) After material obtained through Communications"

1 Surveillance has been used for the purpose for which information was given,
2 the material shall not be retained, but instead be immediately destroyed or
3 returned to those affected.

4 (17) Whistleblowers are also adequately protected by this Act from
5 any form of sanction, attack, arrest or subjected to any civil or criminal
6 proceedings.

7 (18) All persons affected by illegal surveillance activities shall be
8 adequately compensated by the surveilling entity.

9 (19) Every person shall have the right to due process in relation to any
10 legal claims or violations of the law regarding the Internet. Standards of
11 liability, including defences in civil cases, shall take into account the overall
12 public interest in protecting both the expression and the forum in which it is
13 made.

Personal Data
Protection

14 11.-(1) Every person is entitled to the collection, use and disclosure of
15 personal data by Organizations in a manner that recognizes both the right of
16 individuals to protect their personal data, including rights of access and
17 correction, as well as the need of organizations to collect, use or disclose
18 personal data for legitimate and reasonable purposes as appropriate in the
19 circumstances.

20 (2) The use of Personal Data under this section shall be in accordance
21 with the following—

22 (a) Consent—Organizations may collect, use or disclose personal data
23 only with the individual's knowledge and consent;

24 (b) Purpose—Organizations may collect, use or disclose personal data
25 in an appropriate manner for the circumstances, and only if they have informed
26 the individual of purposes for the collection, use or disclosure; and

27 (c) Reasonableness—Organizations may collect, use or disclose
28 personal data only for purposes that would be Personal Data Protection. 15
29 considered appropriate to a reasonable person in the given circumstances.

1 (3) The obligations of an Organization with respect to personal
2 data includes—

3 (a) An Organization is responsible for personal data in its
4 possession or under its control;

5 (b) In meeting its responsibilities under this Section, an
6 Organization shall consider what a reasonable person would consider
7 appropriate in the circumstances;

8 (c) An Organization shall designate one or more individuals to be
9 responsible for ensuring that the Organization complies with the provision
10 of this Section;

11 (d) An individual designated under Paragraph (c) above may
12 delegate to another individual the responsibility conferred by that
13 designation;

14 (e) An Organization shall make available to the public the business
15 contact information of at least one of the individuals designated under
16 Paragraph (c) or delegated under Paragraph (d);

17 (f) The designation of an individual by an Organization under
18 paragraph (c) shall not relieve the Organization of any of its obligations
19 under this Section.

20 (4) An Organization shall have the same obligation under this
21 Section in respect of personal data processed on its behalf and for its
22 purposes by a data intermediary as if the personal data were processed by the
23 Organization itself.

24 (5) This Act shall not apply in respect of—

25 (a) Personal data about an individual that is contained in a record
26 that has been in existence for at least 100 years;

27 (b) Personal data about a deceased individual except that the
28 provisions relating to the disclosure of personal data and shall apply in
29 respect of personal data about an individual who has been dead for 25 years;

30 (c) This Section shall also apply to 16 business contact

Consent for
collection, use and
disclosure of
Personal Data

1 information.

2 (6) An Organization shall not, on or after the appointed day, collect,
3 use or disclose personal data about an individual unless-

4 (a) The individual gives, or is deemed to have given, his consent under
5 this Act to the collection, use or disclosure, as the case may be; or

6 (b) The collection, use or disclosure, as the case may be, without the
7 consent of the individual is required or authorized under this Section or any
8 other written law.

9 (7) An individual has not given consent under this Subsection for the
10 collection, use or disclosure of personal data about the individual by an
11 Organization for a purpose unless-

12 (a) The individual has been provided with the information; and

13 (b) The individual provided his consent for that purpose in
14 accordance with this Section.

15 (8) An Organization shall not-

16 (a) As a condition of providing a product or service, require an
17 individual to consent to the collection, use or disclosure of personal data about
18 the individual beyond what is reasonable to provide the product or service to
19 that individual; or

20 (b) Obtain or attempt to obtain consent for collecting, using or
21 disclosing personal data by providing false or misleading information with
22 respect to the collection, use or disclosure of the personal data, or using
23 deceptive or misleading practices.

24 (9) In this Section, references to consent given, or deemed to have
25 been given, by an individual for the collection, use or disclosure of personal
26 data about the individual shall include consent given, or deemed to have been
27 given, by any person validly acting on behalf of that individual for the
28 collection, use or disclosure of such personal data.

29 (10) An individual is deemed to consent to the collection, use or
30 disclosure of personal data about the individual by an Organization for a

1 purpose if the individual, without actually giving consent referred to in this
2 Act, voluntarily provides the personal data to the Organization for that
3 purpose.

4 (11) If an individual gives, or is deemed to have given, consent to
5 the disclosure of personal data about the individual by one Organization to
6 another Organization for a particular purpose, the individual is deemed to
7 consent to the collection, use or disclosure of the personal data for that
8 particular purpose by that other Organization.

9 (12) On giving reasonable notice to the Organization, an individual
10 may at any time withdraw any consent given, or deemed to have been given
11 under this Section, in respect of the collection, use or disclosure by that
12 Organization of personal data about the individual for any purpose.

13 (13) On receipt of the notice referred to in Sub-section (12), the
14 Organization concerned shall inform the individual of the likely
15 consequences of withdrawing his consent.

16 (14) An Organization shall not prohibit an individual from
17 withdrawing his consent to the collection, use or disclosure of personal data
18 about the individual, but this section shall not affect any legal consequences
19 arising from such withdrawal.

20 (15) If an individual withdraws consent to the collection, use or
21 disclosure of personal data about the individual by an Organization for any
22 purpose, the Organization shall cease (and cause its data intermediaries and
23 agents to cease) collecting, using or disclosing the personal data, as the case
24 may be, unless such collection, use or disclosure, as the case may be, without
25 the consent of the individual is authorized under this Section or other written
26 law.

27 (16) An Organization may collect, use or disclose personal data
28 about an individual without the consent of the individual or from a source
29 other than the individual in any of the following 18 circumstances-

30 (a) It is necessary to respond to an emergency that threatens the life,

- 1 health or safety of the individual or another individual;
- 2 (b) The personal data is publicly available;
- 3 (c) The collection, use or disclosure is necessary for any investigation
4 or proceedings, if it is reasonable to expect that seeking the consent of the
5 individual would compromise the availability or the accuracy of the personal
6 data;
- 7 (d) The collection, use or disclosure is necessary for evaluative
8 purposes;
- 9 (e) The personal data is collected, used or disclosed solely for artistic
10 or literary purposes;
- 11 (f) The personal data is collected, used or disclosed by a news
12 Organization solely for its news activity;
- 13 (g) The personal data is collected, used or disclosed by a credit bureau
14 from a member of the credit bureau to create a credit report, or by a member of
15 the credit bureau from a credit report provided by the credit bureau to that
16 member in relation to a transaction between the member and the individual;
- 17 (h) The personal data is collected, used or disclosed to confer an
18 interest or a benefit on the individual under a private trust or a benefit plan, and
19 to administer such trust or benefit plan, at the request of the settlor or the person
20 establishing the benefit plan, as the case may be;
- 21 (i) The personal data is included in a document-
- 22 (i) Produced in the course, and for the purposes, of the individual's
23 employment, business or profession; and
- 24 (ii) Collected, used or disclosed for purposes consistent with the
25 purposes for which the document was produced;
- 26 (j) The personal data-
- 27 (i) is collected, used or disclosed by an Organization, being a party or
28 a prospective party to a business asset transaction with another Organization,
29 from that other Organization;
- 30 (ii) is about an employee, customer, director, officer or shareholder of

1 the other Organization; and

2 (iii) relates directly to the part of the other Organization or its
3 business assets with which the business asset transaction is concerned;

4 (k) The personal data was disclosed by a public agency, and the
5 collection, or use is consistent with the purpose of the disclosure by the
6 public agency; or

7 (l) The personal data-

8 (i) Was disclosed to the Organization; and

9 (ii) Is collected by the Organization for purposes consistent with
10 the purpose of that disclosure.

11 (17) A responsible party must take reasonably practical steps to
12 ensure that the personal information is complete, accurate, not misleading,
13 and updated where necessary.

14 (18) In taking the steps referred to in Subsection (17), the
15 responsible party must have regard to the purpose for which information is
16 collected or further processed.

17 (19) The processing of personal information of a data subject for
18 the purpose of direct marketing by means of any form of electronic
19 communication, including but not limited to automated calling machines,
20 facsimile machines, SMSs or e-mail is prohibited unless the data subject has
21 expressly given his or her consent.

22 (20) A responsible party may approach a data subject whose
23 consent is required in terms of Subsection (19); and who has not previously
24 withheld such consent, only in order to request the consent of the data
25 subject.

26 (21) The data subject's consent must be requested in the prescribed
27 manner and form.

28 (22) A responsible party may only process the personal
29 information of a data subject who is a customer of the responsible party in
30 terms of Subsection (19)-

1 (a) if the responsible party has obtained the contact details of the data
2 subject in the context of the sale of a product or service;

3 (b) for the purpose of direct marketing of the responsible party's
4 similar products or services; and

5 (c) if the data subject has been given a reasonable opportunity to
6 object free of charge and in a manner free of unnecessary formality, to such use
7 of his or its electronic details—

8 (i) at the time when the information was collected; and

9 (ii) on the occasion of each communication with the data subject for
10 the purpose of marketing if the data subject has not initially refused such use.

11 (23) Any communication for the purpose of direct marketing must
12 contain—

13 (a) details of the identity of the sender or the person on whose behalf
14 the communication has been sent; and

15 (b) an address or other contact details to which a recipient may send a
16 request terminating such communication.

Transfer of Personal
Information outside
Nigeria

17 (24) A data subject who is a subscriber to an electronic directory of
18 subscribers available to the public or obtainable through directory enquiry
19 services, in which his or its personal information is included, must be informed,
20 free of charge and before the information is included in the directory—(a) about
21 the purpose of the directory; and (b) about any further uses to which the
22 directory may possibly be put, based on search functions embedded in
23 electronic versions of the directory.

24 (25) This Section shall not apply to editions of directories that were
25 produced in electronic forms prior to the commencement of this Act.

26 (26) The provisions of Sub-section (28) do not apply if the decision—

27 (a) has been taken in connection with the conclusion or execution of a
28 contract, and the request of the data subject in terms of the contract has been
29 met;

30 (b) appropriate measures have been taken to protect the data subject's

1 legitimate interest;

2 (c) Is governed by a law or code of conduct in which appropriate
3 measures are specified for protecting the legitimate interest of the data
4 subjects.

5 (27) A responsible party within Nigeria may not transfer, transmit,
6 or cause to be transferred or transmitted by any means whatsoever, of
7 personal information about a data subject to a third party who is in a foreign
8 country unless-

9 (a) The third party who is recipient of the information is subject to a
10 law, binding corporate rules, or binding agreements which provide an
11 adequate level of protection that-

12 (i) effectively upholds principles for reasonable processing of
13 information that are substantially similar to the conditions for the lawful
14 processing of personal information relating to a data subject who is a natural
15 person and, where applicable, a juristic person; and

16 (ii) includes provisions, that are substantially similar to this sub-
17 section, relating to the further transfer of personal information from the
18 recipient to third parties who are in a foreign country;

19 (b) The data subject consents to the transfer;

20 (c) The transfer is necessary for the performance of a contract
21 between the data subject and a responsible party, or for the implementation
22 of a pre-contractual measures taken in response to the data subject's request;

23 (d) The transfer is necessary for the conclusion or performance of a
24 contract concluded in the interest of the data subject between the responsible
25 party and a third party; and

26 (e) The transfer is for the benefit of the data subject, and-

27 (i) it is not reasonably practicable to obtain the consent of the data
28 subject to the transfer;

29 (ii) if it were reasonably possible to obtain such consent, the data
30 subject would be likely to give it.

Freedom of
opinion online

Freedom of
Expression online

1 12.-(1) The right to opinion and expression on the Internet shall not be
2 subject to any restrictions, save as provided for under the 1999 Constitution of
3 the Federal Republic of Nigeria (as amended), the Freedom of Information Act
4 2011, and other relevant legislations.

5 13.-(1) Every person shall have the right to freely express opinion
6 online without interference; this right includes the freedom to seek, receive and
7 impart information and ideas, regardless of digital frontiers.

8 (2) Under this Act, Freedom of expression further includes the
9 freedom to express and impart information and ideas of all kinds that can be
10 transmitted to others, in whatever form, and regardless of media. Information
11 or ideas that may be regarded as critical or controversial by the Authorities or
12 by a majority of the population, including ideas or views that may "shock,
13 offend or disturb" are also covered by the right to impart information and ideas
14 of all kinds through any media and regardless of frontiers.

15 (3) Means of expression shall include books, newspapers, pamphlets,
16 posters and banners in digital format or online, as well as all forms of audio-
17 visual, electronic and internet-based modes of expression.

18 (4) The right to freedom of expression includes the right to seek and
19 receive information through the use of the Internet.

20 (5) The government shall not use or compel intermediaries to
21 undertake censorship on its behalf and intermediaries shall not be required to
22 prevent, hide or block content or disclose information about Internet users, or
23 to remove access to user-generated content, including those that infringe
24 copyright laws, without the leave of court.

25 (6) The decision of intermediaries which has the tendency to affect the
26 interest of a user shall be made taking into account the need to protect
27 expression that is legitimate under international standards.

28 (7) Professional journalists, bloggers as well as citizen journalists and
29 others who contribute to shaping public debate and public opinion on the
30 Internet shall be recognised as agents of the larger society who enable the

1 formation of opinions, ideas, decision-making and democracy.

2 (8) Inconsistent and abusive application of legislation shall not be
3 used to censor criticism and debate concerning public issues and to foster a
4 climate of fear and self-censorship among media actors and the public at
5 large.

6 (9) The abuse of the freedom of expression under the guise of
7 protection of national security is prohibited. Consequently the state shall
8 balance the need by ensuring that anti-terrorism laws, treason laws or
9 similar provisions relating to national security conform with their
10 obligations under international human rights law.

11 (10) The right to freedom of expression on the Internet shall not be
12 subject to any restrictions, except those which are provided by law, for a
13 legitimate purpose and necessary and proportionate in a democratic society,
14 as consistent with international human rights standards.

15 (11) Any restriction on freedom of expression must be provided by
16 law, and shall only be imposed for the grounds set out in international human
17 rights law, and shall be, as a matter of obligation, in conformity to the strict
18 tests of necessity and proportionality.

19 (12) No restriction on freedom of expression on the ground of
20 protection of the rights of others, including copyright, may be imposed
21 unless the State can demonstrate that the restriction is prescribed by law and
22 is necessary in a democratic society to protect those interests. The burden of
23 demonstrating the validity of the restriction rests with the State or the
24 copyright holder.

25 Provided that—

26 (a) “Prescribed by law” means that the law must be accessible,
27 unambiguous, drawn narrowly and with sufficient precision so as to enable
28 individuals to foresee whether a particular action is unlawful;

29 (b) This Act is premised on the rule of law and thus provides for
30 prompt, full and effective scrutiny of the validity of the restriction by an

1 independent court, tribunal or other independent adjudicatory body;

2 (c) Any restriction on freedom of expression that the State seeks to
3 justify on grounds of protection of copyright interests must have the genuine
4 purpose and demonstrable effect, on the basis of independent evidence, of
5 protecting the ends that copyright seeks to achieve;

6 (d) Disconnection from access to the Internet on grounds of copyright
7 is always a disproportionate restriction on the right to freedom of expression;

8 (e) Filtering, blocking, removal and other technical or legal limits on
9 access to content are serious restrictions on freedom of expression and can only
10 be justified if they strictly comply with international human rights standards
11 relating to limitations and due process;

12 (f) Website blocking on grounds of copyright protection shall be
13 considered a disproportionate restriction on freedom of expression because of
14 associated risks of over-blocking and the general lack of effectiveness of this
15 measure;

16 (g) Insofar as website blocking may already be permitted by law, this
17 measure shall only be imposed by courts or other independent adjudicatory
18 bodies. In determining the scope of any blocking order, the courts or
19 adjudicatory bodies shall address themselves to the following—

20 (i) Any blocking order shall be as targeted as possible;

21 (ii) No blocking order should be granted unless the rights holder
22 seeking the order has established copyright in the works which are said to be
23 unlawfully accessed;

24 (iii) No blocking injunction should be granted beyond the works in
25 which copyright has been established by the rights holders;

26 (iv) Whether the blocking order is the least restrictive means available
27 to bring an end to individual acts of infringement including an assessment of
28 any adverse impact on the right to freedom of expression;

29 (v) Whether access to other noninfringing material will be impeded
30 and if so to what extent, bearing in mind that in principle, noninfringing content

1 should never be blocked;

2 (vi) The overall effectiveness of the measure and the risks of
3 overblocking;

4 (vii) Whether the blocking order should be of limited duration;

5 (viii) Website blocking orders to prevent future copyright
6 infringements are a form of prior censorship and as such are a
7 disproportionate restriction on freedom of expression.

8 (h) A restriction on freedom of expression is proportionate in a
9 democratic Nigeria only if—

10 (i) It is the least restrictive means available for protecting that
11 interest; and

12 (ii) The restriction is compatible with democratic principles.

13 (i) Protection of national security or countering
14 terrorism/insurgency cannot be used to justify restricting the right to
15 expression unless it can be demonstrated that—

16 (i) the expression is intended to incite imminent violence;

17 (ii) it is likely to incite such violence; and

18 (iii) there is a direct and immediate connection between the
19 expression and the likelihood or occurrence of such violence.

20 (j) The courts shall prescribe stringent procedures for allowing
21 consumer groups or other interested parties to intervene in injunction
22 proceedings in which a blocking order is sought;

23 (k) Knowingly submitting a court application for blocking of
24 content without copyright should be penalized and those harmed by such
25 applications shall be compensated, the amount of which shall be determined
26 by the court. The same applies to overbroad and negligent blocking
27 applications;

28 (l) Any restriction that prevents the flow of information online
29 shall be in line with permissible limitations as set out in international human
30 rights law;

1 (m) Independence for both public and private media, fair and
2 independent media markets shall be held as essential for exercising the right to
3 free expression.

4 (13) Any speech, gesture or conduct, writing, or display capable of
5 inciting violence or prejudicial action against or by a protected individual or
6 group, by disparaging or intimidating a protected individual or group on the
7 basis of attributes such as gender, ethnic origin, religion, race, disability, or
8 sexual orientation, amounts to hate speech and is forbidden.

9 (14) Hate Speech on social media or other online platforms which
10 incites violence, hatred or discrimination against individuals or groups
11 identified by a specific set of characteristics are prohibited. (15) Government
12 concerns about hate speech shall not be abused to discourage citizens from
13 engaging in legitimate democratic debate on matters of general interest.

14 (16) It shall be the duty of the courts to make a distinction between, on
15 the one hand, genuine and serious incitement to extremism and, on the other
16 hand, the right of individuals (including journalists and politicians) to express
17 their views freely and to "offend, shock or disturb" as a way of combating
18 certain forms and expressions of hate speech.

19 (17) Censorship on the Internet, which usually takes the form of laws
20 allowing for the total or partial banning of certain web pages and in certain
21 extreme circumstances, where the State resorts to the complete disconnection
22 of the Internet network, thus isolating a whole region from the rest of the
23 country and the world at large, is a violation of the freedom of expression.

24 (18) The jamming of wireless signals, another means of censorship
25 which deprives individuals of their right to freedom of opinion and expression,
26 is prohibited.

27 (19) The state shall not unduly restrict, control, manipulate and censor
28 content disseminated via the Internet without any legal basis, or on the basis of
29 broad and ambiguous laws, without justifying the purpose of such actions;
30 and/or in a manner that is clearly unnecessary and/or disproportionate to

1 achieving the intended aim.

2 14.-(1) The use and re-use of government held data and Freedom of
Information Online
3 information shall be available free of charge wherever practical, and if not,
4 charging shall be transparent, reasonable, the same for all users, and not
5 designed as a barrier to the use or reuse of the data.

6 (2) The existing obligation on public bodies to share all
7 information produced with the support of public funds in terms of
8 subsection (1), subject only to clearly defined rules set out in law, as
9 established by the Declaration of Principles on Freedom of Expression in
10 Africa, shall extend to the proactive release of such information on the
11 World Wide Web in openly licensed, freely reuseable formats.

12 (3) Copyrighted materials held by public bodies shall be licensed
13 for re-use in accordance with relevant access to information laws and
14 licensing frameworks.

15 (4) The right of citizens to access the Internet for the purposes of
16 information gathering or sharing, conducting business and/or expressing
17 personal opinion is hereby guaranteed; it shall be illegal for government or
18 any entity to deny or censor access to the Internet without providing
19 adequate and acceptable reasons.

20 (5) The duty in terms of Sub-section (2) presupposes providing
21 access to particularly rural areas and the urban poor where Internet
22 penetration is low or nonexistent, lack of technological availability, slower
23 Internet connection, and/or higher costs.

24 (6) Priority shall be accorded to persons with disabilities and
25 persons belonging to minority groups, who often face barriers to accessing
26 the Internet in a way that is meaningful, relevant and useful to them in their
27 daily lives.

28 (7) Where the infrastructure for Internet access is present, the
29 government shall support initiatives to ensure that online information can be
30 accessed in a meaningful way by all sectors of the population, including

1 persons with disabilities and persons belonging to linguistic minorities.

2 (8) Interference which may arise out of abusive, opportunistic or
3 discriminatory (variable geometry) application of various laws, interference
4 with privately operated Internet based platforms or applications, are
5 prohibited.

6 (9) Blocking, which refers to measures taken to prevent certain
7 content from reaching an end-user, or extensive filtering systems that block
8 access to websites containing key terms includes preventing users from
9 accessing specific websites, Internet Protocol (IP) addresses, domain name
10 extensions, the taking down of websites from the web server where they are
11 hosted, or using filtering technologies to exclude pages containing keywords
12 or other specific content from appearing. The arbitrary act of blocking access
13 to certain digital media such as the social network is prohibited.

14 (10) Unlawful, unauthorised and undue restriction on media
15 freedom and pluralism which hinders the freedom to receive and impart
16 information, diminishes media's ability to act as a public watchdog holding
17 power to account, and which in turn undermines both public trust in the
18 media and the exercise of democracy itself, is prohibited.

19 (11) Illegitimate types of information which may be restricted
20 include child pornography (to protect the rights of children), hate speech (to
21 protect the rights of affected communities), defamation (to protect the rights
22 and reputation of others against unwarranted attacks), direct and public
23 incitement to commit genocide (to protect the rights of others), and advocacy
24 of national, racial or religious hatred that constitutes incitement to
25 discrimination, hostility or violence (to protect the rights of others, such as
26 the right to life).

27 (12) Notwithstanding these provisions, the relevant laws shall apply
28 in cases where the content infringes on the rights of another citizen-

29 (1) Everyone shall have the right to peaceful assembly and
30 association online, including through social networks and platforms.

1 (2) Organisers and participants of peaceful assemblies have the
2 right to access the Internet and other new technologies at all times, without
3 interference except those which are provided by law, for a legitimate
4 purpose and necessary and proportionate in a democratic society, as
5 consistent with international human rights standards.

6 (3) The freedom of assembly and association as guaranteed by
7 section 40 of the 1999 constitution of the Federal Republic of Nigeria (as
8 amended) shall apply to every Internet activity.

9 (4) Social and economic openness, to support innovation and guard
10 against monopolies, is hereby protected.

11 (5) In accordance with the principle of Net Neutrality, all data on
12 the Internet shall be treated in an equal and non-discriminatory manner, and
13 shall not be charged differentially, according to user, content, site, platform,
14 application, type of attached equipment, and modes of communication or
15 any other consideration whatsoever.

16 (6) There shall be no special privileges for, or obstacles against, the
17 exchange of information online or any party or content on economic, social,
18 cultural, or political grounds.

19 (7) Nothing in this Section may be interpreted as preventing
20 affirmative action aimed at ensuring substantive equality for marginalised
21 peoples or groups.

22 (1) Every person shall have the right to learn: traditional students,
23 non-traditional students, adults, children, and teachers, independent of age,
24 gender, race, social status, sexual orientation, economic status, state of
25 origin, religion, bodily ability, and environment anywhere and everywhere
26 in Nigeria.

27 (2) It shall be the fundamental principle and practice of
28 government agencies responsible for educational policymaking to include
29 compulsory Internet literacy skills in school curricula, and support similar
30 learning modules outside of schools.

(3) In addition to basic skills training, modules shall clarify the benefits of accessing information online, and of responsibly contributing information.

(4) The education in terms of Subsection (2) shall also be directed towards helping individuals learn how to protect themselves against harmful content, and explain the potential consequences of revealing private information on the Internet.

(5) Online learning, which has the potential to ensure that the right to education is a reality for a greater percentage of the nation's population, shall be promoted to give universal access to learning.

Net Neutrality

(6) To ensure the right to access, learning shall be affordable and available, offered in myriad formats, to students located in a specific place and students working remotely, adapting itself to Freedom of Assembly and Association Online Net Neutrality 32 people's different lifestyles, mobility needs, and schedules.

(7) Media and information literacy shall be promoted to enable all people to access, interpret and make informed judgments as users of information, as well as to create information.

Internet Access
and the necessary
infrastructure

(8) Accordingly, flowing from Subsection 7, media and information literacy programmes shall be instituted in schools and in other public institutions, wherein practical school children, and other learners, shall have access to Internet enabled devices.

(9) It shall be the duty of Government at all levels to ensure that people with disabilities have equal access to knowledge. The lack of copyright exceptions benefiting people with sensory impairments constitute a breach of their rights to freedom of expression, private life and their right to participate in cultural life. Equal access to knowledge by people of all languages and levels of literacy shall be promoted. The lack of copyright exceptions benefiting minority language speakers and persons with low literacy levels undermines their rights to freedom of expression, private life and their right to participate in

1 cultural life.

2 (10) Student privacy shall be protected as an inalienable right
3 regardless of whether learning takes place in a brick-and-mortar institution
4 or online.

5 (11) Students and other learners have a right to know how data
6 collected about their participation in the online system will be used by the
7 organization and made available to others.

8 (12) The provider shall offer clear explanations of the privacy
9 implications of students' choices.

10 (13) Learners within a global, digital commons shall have the right
11 to work, network, and contribute to knowledge in public; to share their ideas
12 and their learning in visible and connected ways if they so choose.

13 (14) Courses offered shall encourage open participation and
14 meaningful engagement with real audiences where possible, including
15 peers and the broader public.

16 (15) Online students also have the right to create and own
17 intellectual property and data associated with their participation in online
18 courses.

19 (16) Online programs shall encourage openness and sharing, while
20 working to educate students about the various ways they can protect and
21 license their data and creative work.

22 (17) Any changes in terms of service shall be clearly
23 communicated by the provider, and they shall never erode the original terms
24 of privacy or the intellectual property rights to which the student agreed.

25 (18) Students shall have the right to know how their participation
26 supports the financial health of the online system in which they are
27 participating.

28 (19) They shall have the right to fairness, honesty, and transparent
29 financial accounting. This is also true of courses that are "free".

Right to education
online

1 (20) The provider shall offer clear explanations of the financial
2 applications of students' choices.

3 (21) Students shall have the right to understand the intended
4 outcomes—educational, vocational, even philosophical—of an online program
5 or initiative.

6 (22) If a credential or badge or certification is promised by the
7 provider, its authenticity, meaning, and intended or historical recognition by
8 others – such as employers or academic institutions) shall be clearly
9 established and explained.

10 (23) In view of the prospects held by ICT for the socioeconomic
11 development and transformation of the country, research capacity and
12 appropriate human resource development in the field of ICT skills shall be
13 promoted with a view to—

14 (a) Introduce and extend e-Learning in institutions of learning;

15 (b) Promote development of specialist/expert capacity in ICT;

16 (c) Promote Digital Literacy;

17 (d) Promote ICT for Education;

18 (e) Accelerate Knowledge Development and Management;

19 (f) Encourage the utilization of ICT across all socio-economic sectors
20 in Nigeria;

21 (g) Increase research and development capacity in ICT sectors; and

22 (h) Harness skills and expertise of Nigerians in Diaspora in ICT
23 development.

24 (24) Education and innovation are interrelated drivers of
25 development, which shall be facilitated by ICTs.

Access to
knowledge and
education

26 (25) Teacher professional development, digital learning resources,
27 affordable technologies, education management information systems and
28 National Research and Education Networks shall be accorded priority.

29 (26) Teachers' capacity in ICT shall be enhanced, as effective
30 integration of technology into teaching and learning requires well qualified

1 educators, a clear focus on equipping teachers with ICT literacy skills and
2 support for teachers to use skills and technology in teaching and learning
3 online.

4 (27) Educators and students shall access learning materials and
5 collaboration platforms at affordable rates as more functional, low-cost
6 devices become available.

7 (28) Broadband access shall be made commonly available as
8 connectivity is crucial for accessing resources, and requires continued focus
9 on competitive broadband access using suitable technologies – wired and
10 wireless, and national collaborative networks.

11 (29) Access to content shall be improved by open educational
12 resources, which can be copied and adapted without licence fees-

Right to create
public knowledge

13 (1) An open, modernized e-governance system enabled by free-
14 flow and access to information and the manner which citizens and
15 businesses interact with government representatives and other agents of the
16 state shall be pursued vigorously.

17 (2) Governments shall recognize the power of social media and use
18 it to democratic advantage, in particular to reinforce democratic processes,
19 drive efficiency, foster innovation, empower public sector workers and
20 expose corruption.

21 (3) An effective e-governance service delivery system shall be
22 pursued by the establishment of accurate, effective and efficient national
23 identification systems, incorporating technology that reduces fraud and
24 identity theft.

Financial
Transparency

25 PART III - OFFENCES AND PENALTIES

26 *General Offences and Penalties*

27 16.-(1) Any person, who, intentionally and without authorization
28 or in excess of authority, commits an offence contrary to the provisions of
29 Section 7 (1) of this Act, shall upon conviction be liable to five years
30 imprisonment with an option of a fine not less than the sum of one million

Pedagogical
Transparency

1 naira or to both. In the case of a body corporate, upon conviction, a fine of not
2 less than five million naira shall apply.

3 (2) Any person, who intentionally and without authorization or in
4 excess of authority, commits an offence contrary to the provisions of Section
5 12 of this Act shall upon conviction be sentenced to a prison term of five years
6 without an option of fine, in addition to compensating the victim where
7 necessary, in a sum to be determined by the court. In the case of a body
8 corporate, upon conviction, a fine of not less than ten million naira shall apply
9 in addition to compensating the victim where necessary, in a sum to be
10 determined by the court.

11 (3) Any person who intentionally and without authorization or in
12 excess of authority, publishes online any form of hate speech, such as the
13 advocacy of regional, racial or religious hatred that constitutes incitement to
14 discrimination, hostility or violence, shall upon conviction be sentenced to a
15 term of not less than one year or to a fine of not less than one million naira. In
16 the event that such publication results in loss of lives and destruction of
17 property, such a person is liable on conviction to imprisonment for a term of not
18 less than seven years, or to a fine not less than five million naira or to both fine
19 and imprisonment including compensation to the victims. In the case of a body
20 corporate, upon conviction, a fine of not less than ten million naira shall apply
21 in addition to compensating the victim where necessary, in a sum to be
22 determined by the court.

23 (4) Any person who undertakes illegal Communications Surveillance
24 surveillance and unlawful interception/interference contrary to section 13 of
25 this Act commits an offence and upon conviction shall be liable to a term of
26 imprisonment not less than ten years and a payment of compensation not less
27 than seven million naira or both.

28 In proceedings against a person for offences under section 22 of this Act, it is a
29 defence for that person to prove-

of not

1 (1) that at the time the alleged offence took place he was under the
2 age of eighteen;

or in

3 (2) the person was prevented from complying with the relevant
4 provisions by stress of weather or other reasonable cause;

action

years

5 (3) that the action was necessary to save or protect life or health of
6 some person(s), to protect serious damage to property, or to avoid adverse
7 effect on the environment;

here

body

apply

8 (4) the commission of the offence was due to a mistake, accident
9 beyond control or due to reliance on information supplied by the default of
10 another person;

or in

11 (5) Exemptions: In the event of a breach the responsible party may
12 raise any of the following defences against an action for damages-

the

at to

13 (a) Vis Major;

to a

14 (b) Consent of the Plaintiff;

In

15 (c) Fault on the part of the Plaintiff;

of

16 (d) Compliance was not reasonably practicable in the
17 circumstances of the particular case;

not

line

18 (e) The National Human Rights Commission has granted a
19 gazetted exemption to the responsible party on the basis of national interest
20 or for the data subject's benefit.

body

ply

be

21 PART IV - ADMINISTRATION AND ENFORCEMENT

22 This Act shall be administered by the National Human Rights Commission
23 in consultation with other relevant agencies of government, relevant civil
24 society actors, and relevant private sector members.

ice

of

of

25 PART V - JURISDICTION AND INTERNATIONAL CO-OPERATION

ss

26 17. The Federal and State High Courts shall have original
27 jurisdiction to the application of this Act.

a

28 PART VI - ENFORCEMENT OF VICTIMS' RIGHTS

29 18.-(1) A data subject or at the request of a data subject or the
30 National Human Rights Commission, may institute a civil action for

e-Governance

1 damages in a Court having jurisdiction against a responsible party for breach of
 2 any part of this Act whether or not there is intent or negligence on the part of the
 3 responsible party.

4 (2) A court hearing proceedings in terms of Subsection (1) may award
 5 an amount that is just and equitable, including-

6 (a) payment of damages as compensation for patrimonial or non-
 7 patrimonial loss suffered by a data subject as a result of breach of the provisions
 8 of this Section;

9 (b) Aggravated damages, in a sum to be determined at the discretion
 10 of the court;

11 (c) Interest; and

12 (d) Cost of suit on such scale as may be determined by the court.

13 PART VII – MISCELLANEOUS

14 19. Regulations - The National Human Rights Commission shall
 15 make Regulations published in government Gazette.

Offences related
to Big Data

16 20. Schedules - There is attached to this Act a Directory of all current
 17 Service Providers in Nigeria responsible for holding personal data.

Interpretation

18 21. "An anonym" means an authenticated attribute that is not linked to
 19 an identifier;

20 "Automated Calling Machine" means a machine that is able to perform
 21 automated calls without human intervention;

22 "Autonomous system administrator" means an individual or legal entity that
 23 administers specific blocks of IP addresses and its specific autonomous routing
 24 system, duly registered in the national entity responsible for the geographical
 25 registration and distribution of IP addresses related to the Country;

26 "Cloud storage" a service model in which data is maintained, managed and
 27 backed up remotely and made available to users over a network (typically the
 28 Internet);

29 "Data Controller" means the natural or legal person, public authority, agency
 30 or any other body which alone or jointly with others determines the purposes

- 1 and means of the processing of personal data; where the purposes and means
2 of processing are determined by national or Community laws or regulations.
3 The controller or the specific criteria for his nomination may be designated
4 by national or Community law;
- 5 “Data Custodian” means any person who is responsible for providing a
6 secure infrastructure in support of the data, including, but not limited to,
7 providing physical security, backup and recovery processes, granting access
8 privileges to system users as authorized by data trustees or their designees
9 and implementing and administering controls over the information;
- 10 “Data Processor” means natural or legal person, public authority, agency,
11 organizations or any other body involved in processing of personal data or
12 processes personal data on behalf of a controller;
- 13 “Data Subject” means an identifiable person; one who can be identified
14 directly or indirectly, in particular by reference to an identification number
15 or to one or more factors specific to his physical, physiological, mental,
16 economic, cultural or social identity;
- 17 “Expression” means any commentary on a person's own or on public affairs.
18 Canvassing, discussion on human rights, journalism, scientific research,
19 expression of ethnic, cultural, linguistic and religious identity and artistic
20 expression, advertising, teaching are all examples of expressions that are
21 covered by the freedom of expression. It also includes political discourse;
- 22 “Internet” means a publicly accessible system of networks that connects
23 computers around the world via the TCP/IP protocol;
- 24 “Internet protocol address” or “IP address” means the code assigned to a
25 terminal from a network to enable their identification, defined according to
26 international standards;
- 27 “Internet application” means a set of functionalities that can be accessed
28 through a device connected to the Internet;
- 29 “Internet connection” means the enabling of a device for sending and
30 receiving data packets over the Internet;

- 1 "Connection record/log" means the set of information pertaining to the date
2 and time of the beginning and end of a connection to the internet, the duration
3 thereof and the IP address used by the device to send and receive data packages;
4 "Metadata" means data that describe other data. This includes but is not limited
5 to data elements in digital camera, digital music files and similar files;
6 "Owner" means anyone who created or can assert creative rights to a product or
7 service;
8 "Personal data" means any information relating to an identified or 7
9 identifiable natural person ("data subject"); information relating to an
10 individual, whether it relates to his or her private, professional or public life;
11 "Personal data" includes but is not limited to anything from a name, address, a
12 photo, an email address, bank details, posts on social networking websites,
13 medical information, or a computer's IP address;
14 "Personal data filing system" means any structured set of personal data which
15 are accessible according to specific criteria, whether centralized, decentralized
16 or dispersed;
17 "Personal information" means information about an identifiable individual,
18 but does not include the name, title or business address or telephone number of
19 an employee of an organization;
20 "Platforms" refer to the entirety of software and/or hardware that make(s) a
21 service available to users;
22 "Processing of personal data" means any operation or set of operations which
23 is performed upon personal data, whether or not by automatic means, such as
24 collection, recording, organization, storage, adaptation or alteration, retrieval,
25 consultation, use, disclosure by transmission, dissemination or otherwise
26 making available, alignment or combination, blocking, erasure or destruction;
27 "Protected speech" means the form of speech protected under this Act. It shall
28 extend to novel forms of conversation introduced by digital mediums which
29 include but are not restricted to;
30 "retweets", "likes", "favourites", "shares", online comments, joining groups

1 on social networking sites and similar forms of speeches;
2 “Registrations of access to Internet applications” means the set of
3 information regarding the date and time of use of a particular internet
4 application from a particular IP address;
5 “Subscriber” means any person who is party to a contract with a provider of
6 publicly available electronic communication services for the supply of such
7 services;
8 “Whistle blowers” refer to anyone who has and reports insider knowledge of
9 illegal activities occurring in an organization. Whistle blowers can be
10 employees, suppliers, contractors, clients or any individual who somehow
11 becomes aware of illegal activities taking place in a business either through
12 witnessing the behavior or being told about it. .

13 22. This Bill may be cited as the Digital Rights and Freedom Bill, Short Title
14 2016.

EXPLANATORY MEMORANDUM

This Bill seeks to protect Internet users in Nigeria from infringement of their fundamental freedoms and to guarantee application of human rights for users of digital platforms and/or Digital media.