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, 2017 (HB. 490)

[ ] Commencement

ENACTED by the National Assembly of the Federal Republic of Nigeria—

PART I - PRELIMINARY

1. The Objectives of this Bill are to: Objectives

(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

(i) equip the judiciary with the necessary legal framework to protect human rights online.

2. The provisions of this Bill shall apply throughout the Federal Republic of Nigeria. Application.

PART II - FUNDAMENTAL RIGHTS AND FREEDOMS

3. (1) Unlawful, unauthorised and undue interference with the online privacy of any person, is prohibited under this Bill. Right to digital privacy.

(2) Except the context otherwise provides, the Rule of Confidentiality shall apply to the entire provisions of this Bill.

4. (1) Every person shall have the right to communicate anonymously online without fear of interference with correspondence. Anonymity.

(2) Every person shall have the right to express themselves anonymously online and shall not be compelled to adopt real name registration systems.

(3) Internet Service Providers shall uphold and respect the human rights of customers by supporting the exercise of anonymous speech.

5. (1) Every person is guaranteed the confidentiality of his personal data. Data and information privacy.

(2) The integrity and confidentiality of personal data and information of citizens is inviolable and therefore guaranteed.

(3) There shall be clear procedures by which the private data of individuals, stored by intermediaries, can be accessed.

(4) Requests for private data shall follow legally stipulated procedures and Court warrants shall be necessary in order for an intermediary to honour a request for private data, which request shall be reported to the concerned individual.

(5) Every private entity in Nigeria holding citizen data – personal details of private individuals – shall publish in two National Newspapers bi-annual periodic reports detailing the nature and frequency of government requests.

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

(7) Under certain exceptional situations where the State may limit the right to privacy for the purposes of administration of criminal justice or prevention of crime, such measures shall be in compliance with the international human rights framework, with adequate safeguards against abuse.

(8) Measures referred to in sub-clause (7) include ensuring that any measure to limit the right to privacy is taken on the basis of a specific decision by a State Authority expressly empowered by law to do so, and shall respect the principles of necessity and proportionality.

6. (1) Every data owner is entitled to the ownership of his or her data stored in the cloud regardless of where it is stored. Data in the cloud.

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

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

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

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

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

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

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

(9) A data Owner shall have the right to know the status of Cyber Risk insurance and certification of the Provider.

7. (1) Every person shall be entitled to the ownership of online content created by themselves or their agents, and shall be responsible for them. Data ownership.

(2) The digital assets or data sets of an owner such as passwords, instructive memos, digital contracts, digital receipts, pictures, medical information, bank accounts, writings, social interactions or anything else that a user has access to primarily in the digital space is inheritable to be managed and owned by his heirs or next of kin.

(3) Service providers shall strictly protect the privacy rights of owners against violation by third parties and by the service providers themselves or their agents howsoever; the occurrence of which shall give rise to compensation as shall be determined by the court having due regard to the extent of damage.

8. No person, masquerading as a legal entity or otherwise, is entitled to hold and own sensitive information on the internet such as usernames, passwords, credit card or bank information, and similar information of an individual without authorised access. Phishing.

9. (1) Notwithstanding the provisions of section 5 of this Bill, the right to privacy shall be derogated only in the following conditions– Surveillance and lawful interception.

(a) any interference with privacy rights shall be properly published in a Gazette and available to the general public. Any person who is the subject of such lawful interference shall be duly notified within seven days upon the completion of such lawful interference;

(b) where interference is unavoidable, the collection, interception and retention of communications data, shall only be lawfully carried out with an appropriate Court Order having been sought and obtained, and a period specified;

(c) any measure to undertake lawful interference shall not be applied in a manner that discriminates on the basis of ethnicity, sex, religion, political or other opinion, national, property, or other status;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(8) Government agencies shall obtain a search warrant based on probable cause before they can track, prospectively or retrospectively, the location of a cell phone or other mobile communications devices.

(9) Before obtaining transactional data in real time about when and with whom an individual communicates using email, instant messaging, text messaging, the telephone or any other communications technology, government agencies shall demonstrate to a court that such data is relevant to an authorized criminal investigation.

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

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

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

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

(14) After material obtained through Communications Surveillance has been used for the purpose for which information was given, the material shall not be retained, but instead be immediately destroyed or returned to those affected.

(15) Whistle-blowers are also adequately protected by this Bill from any form of sanction, attack, arrest or subjected to any civil or criminal proceedings.

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

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

Personal data protection.

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

(2) The use of Personal Data under this clause shall be in accordance with the following–

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

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

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

(3) The obligations of an Organization with respect to personal data include–

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

(b) in meeting its responsibilities under this clause an Organization shall consider what a reasonable person would consider appropriate in the circumstances;

(c) an Organization shall designate one or more individuals to be responsible for ensuring that the Organization complies with the provision of this clause;

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

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

(f) the designation of an individual by an Organization under paragraph (c) shall not relieve the Organization of any of its obligations under this clause.

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

(5) This Bill shall not apply in respect of—

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

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

(c) this clause shall also apply to business contact information.

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

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

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

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

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

(b) the individual provided his consent for that purpose in accordance with this clause.

(8) An Organization shall not-

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

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

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

Consent for collection, use and disclosure of personal data.

11. (1) An individual is deemed to consent to the collection, use or disclosure of personal data about the individual by an Organization for a purpose if the individual, without actually giving consent referred to in this Bill, voluntarily provides the personal data to the Organization for that purpose .

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

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

(4) On receipt of the notice referred to in sub-clause (3), the Organization concerned shall inform the individual of the likely consequences of withdrawing his consent.

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

(6) If an individual withdraws consent to the collection, use or disclosure of personal data about the individual by an Organization for any purpose, the Organization shall cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data, as the case may be, unless such collection, use or disclosure, as the case

may be, without the consent of the individual is authorized under this Bill or other written law.

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

(a) it is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual;

(b) the personal data is publicly available;

(c) the collection, use or disclosure is necessary for any investigation or proceedings, if it is reasonable to expect that seeking the consent of the individual would compromise the availability or the accuracy of the personal data;

(d) the collection, use or disclosure is necessary for evaluative purposes;

(e) the personal data is collected, used or disclosed solely for artistic or literary purposes;

(f) the personal data is collected, used or disclosed by a news Organization solely for its news activity;

(g) the personal data is collected, used or disclosed by a credit bureau from a member of the credit bureau to create a credit report, or by a member of the credit bureau from a credit report provided by the credit bureau to that member in relation to a transaction between the member and the individual;

(h) the personal data is collected, used or disclosed to confer an interest or a benefit on the individual under a private trust or a benefit plan, and to administer such trust or benefit plan, at the request of the settlor or the person establishing the benefit plan, as the case may be;

(i) the personal data is included in a document-

(i) produced in the course, and for the purposes, of the individual's employment, business or profession; and

(ii) collected, used or disclosed for purposes consistent with the purposes for which the document was produced.

(j) the personal data-

(i) is collected, used or disclosed by an Organization, being a party or a prospective party to a business asset transaction with another Organization,

from that other Organization;

(ii) is about an employee, customer, director, officer or shareholder of the other Organization; and

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

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

(l) the personal data-

(i) was disclosed to the Organization; and

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

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

(9) In taking the steps referred to in sub-clause (8), the responsible party must have regard to the purpose for which information is collected or further processed.

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

(11) A responsible party may approach a data subject whose consent is required in terms of sub-clause (10); and who has not previously withheld such consent, only in order to request the consent of the data subject.

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

(13) A responsible party may only process the personal information of a data subject who is a customer of the responsible party in terms of sub-clause (10)-

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

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

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

details–

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

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

(14) Any communication for the purpose of direct marketing must contain–

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

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

Transfer of personal information outside Nigeria.

12. (1) A data subject who is a subscriber to an electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which his or its personal information is included, must be informed, free of charge and before the information is included in the directory–

(a) about the purpose of the directory; and

(b) about any further uses to which the directory may possibly be put, based on search functions embedded in electronic versions of the directory.

(2) This clause shall not apply to editions of directories that were produced in electronic forms prior to the commencement of this Bill.

(3) The provisions of sub-clause (1) do not apply if the decision –

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

(b) appropriate measures have been taken to protect the data subject's legitimate interest;

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

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

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

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

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

(b) the data subject consents to the transfer;

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

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

(e) the transfer is for the benefit of the data subject, and–

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

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

Freedom of expression online.

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

Freedom of expression of opinion online.

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

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

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

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

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

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

(7) Professional journalists, bloggers as well as citizen journalists and others who contribute to shaping public debate and public opinion on the Internet shall be recognized as agents of the larger society who enable the formation of opinions, ideas, decision-making and democracy.

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

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

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

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

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

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

(b) this Bill is premised on the rule of law and thus provides for prompt, full and effective scrutiny of the validity of the restriction by an independent court, tribunal or other independent adjudicatory body;

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

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

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

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

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

(i) any blocking order shall be as targeted as possible;

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

(iii) no blocking injunction should be 26 granted beyond the works in which copyright has been established by the rights holders;

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

(v) whether access to other non-infringing material will be impeded and if so to what extent, bearing in mind that in principle, non-infringing content should never be blocked;

(vi) the overall effectiveness of the measure and the risks of over-blocking;
(vii) whether the blocking order should be of limited duration;

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

(h) a restriction on freedom of expression is proportionate in a democratic Nigeria only if–

(i) it is the least restrictive means available for protecting that interest; and

(ii) the restriction is compatible with democratic principles.

(i) protection of national security or countering terrorism/insurgency cannot be used to justify restricting the right to expression unless it can be demonstrated that–

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

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

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

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

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

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

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

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

(14) Hate Speech on social media or other online platforms which incites violence, hatred or discrimination against individuals or groups identified by a specific set of characteristics are prohibited.

(15) Government concerns about hate speech shall not be abused to discourage citizens from engaging in legitimate democratic debate on matters of general interest.

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

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

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

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

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

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

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

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

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

(6) Priority shall be accorded to persons with disabilities and persons belonging to

minority groups, who often face barriers to accessing the Internet in a way that is meaningful, relevant and useful to them in their daily lives.

(7) Where the infrastructure for Internet access is present, the government shall support initiatives to ensure that online information can be accessed in a meaningful way by all sectors of the population, including persons with disabilities and persons belonging to linguistic minorities.

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

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

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

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

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

Right to peaceful assembly and association online.

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

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

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

activity.

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

(5) All data on the Internet shall be treated in an equal and non-discriminatory manner, and shall not be charged differentially, according to user, content, site, platform, application, type of attached equipment, and modes of communication or any other consideration whatsoever.

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

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

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

(2) It shall be the fundamental principle and practice of government agencies responsible for educational policymaking to include compulsory Internet literacy skills in school curricula, and support similar 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 sub-clause (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.

(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.

(8) Accordingly, flowing from sub-clause 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.

(10) 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.

(11) 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 cultural life.

Protection of privacy of students and learners.

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

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

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

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

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

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

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

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

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

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

Right to Education Online.
(11) The provider shall offer clear explanations of the financial implications of students' choices.

(12) Students shall have the right to understand the intended outcomes–educational, vocational, even philosophical of an online program or initiative.

19. (1) If a credential or badge or certification is promised by the provider, its authenticity, meaning, and intended or historical recognition by others – such as employers or academic institutions) shall be clearly established and explained. Right to create public knowledge

(2) Research capacity and appropriate human resource development in the field of ICT skills shall be promoted with a view to–

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

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

(c) promote Digital Literacy;

(d) promote ICT for Education;

(e) accelerate Knowledge Development and Management;

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

(g) increase research and development capacity in ICT sectors; and

(h) harness skills and expertise of Nigerians in Diaspora in ICT development.

(3) Education and innovation are interrelated drivers of development, which shall be facilitated by ICTs, access to knowledge and education.

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

(5) Teachers' capacity in ICT shall be enhanced, as effective integration of technology into teaching and learning requires well qualified educators, a clear focus on equipping teachers with ICT literacy skills and support for teachers to use skills and technology in teaching and learning online.

(6) Educators and students shall access learning materials and collaboration platforms at

affordable rates as more functional, low-cost devices become available.

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

(8) Access to content shall be improved by open educational resources, which can be copied and adapted without licence fees.

E-governance and financial transparency.

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

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

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

PART III - OFFENCES AND PENALTIES

General Offences and Penalties

Pedagogical transparency.

21. (1) Any person, who, intentionally and without authorization or in excess of authority, commits an offence contrary to the provisions of clause 5 (1) of this Bill, shall upon conviction be liable to five years imprisonment with an option of a fine not less than the sum of one million naira or to both. In the case of a body corporate, upon conviction, a fine of not less than five million naira shall apply.

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

(3) Any person who intentionally and without authorization or in excess of authority, publishes online any form of hate speech, such as the advocacy of regional, racial or religious hatred that constitutes incitement to discrimination, hostility or violence, shall upon conviction be sentenced to a term of not less than one year or to a fine of not less than one million naira.

(4) In the event that such publication in sub-clause (3) results in loss of lives and

destruction of property, such a person is liable on conviction to imprisonment for a term of not less than seven years, or to a fine not less than five million naira or to both fine and imprisonment including compensation to the victims. In the case of a body corporate, upon conviction, a fine of not less than ten million naira shall apply in addition to compensating the victim where necessary, in a sum to be determined by the court.

(5) Any person who undertakes illegal Communications Surveillance and unlawful interception/interference contrary to clause 10 of this Bill commits an offence and upon conviction shall be liable to a term of imprisonment not less than ten years and a payment of compensation not less than seven million naira or both.

(6) In proceedings against a person for offences under this clause, it is a defence for that person to prove-

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

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

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

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

(e) exemptions: In the event of a breach the responsible party may raise any of the following defences against an action for damages-

(i) vis major;

(ii) consent of the Plaintiff;

(iii) fault on the part of the Plaintiff;

(iv) compliance was not reasonably practicable in the circumstances of the particular case;

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

PART IV-JURISDICTION AND INTERNATIONAL CO-OPERATION

22. The Federal and State High Courts shall have original jurisdiction to the application of this Bill. Jurisdiction.

PART V-ENFORCEMENT OF VICTIMS' RIGHTS

23. (1) A data subject or at the request of a data subject or the National Human Rights Commission, may institute a civil action for damages in a Court having jurisdiction against a responsible party for breach of any part of this Bill whether or not there is intent or negligence on the part of the responsible party. E-Governance.

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

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

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

(c) interest; and

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

PART VI – MISCELLANEOUS

24. The National Human Rights Commission shall make Regulations published in government Gazette. Regulations.

25. In this Bill, unless the context otherwise requires - Interpretation.

"An anonym" means an authenticated attribute that is not linked to an identifier;

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

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

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

"Data Controller" means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations. The controller or the specific criteria for his nomination may be designated by national or Community law;

"Data Custodian" means any person who is responsible for providing a secure infrastructure in support of the data, including, but not limited to, providing physical security, backup and recovery processes, granting access privileges to system users as authorized by data trustees or their designees and implementing and administering controls over the information;

“Data Processor” means natural or legal person, public authority, agency, organizations or any other body involved in processing of personal data or processes personal data on behalf of a controller;

“Data Subject” means an identifiable person; one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

“Expression” means any commentary on a person’s own or on public affairs. Canvassing, discussion on human rights, journalism, scientific research, expression of ethnic, cultural, linguistic and religious identity and artistic expression, advertising, teaching are all examples of expressions that are covered by the freedom of expression. It also includes political discourse;

“Internet” means a publicly accessible system of networks that connects computers around the world via the TCP/IP protocol;

“Internet protocol address” or “IP address” means the code assigned to a terminal from a network to enable their identification, defined according to international standards;

“Internet application” means a set of functionalities that can be accessed through a device connected to the Internet;

“Internet connection” means the enabling of a device for sending and receiving data packets over the Internet;

“Connection record/log” means the set of information pertaining to the date and time of the beginning and end of a connection to the internet, the duration thereof and the IP address used by the device to send and receive data packages;

“Metadata” means data that describe other data. This includes but is not limited to data elements in digital camera, digital music files and similar files;

“Owner” means anyone who created or can assert creative rights to a product or service;

“Personal data” means any information relating to an identified or 7 identifiable natural person ("data subject"); information relating to an individual, whether it relates to his or her private, professional or public life;

“Personal data” includes but is not limited to anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer’s IP address;

“Personal data filing system” means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed;

“Personal information” means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization;

"Platforms" refer to the entirety of software and/or hardware that make(s) a service available to users;

"Processing of personal data" means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

"Protected speech" means the form of speech protected under this Bill. It shall extend to novel forms of conversation introduced by digital mediums which include but are not restricted to;

"retweets", "likes", "favourites", "shares", online comments, joining groups on social networking sites and similar forms of speeches;

"Registrations of access to Internet applications" means the set of information regarding the date and time of use of a particular internet application from a particular IP address;

"Subscriber" means any person who is party to a contract with a provider of publicly available electronic communication services for the supply of such services;

"Whistle blowers" refer to anyone who has and reports insider knowledge of illegal activities occurring in an organization. Whistleblowers can be employees, suppliers, contractors, clients or any individual who somehow becomes aware of illegal activities taking place in a business either through witnessing the behavior or being told about it.

26. This Bill may be cited as the Digital Rights and Freedom Bill, 2017. Citation.

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.

PASSED BY THE HOUSE OF REPRESENTATIVES ON TUESDAY, 19TH DECEMBER, 2017

……	……
Speaker	Clerk
House of Representatives	House of Representatives