

A BILL

FOR

AN ACT TO PROVIDE FOR THE REGULATION OF TELECOMMUNICATION FACILITIES TO SUPPORT INVESTIGATIONS AND FOR OTHER MATTERS CONNECTED THEREWITH 2012.

SPONSORED BY SENATOR EMMANUEL PAULKER

[] Commencement

BE IT ENACTED by the National Assembly of the Federal Republic of Nigeria as follows:

1 1. This Bill may be cited as the Regulation of Telecommunications Short Title
2 Facilities to Support Investigations Bill, 2012.

3 2. -(1) in this Bill unless the context otherwise requires.
4 "authorized", in relation to a person, means having authority to intercept
5 communications and these includes the Nigerian Communications
6 Commission Nigeria Police, the State Security Service, the National
7 Intelligence Agency and other Law Enforcement Agencies.
8 "communication" means a communication effected by a means of
9 telecommunication and any related telecommunications data or other
10 ancillary information.

11 "intercept" includes listen to, record or acquire a communication or acquire
12 the substance, meaning or purport of the communication.

13 "Minister" means the Minister responsible for Defence.

14 "person" includes a partnership, government, a government agency and any
15 other person "prescribed" means prescribed by the regulations.

16 "telecommunications data" means data relating to the telecommunications
17 functions of dialling, routing, addressing or signalling that identifies or
18 purports to identify the origin, type, direction, date, time, duration, size,
19 destination or termination of a telecommunication generated or received by

1 means of a telecommunications facility or the type of telecommunications
2 service used.

3 "Telecommunications facility" means any facility, apparatus or other thing that
4 is used for telecommunications or for any operation directly connected with
5 telecommunications. "telecommunications service" means a service, or a
6 feature of a service, that is provided by means of telecommunications facilities.

7 "telecommunications service provider" means a person or a group that provides
8 telecommunications services.

9 "transmission apparatus" means any apparatus of a prescribed class whose
10 principal functions are one or more of the following:

11 (a) the switching or routing of communications;

12 (b) the input, capture, storage, organization, modification, retrieval,
13 output or other processing of communications;

14 (c) the control of the speed, code, protocol, content, format, switching
15 or routing or similar aspects of communications; and

16 (d) any other function that is similar to one described in paragraphs (a)
17 to (c).

Objective

18 3. The aim of this Act is to ensure that telecommunications service
19 providers have the capability to enable national security and law enforcement
20 agencies to exercise their authority to intercept communications and to require
21 telecommunications service providers to provide subscriber and other
22 information, without unreasonably impairing the privacy of individuals, the
23 provision of telecommunications services to Nigerians.

24 OBLIGATIONS CONCERNING INTERCEPTIONS

Obligation
to have
capabilities

25 4. -(1) For the purpose of enabling authorized persons to exercise their
26 authority to intercept communications, every telecommunications service
27 provider must have the capability to do the following:

28 (a) provide intercepted communications to authorized persons; and

29 (b) provide authorized persons with the prescribed information that is
30 in the possession or control of the service provider respecting the location of

1 equipment used in the transmission of communications.

2 (2) A telecommunications service provider, in connection with the
3 interception of communications, must comply with any prescribed
4 confidentiality or security measures.

5 (3) If an intercepted communication is encoded, compressed,
6 encrypted or otherwise treated by a telecommunications service provider,
7 the service provider must use the means in its control to provide the
8 intercepted communication in the same form as it was before the
9 communication was treated by the service provider.

10 (4) Despite subsection (3), a telecommunications service provider
11 is not required to make the form of an intercepted communication the same
12 as it was before the communication was treated if-

13 (a) the service provider would be required to develop or acquire
14 decryption techniques or decryption tools;

15 (b) the treatment is intended only for the purposes of generating a
16 digital signature or for certifying a communication by a prescribed
17 certification authority, and has not been used for any other purpose.

18 (5) A telecommunications service provider that is capable of
19 providing intercepted communications to an authorized person in more
20 than one form or manner that conforms with the regulations must provide
21 them in whichever of those forms or manners the authorized person
22 requires.

23 5. The operational requirements in respect of any transmission
24 apparatus are that the telecommunications service providers operating the
25 apparatus have the capability to do the following:

26 (a) enable the interception of communications generated by or
27 transmitted through the apparatus to or from any temporary or permanent
28 user of the service provider's telecommunications services;

29 (b) isolate the communication that is authorized to be intercepted
30 from other information, including-

Operational
requirements for
transmission
apparatus

1 (i) isolating the communications of the person whose communications
2 are authorized to be intercepted from those of other persons, and

3 (ii) isolating the telecommunications data of the person whose
4 communications are authorized to be intercepted from the rest of the person's
5 communications;

6 (c) provide prescribed information that permits the accurate
7 correlation of all elements of intercepted communications; and

8 (d) enable simultaneous interceptions by authorized persons from
9 multiple national security and law enforcement agencies of communications of
10 multiple users, including enabling-

11 (i) at least the minimum number of those interceptions, and

12 (ii) any greater number of those interceptions - up to the maximum
13 number - for the period that an agency requests.

No. Degradation
of capabilities

14 6. A telecommunications service provider that meets, in whole or in
15 part, an operational requirement in respect of transmission apparatus that the
16 service provider operates must continue to so meet that operational requirement.

Maintaining
capabilities in
respect of new
services

17 7. A telecommunications service provider that meets, in whole or in
18 part, an operational requirement in respect of transmission apparatus that the
19 service provider operates in connection with any of the service provider's
20 telecommunications services must meet that operational requirement to the
21 same extent in respect of any new service that the service provider begins to
22 provide using that apparatus.

Beginning to
operate
transmission
apparatus

23 8. -(1) A telecommunications service provider that begins to operate
24 any transmission apparatus for the purpose of providing telecommunications
25 services must meet the operational requirements in respect of the apparatus,
26 whether by means of the apparatus itself or by any other means.

27 (2) Subsection (1) does not apply in respect of transmission apparatus
28 that a telecommunications service provider acquires from another
29 telecommunications service provider and operates in order to continue to
30 provide the same telecommunications service to approximately the same users.

1 However, the acquiring service provider must continue to meet any
2 operational requirements in respect of the transmission apparatus that the
3 service provider from whom it was acquired' was obligated to meet.

4 9. -(1) When a telecommunications service provider installs new
5 software for any transmission apparatus that the service provider operates,
6 the service provider must meet the operational requirements in respect of
7 that apparatus to the extent that would be enabled by the installation of the
8 software in the form available from the software's manufacturer that would
9 most increase the service provider's ability to meet those operational
10 requirements.

New software

11 (2) Subsection (1) applies even if the form of the software in
12 question would require the telecommunications service provider to acquire
13 additional software, licences or telecommunications facilities to achieve
14 that increased ability.

15 10. Subject to section 14, a telecommunications service provider
16 is not required, under sections 8 to 11, to increase the service provider's
17 capability to enable simultaneous interceptions beyond the applicable limit.

Acceptable
limit

18 11. -(1) The Minister may, by order made on the application of a
19 telecommunications service provider, suspend in whole or in part any
20 obligation of the service provider to meet an operational requirement that
21 would arise from the operation of section 10 or 11.

Order suspending
obligations

22 (2) The application must-

23 (a) specify the operational requirement with respect to which an
24 order is sought;

25 (b) set out the reasons for making the application;

26 (c) include a plan that-

27 (i) sets out the measures by which and the time within which the
28 telecommunications service provider proposes to meet the operational
29 requirement specified in accordance with paragraph (a),

30 (ii) describes any measures that the service provider proposes to

1 take to improve the service provider's capability to meet the operational
2 requirements, even if they are not yet applicable, and

3 (iii) identifies the stages at which and methods by which the Minister
4 can measure progress in the implementation of the plan and the time, manner
5 and form for reports the service provider proposes to make to the Minister; and

6 (d) conform with the prescribed requirements relating to the content or
7 form of the application or the manner in which it is to be made.

8 (3) In deciding whether to make an order, the Minister must take into
9 account the public interest in national security and law enforcement and the
10 commercial interests of the telecommunications service provider as well as any
11 other matter that the Minister considers relevant.

12 (4) The Minister must, within 120 days after the day on which the
13 Minister receives the application, notify the applicant of the Minister's decision
14 to accept or refuse it and, if no notification has been received by the applicant at
15 the end of that period, the Minister is deemed to have refused the application.

16 (5) In the order, the Minister may include any conditions that the
17 Minister considers appropriate and must fix its term for a period of not more than
18 three years.

19 (6) The telecommunications service provider must comply with the
20 conditions of the order as soon as the service provider begins to operate the
21 telecommunications apparatus or installs the new software, as the case may be.

22 (7) The Minister may revoke an order on written notice to the
23 telecommunications service provider if-

24 (a) the service provider has contravened this Act, the regulations or the
25 conditions of the order; and

26 (b) the order was obtained through misrepresentation.

27 **12.** The Minister may, at the request of the Inspector General of Police
28 or the Director State Security Service and if in the Minister's opinion it is
29 necessary to do so, order a telecommunications service provider-

30 (A) to comply with any obligation under subsections 6(1) and (2) in a

1 manner or within a time that the Minister specifies;

2 (b) to enable, in a manner or within a time that the Minister
3 specifies, a number of simultaneous interceptions greater than any
4 maximum or limit that would otherwise apply;

5 (c) to comply, in a manner or within a time that the Minister
6 specifies, with any confidentiality or security measures respecting
7 interceptions that the Minister specifies in addition to those referred to in
8 subsection 6(2);

9 (d) to meet an operational requirement in respect of transmission
10 apparatus operated by the service provider that the service provider would
11 not otherwise be required to meet; and

12 (e) to meet an operational requirement in respect of transmission
13 apparatus operated by the service provider in a manner or within a time that
14 the Minister specifies.

15 (3) The Inspector General of Police or the Director State Security
16 Service as the case may be, must pay the telecommunications service
17 provider an amount that the Minister considers reasonable towards the
18 expenses that the Minister considers are necessary for the service provider
19 to incur initially to comply with an order made under this section.

20 (4) The Minister may provide the telecommunications service
21 provider with any equipment or other thing that the Minister considers the
22 service provider needs to comply with an order made under this section.

23 (5) Sections 6 and 9 do not apply in respect of any equipment or
24 other thing provided by the Minister under subsection (4). However, the
25 telecommunications service provider must provide notice to the Minister of
26 any problems with the equipment or other thing provided and provide
27 assistance in resolving the problem.

28 OBLIGATIONS CONCERNING SUBSCRIBER INFORMATION

29 13. -(1) Every telecommunications service provider must provide
30 a person designated under subsection (3), on his or her written request, with

Provision of
subscriber
information

1 any information in the service provider's possession or control respecting the
2 name, address, telephone number and electronic mail address of any subscriber
3 to any of the service provider's telecommunications services and the Internet
4 protocol address, mobile identification number, electronic serial number, local
5 service provider identifier, international mobile equipment identity number,
6 international mobile subscriber identity number and subscriber identity module
7 card number that are associated with the subscriber's service and equipment.

8 (2) A designated person must ensure that he or she makes a request
9 under subsection (1) only in performing, as the case may be, a duty or function-

10 (a) of the state Security Service under the Security Service Act;

11 (b) of a police service, including any related to the enforcement of any
12 laws in Nigeria.

13 (3) The Inspector General of Police or the Director State Security
14 Service may designate for the purposes of this section any employee of his or her
15 agency, or a class of such employees, whose duties are related to protecting
16 national security or to law enforcement.

17 (4) The number of persons designated under subsection (3) in respect
18 of a particular agency may not exceed the greater of five and the number that is
19 equal to five per cent of the total number of employees of that agency.

Exceptional
circumstances

20 **14.** -(1) A police officer may request a telecommunications service
21 provider to provide the officer with the information referred to in subsection
22 16(1) in the following circumstances:

23 (a) the officer believes on reasonable grounds that the urgency of the
24 situation is such that the request cannot, with reasonable diligence, be made
25 under that subsection;

26 (b) the officer believes on reasonable grounds that the information
27 requested is immediately necessary to prevent an unlawful act that would cause
28 serious harm to any person or to property; and

29 (c) the information directly concerns either the person who would
30 perform the act that is likely to cause the harm or is the victim, or intended

1 victim, of the harm.

2 The police officer must inform the telecommunications service provider of
3 his or her name, rank, badge number and the agency in which he or she is
4 employed and state that the request is being made in exceptional
5 circumstances and under the authority of this subsection.

6 (2) The telecommunications service provider must provide the
7 information to the police officer as if the request were made by a designated
8 person under subsection 16(1).

9 (3) The police officer must, within 24 hours after making a request
10 under subsection (1), communicate to a designated person employed in the
11 same agency-as the officer all of the information relating to the request that
12 would be necessary if it had been made under subsection 13(1) and inform
13 that person of the circumstances referred to in paragraphs (1)(a) to (c).

14 (4) On receiving the information, the designated person must in
15 writing inform the telecommunications service provider that the request
16 was made in exceptional circumstances under the authority of subsection
17 (1).

18 15. -(1) A designated person who makes a request under
19 subsection 13(1), or who receives information under subsection 14(3), must
20 create a record that-

Creation of
record by
designated
person

21 (a) in the case of a request under subsection 13(1), identifies the
22 duty or function referred to in subsection 13(2) in the performance of which
23 the request is made, describes the relevance of the information requested to
24 that duty or function and includes any other information that justifies the
25 request and any other prescribed information; and

26 (b) in the case where the designated person receives information
27 under subsection 14(3), includes the information referred to in paragraph
28 (a) as well as the circumstances referred to in paragraphs 14(1)(a) to (c).

29 (2) The agency that employs the designated person must retain
30 records created under subsection (1) and deal with the information provided

1 in response to requests made under subsection 13(1) or 14(1).

Use of
Information

2 **16.** Information that is provided in response to a request made under
3 subsection 13(1) or 14(1) must not, without the consent of the individual to
4 whom it relates, be used by the agency in which the designated person or police
5 officer is employed except for the purpose for which the information was
6 obtained or for a use consistent with that purpose.

Internal
audit

7 **17.** -(1) The Inspector General of Police or the Director State Security
8 Service who makes a designation must cause internal audits to be regularly
9 conducted of the practices of his or her agency to ensure compliance with
10 sections 13 to 16 and the regulations made for the purposes of those sections and
11 of the internal management and information systems and controls concerning
12 requests made under sections 13 and 14.

13 (2) The person who causes an internal audit to be conducted must,
14 without delay, make a report to the responsible minister of anything arising out
15 of the audit that in his or her opinion should be brought to the attention of that
16 minister including any corrective action proposed or taken.

17 (3) A person conducting an internal audit under this section may
18 require a telecommunications service provider to give the person access to any
19 records in the possession or control of the service provider that are relevant to
20 the audit.

Entitlement
to fee

21 **18.** -(1) A telecommunications service provider that provides
22 information to a person under section 16 or 17 is entitled to be paid the
23 prescribed fee for providing the information.

Notification
simultaneous
interception
capability

24 **19.** A telecommunications service provider must notify the Minister
25 when-

26 (a) in respect of any particular transmission apparatus, the increased
27 number of simultaneous interceptions that the service provider is required, as a
28 result of a request referred to in subparagraph 7(d)(ii), to be capable of enabling
29 is 75% or more of the maximum number that is applicable under that
30 subparagraph;

1 (b) the number of simultaneous interceptions that the service
2 provider is required, under sections 6, to 9, to be capable of enabling is 75%
3 or more of the global limit that is applicable under section 10.

4 20. -(1) A telecommunications service provider must, on the
5 request of the Nigeria Police or the State Security Service, provide a list of
6 the names of the persons who are employed by or carrying out work for the
7 service provider who may assist in the interception of communications.

Persons engaged
in interceptions

8 (2) A telecommunications service provider must provide any
9 changes to the list to the agency who made the request.

10 (3) The Nigeria Police or the State Security Service may conduct
11 an investigation for the purposes of a security assessment of any of those
12 persons who consent to the investigation.

13 21. -(1) If the prescribed conditions are met, a telecommunications
14 service provider that provides under this Act prescribed specialized
15 telecommunications support to the Nigeria Police ,the State Security
16 Service or any law enforcement agency is entitled, on request, to be paid an
17 amount determined in accordance with the regulations for providing that
18 support.

Specialized
telecommunications
support

19 (2) The amount must be paid by the agency that received the
20 specialized telecommunications support.

21 22. -(1) A telecommunications service provider that acquires
22 transmission apparatus referred to in subsection 8(2) must, before using it in
23 providing telecommunications services, submit to the Minister a report in
24 the prescribed form and manner containing the following information:

Mandatory
reporting
acquisition of
transmission
apparatus

25 (a) the prescribed information concerning the extent to which the
26 service provider meets operational requirements in respect of the
27 transmission apparatus; and

28 (b) any prescribed information relevant to the administration of
29 this Act.

30 (2) A telecommunications service provider must, at the request of

1 the Minister, submit a report or further report in the form and manner, and within
2 the period, that the Minister specifies containing the information referred to in
3 paragraphs (1)(a) and (b) and any additional related information that the Minister
4 specifies.

Statement

5 (3) Every report submitted under this section must include a written
6 statement certifying that it does not contain any untrue statements or omissions
7 of material facts, that it fairly presents the telecommunications service
8 provider's operations at the time of submission and that the signator has taken
9 steps to ensure the report's accuracy and promises to correct any material error
10 that is detected in the report after its submission and to submit a revised report to
11 the Minister as soon as possible, with another similar written statement
12 accompanying it.

Signator of
statement

13 (4) The statement must be signed-

14 (a) if the telecommunications service provider by one of its officers or
15 directors; and

16 (b) in any other case, by an individual who is an owner of the
17 telecommunications service provider or by an officer or a director of a
18 corporation that is an owner of the telecommunications service provider.

No redundant
performance
required

19 23. If two or more telecommunications service providers have, in
20 effect, the same obligation under this Act in connection with any given
21 transmission apparatus or a given interception and anyone of them performs that
22 obligation, it is deemed to be performed by all.

23 EXEMPTIONS

Exemption
regulation

24 24. -(1) The President may, on the recommendation of the Minister, by
25 regulation, exempt any class of telecommunications service providers from all
26 or part of the obligations under any of sections 4, 7 to 9, 13, 14 and 26 or under
27 any regulations made for the purposes of those sections.

28 (2) Before making or amending such a regulation, the President must
29 consider-

30 (A) the extent to which the exemption would adversely affect national

1 security or law enforcement;

2 (b) whether the telecommunications service providers can comply
3 with the obligations from which they would be exempted;

4 (c) whether "the costs of compliance with those obligations would
5 have an unreasonable adverse effect on the business of the
6 telecommunications service providers; and

7 (d) whether compliance with those obligations would
8 unreasonably impair the provision of telecommunications services to
9 Nigerians.

10 (3) In the regulation, the President may include any conditions that
11 the he considers appropriate and must fix its term for a period of not more
12 than two years.

13 ADMINISTRATION

14 25. -(1) For the purposes of the administration of this Act, the Designation
15 Minister may designate persons or classes of persons to exercise powers in
16 relation to any matter referred to in the designation.

17 (2) Designated persons are to receive a certificate attesting to their
18 designation and must, on request, present the certificate to any person
19 appearing to be in charge of any place that they enter.

20 26. -(1) A person who is designated to verify compliance with this Authority
to enter
21 Act may, for that purpose, enter any place owned by, or under the control of,
22 any telecommunications service provider in which that person has
23 reasonable grounds to believe there is any document, information,
24 transmission apparatus, telecommunications facility or any other thing to
25 which this Act applies.

26 (2) The designated person may, for the purpose of verifying
27 compliance with this Act-

28 (a) examine any document, information or thing found in the place
29 and open or cause to be opened any container or other thing;

30 (b) examine or test or cause to be tested any telecommunications

1 facility or transmission apparatus or related equipment found in the place;

2 (c) use, or cause to be used, any computer system at the place to search
3 and examine any information contained in or available to the system;

4 (d) reproduce, or cause to be reproduced, any information in the form
5 of a printout, or other intelligible output, and remove the printout, or other
6 output, for examination or copying; and

7 (e) use, or cause to be used, any copying equipment or means of
8 telecommunication at the place.

9 (3) The owner or person in charge of the place and every person who is
10 in the place must give all assistance that is reasonably required to enable the
11 designated person to verify compliance with this Act and must provide any
12 documents, data and information that are reasonably required for that purpose.

13 (4) The designated person, when entering a place referred to in
14 subsection (1), may be accompanied by any person chosen by the designated
15 person.

Authority to
issue warrant

16 27. -(1) If the place referred to in subsection 30(1) is a dwelling-house,
17 the designated person is not authorized to enter it without the consent of the
18 occupant except under the authority of a warrant issued under subsection (2).

19 (2) On ex parte application, a judge may issue a warrant authorizing a
20 designated person who is named in it to enter a dwelling-house, subject to any
21 conditions that may be specified in the warrant, if the justice is satisfied by
22 information on oath that-

23 (a) the dwelling-house is a place referred to in subsection 34(1);

24 (b) entry to the dwelling-house is necessary for the purpose of
25 verifying compliance with this Act; and

26 (c) entry was refused by the occupant or there are reasonable grounds
27 to believe that entry will be refused or that consent to entry cannot be obtained
28 from the occupant.

Entry onto
private property

29 28. -(1) For the purpose of gaining entry to a place referred to in
30 subsection 34(1), a designated person may enter private property and pass

1 through it, and is not liable for doing so. For greater certainty, no person has
2 a right to object to that use of the property and no warrant is required for
3 entry onto the property unless the property is a dwelling house.

4 (2) A person "may, at the designated person's request, accompany
5 the designated person to assist them to gain entry to the place referred to in
6 subsection 34(1) and is not liable for doing so.

7 **29.** In executing a warrant to enter a dwelling-house, a designated Use of force
8 person must not use force unless they are accompanied by a peace officer
9 and the use of force has been specifically authorized in the warrant.

10 **30.** -(1) A person must not knowingly make a false or misleading
11 statement or provide false or misleading information, in connection with
12 any matter under this Act, to a designated person who is carrying out their
13 functions under section 34. False statements
or information

14 (2) A person must not obstruct or hinder a designated person who
15 is carrying out their functions under section 34.

16 ADMINISTRATIVE MONETARY PENALTIES

17 **31.** Every person who contravenes a provision, order, requirement Violations
18 or condition designated under subparagraph 64(1)(p)(i) commits a
19 violation and is liable to an administrative monetary penalty not exceeding
20 the prescribed maximum or, if no maximum has been prescribed, to a
21 penalty not exceeding N50,000, in the case of an individual, and N250,000,
22 in any other case.

23 **32.** For the purposes of any of sections 39 and 41 to 53, the Designation
24 Minister may designate persons or classes of persons to exercise powers in
25 relation to any matter referred to in the designation.

26 NOTICES OF VIOLATION

27 **33.** -(1) A designated person may issue a notice of violation and Issuance and
service
28 cause it to be served on a person if they believe on reasonable grounds that
29 the person has committed a violation.

30 (2) The Minister may establish the form and content of notices of

- 1 violation, but each notice of violation must-
- 2 (a) set out the name of the person believed to have committed the
- 3 violation;
- 4 (b) identify the violation;
- 5 (c) set out the penalty that the person is liable to pay;
- 6 (d) inform the person that they may, within 30 days after the day on
- 7 which the notice is served or within any longer period specified in it, either pay
- 8 the penalty set out in the notice or make representations with respect to the
- 9 alleged violation or penalty - including any representations about entering into a
- 10 compliance agreement - and set out the manner for doing so; and
- 11 (e) inform the person that, if they fail to pay the penalty or make
- 12 representations in accordance with the notice, they will be considered to have
- 13 committed the violation and the penalty will be imposed.
- 14 (3) The amount of a penalty is, in each case, to be determined taking
- 15 into account the following matters:
- 16 (a) that administrative monetary penalties have as their purpose to
- 17 encourage compliance rather than to punish;
- 18 (b) the nature and scope of the violation;
- 19 (c) the person's history of prior violations or convictions - or
- 20 compliance agreements entered into - under this Act during the five-year period
- 21 immediately before the violation;
- 22 (d) the cumulative amount of the penalties that may be imposed for any
- 23 violation in respect of which section 48 applies;
- 24 (e) any prescribed criteria; and
- 25 (f) any other relevant matter.

26 DETERMINATION OF RESPONSIBILITY AND PENALTY

- Options
- 27 34. -(1) A person who is served with a notice of violation must, in
- 28 accordance with the notice, pay the penalty set out in the notice or make
- 29 representations with respect to the amount of the penalty or the acts or omissions
- 30 that constitute the alleged violation.

1 (2) A person is deemed to have committed the violation if they
2 either pay the penalty in accordance with the notice of violation or do not
3 pay the penalty and do not make representations in accordance with the
4 notice of violation.

5 35. -(1) The person alleged to have committed a violation may
6 make representations to a designated person other than the one who issued
7 the notice of violation.

Making
representations

8 (2) The designated person to whom the representations are made
9 must either-

Compliance
agreement or
decision

10 (a) enter into a compliance agreement with the person on behalf of
11 the Minister;

12 (b) decide on a balance of probabilities whether the person
13 committed the violation and, if so, impose the penalty set out in the notice of
14 violation, a lesser penalty or no penalty, taking into account the matters
15 mentioned in subsection 41(3).

16 The designated person must cause notice of any decision made
17 under paragraph (b) to be issued and served on the person together with
18 written reasons for the decision and notice of the person's right of appeal
19 under subsection 44(1).

20 (3) A compliance agreement-

21 (a) may include any terms that the designated person considers
22 appropriate including a requirement that the person alleged to have
23 committed a violation give reasonable security in a form and an amount that
24 the designated person considers satisfactory for the person's performance of
25 the agreement; and

26 (b) must provide for payment by the person alleged to have
27 committed a violation to the Receiver General of a specified amount not
28 greater than the penalty set out in the notice of violation if the person does
29 not comply with the agreement.

30 (4) Entry into a compliance agreement ends the violation

1 proceedings and precludes any further violation or offence proceedings in
2 relation to the act or omission in question.

3 (5) The Minister may issue and serve a notice of default on a person
4 who has entered into a compliance agreement but has not complied with it. On
5 service of the notice, the person is liable to pay without delay the amount
6 provided for in the agreement, failing which, the Minister may realize any
7 security for the person's performance of the agreement.

8 APPEAL TO MINISTER

Right of
Appeal

9 36. -(1) A person served with notice of a decision made under
10 paragraph 43(2)(b) may, within 30 days after the day on which the notice is
11 served or within any longer period that the Minister allows in accordance with
12 the regulations, appeal the decision to the Minister.

13 (2) On an appeal, the Minister may confirm, set aside or vary the
14 decision of the designated person.

15 RULES ABOUT VIOLATIONS

Vicarious
liability acts
of employees,
agents and
mandataries

16 37. A person is liable for a violation that is committed by the person's
17 employee acting in the course of his or her employment or the person's agent or
18 mandate acting within the scope of his or her authority, whether or not the
19 employee, agent or mandate who actually committed the violation is identified
20 or proceeded against.

Officers of
corporations,
etc

21 38. An officer, director, agent or mandate of a person other than an
22 individual that commits a violation is a party to the violation if he or she directed,
23 authorized, assented to, acquiesced in or participated in the commission of the
24 violation and is liable to the administrative monetary penalty provided for that
25 violation whether or not the person that committed the violation has been
26 proceeded against under sections 41 to 43. For greater certainty/an officer or
27 director, or any agent or mandate who is an individual, is liable only to the
28 penalty provided in respect of an individual.

Defence of due
diligence

29 39. A person is not liable for a violation if they establish that they
30 exercised due diligence to prevent the commission of the violation.

1	40. A violation that is committed or continued on more than one	Continuing violation
2	day constitutes a separate violation for each day on which it is committed or	
3	continued.	
4	41. Any proceedings in respect of a violation may be instituted at	Limitation period or prescription
5	any time within, but not later than, two years after the day on which the	
6	subject matter of the proceedings arose.	
7	42. If it is possible to proceed with any act or omission as a	Violation or offence
8	violation and it is also possible to proceed with it as an offence, proceeding	
9	in one manner precludes proceeding in the other.	
10	43. In any proceeding, in the absence of evidence to the contrary, a	Admissibility of documents
11	document that appears to be a notice issued under subsection 41(1) or 43(2)	
12	or (5) or a certificate issued under subsection 53(1) is presumed to be	
13	authentic and is proof of its contents.	
14	OFFENCES AND PUNISHMENT	
15	44. A person must not do any of the following things in performing	Misleading statements and information
16	any obligation under this Act or in any application, declaration or report	
17	made under it-	
18	(a) knowingly make a false or misleading statement or knowingly	
19	provide false or misleading information; and	
20	(b) knowingly omit to state a material fact or to provide material	
21	information.	
22	45. Every person who wilfully contravenes subsection 4(1) or (2),	Offence
23	any of sections 6 to 9, an order made under subsection 14(1) or any	
24	regulations made under paragraph 64(1)(a) commits an offence and is liable	
25	on prosecution by summary conviction-	
26	(a) in the case of an individual, to a fine not exceeding N100,000;	
27	(b) in any other case, to a fine not exceeding N500,000.	
28	46. -(1) Every person who contravenes subsection 11(6), section	Offence
29	22, 26 or 48 or a condition referred to in subsection 28(3) is guilty of an	
30	offence punishable on summary conviction and liable-	

1 (a) in the case of an individual, to a fine not exceeding N25,000 for a
2 first offence, or N50,000 for a subsequent offence;

3 (b) in any other case, to a fine not exceeding N100,000 for a first
4 offence, or N250,000 for a subsequent offence.

5 (2) Every person who contravenes subsection 34(3) or 38(1) or (2) is
6 guilty of an offence punishable on summary conviction and liable to a fine not
7 exceeding N15,000.

Offence

8 47. Every person who contravenes any provision of this Act or a
9 regulation made under this Act, except in the case of an offence referred to in
10 sections 49 and 50, and is guilty of an offence punishable on summary
11 conviction and liable to a fine not exceeding N250,000.

Consent of
Attorney
General
required

12 48. A prosecution is not to be commenced in respect of an offence
13 referred to in section 55 or subsection 50(1) without the consent of the Attorney
14 General.

Defence of
due diligence

15 49. A person is not to be convicted of an offence under this Act, other
16 than for a contravention of subsection 38(1) or section 54 or an offence referred
17 to in section 55, if they establish that they exercised due diligence to prevent the
18 commission of the offence.

Officers of
corporations,
etc

19 50. If a person other than an individual commits an offence under this
20 Act, every officer, director, agent or mandate of the person who directed,
21 authorized, assented to, acquiesced in or participated in the commission of the
22 offence is a party to and guilty of the offence and liable on conviction to the
23 punishment provided for the offence whether or not the person that committed
24 the offence has been prosecuted or convicted. For greater certainty, an officer or
25 director, or any agent or mandate who is an individual, is liable only to the
26 punishment provided in respect of an individual.

Continuing
offence

27 51. If an offence under this Act is committed or continued on more than
28 one day, the person who committed the offence is liable to be convicted for a
29 separate offence for each day on which the offence is committed or continued.

Consolidated
Revenue
Fund

- 1 55. There is to be paid out of the Consolidated Revenue Fund the sums
2 required to meet the monetary obligations under subsections 12(3), 18(1) and
3 25(1).

EXPLANATORY MEMORANDUM

This Bill seeks to make provisions for telecommunications service providers to put in place and maintain certain capabilities that will facilitate the lawful interception of information transmitted by telecommunications and to provide basic information about their subscribers to the Nigerian Police, the State Security Service and any other law enforcement agency for the enhancement of national security.