**Government of the Republic of Trinidad and Tobago**

**Ministry of the Attorney General and Legal Affairs**

Submission of Information for Study on Freedom of Expression in the Telecommunications and Internet Access Sector

1. ***Laws, regulations and other measures (including where applicable contractual arrangements and extra-legal action) that may permit authorities to require Telecommunications and Internet Service Providers to:-***
2. ***Suspend or restrict access to websites or internet and telecommunications networks;***
3. ***Provide or facilitate access to customer data.***
4. **Telecommunications Act. Chap. 467:31, Section 18 (1) (*m*):**

“18. (1) Subject to the provisions of this Act, the Authority may exercise such functions and powers as are imposed on it by this Act and in particular—

(m) investigate complaints by users, operators of telecommunications networks, providers of telecommunications and broadcasting services or other persons arising out of the operation of a public telecommunications network, or the provision of a telecommunications service or broadcasting service, in respect of rates, billings and services provided generally and to facilitate relief where necessary”

1. **Clauses D 8 & 9 of the Standard Concession Agreement issued pursuant to Section 21 (1) of the Telecommunications Act**

“Content and Compliance with Broadcasting Code

D8. The concessionaire shall at all times in the provision of the Broadcasting Services comply with the provisions of the Broadcasting Code promulgated in accordance with the Act.

D9. Without prejudice to Condition D8, and until such time as a Broadcasting Code is promulgated in accordance with the Act, the concessionaire shall not:-

(a) transmit any programme, information or other material which degrades or portrays in a negative manner or discriminates against or encourages discrimination against any person or group by reason of race, origin, class, religion or sex;

(b) transmit any programme, information or other material which is hostile to any country; or,

(c) broadcast programme, information or other material which endangers the security of the Republic of Trinidad and Tobago, violates any law, is of a defamatory nature, is subversive to peace or public order or is otherwise contrary to the laws of Trinidad and Tobago.”

**(iii) Electronic Transactions Act, Chap. 22:05, Section 51**

51. (1) If an intermediary or telecommunications service provider has actual knowledge that the information in a data message or an electronic record gives rise to civil or criminal liability then, as soon as is practicable after acquiring such knowledge, the intermediary or telecommunications service provider shall—

(a) remove and secure the information from any information system within the control of the intermediary or telecommunications service provider and cease to provide or offer to provide services in respect of that information or take any other action authorized by written law or in accordance with the established code of conduct; and

(b) in the case of criminal liability, notify the appropriate law enforcement authority of the relevant facts and of the identity of the person for whom the intermediary or telecommunications service provider was supplying services in respect of the information, if the identity of that person is known to the intermediary or telecommunications service provider.

(2) An intermediary or telecommunications service provider is not liable, whether in contract, tort, under statute or otherwise, to any person, including any person on whose behalf the intermediary or telecommunications service provider provides services, in respect of information in a data message or an electronic record, for any action the intermediary or telecommunications service provider takes, in good faith, in exercise of the powers conferred by, this section.

(3) Any person who lodges a notification of unlawful activity with an intermediary or telecommunications service provider, knowing that it materially misrepresents the facts, commits an offence and is liable for damages for wrongful removal of the information in a data message or electronic record under subsection(1).”

**(iv) Interception of Communications Act, Chap. 15:08, Section 6**

“6. (1) Except as provided in this section, a person who intentionally intercepts a communication in the course of its transmission by means of a telecommunications network commits an offence and is liable on summary conviction to a fine of five hundred thousand dollars and to imprisonment for seven years.

(2) Notwithstanding any other law, a person does not commit an offence under this section if—

(a) the communication is intercepted in obedience to a warrant issued by a Judge under section 8 or 11;

(b) the communication is intercepted by an authorised officer—

(i) in the interest of national security;

(ii) for the prevention or detection of an offence for which the penalty on conviction is imprisonment for ten years or more, and includes an offence where death, imprisonment for the remainder of a person’s natural life or life imprisonment is the penalty fixed by law;

(iii) for the purpose of safeguarding the economic well-being of the State; or

(iv) for the purpose of giving effect to the provisions of any international mutual assistance agreement, and any communication so intercepted may be used for the purpose of an application under section 8 or 11, but shall not be admissible as evidence in any criminal proceedings;

(c) he has reasonable grounds for believing that the person to whom or by whom the communication is transmitted consents to the interception;

(d) the communication is intercepted as an ordinary incident in the course of employment in the provision of telecommunications services;

(e) the communication is not a private communication;

(f) the communication is a stored communication and is acquired in accordance with any other law; or

(g) the interception is of a communication transmitted by a private telecommunications network and is done by a person who has—

(i) a right to control the operation or use of the network; or

(ii) the express or implied consent of a person referred to in subparagraph (i).

(3) The Court by which a person is convicted of an offence under this section may order that any device used to intercept a communication in the commission of the offence shall be forfeited and disposed of as the Court may think fit.

(4) For the purpose of subsection (1), a communication shall be taken to be in the course of transmission by means of a telecommunications network at any time when the network by means of which the communication is being or has been transmitted is used for storing the communication in a manner that enables the intended recipient to collect it or otherwise have access to it.

(5) Information lawfully intercepted under this Act is exempt information for the purposes of the Freedom of Information Act.”

1. ***Laws, regulations and other measures (including where applicable contractual arrangements and extra-legal action) on the public disclosure of requests made or actions taken to (a) suspend or restrict access to websites and telecommunications networks and the requests to provide or (b) facilitate access to costumer data***

**Telecommunications Act. Chap. 467:31, Section 18 (1) (*q*)**

“18. (1) Subject to the provisions of this Act, the Authority may exercise such functions and powers as are imposed on it by this Act and in particular—

(q) establish a consumer complaints committee to collect, decide on and report on consumer complaints, such reports to be included in the Authority’s annual report”

1. ***Laws, regulations and other measures (including where applicable contractual arrangements and extra-legal action) governing the activities of private entities that provide network components or related technical support, such as network equipment providers, submarine cable providers , and Internet exchange points***

**Telecommunications Act. Chap. 467:31, Sections 32, 36, 40, 48**

“32. Any terminal equipment may be connected to a public telecommunications network where the Authority, after consultation with the concessionaire, has certified such terminal equipment as—

(a) being safe for the user;

(b) being in compliance with international standards, and environmental health and safety standards including standards for electromagnetic radiation and emissions;

(c) meeting requirements of electromagnetic compatibility if specified;

(d) not posing a risk of harm to the network;

(e) effectively utilising the electromagnetic spectrum and preventing interference between

satellite and terrestrial-based systems and between terrestrial systems; and

(f) being compatible with the network.

36. (1) Subject to subsection (2), no person shall—

(a) establish, operate or use a radio-communication service;

(b) install, operate or use any radio-transmitting equipment; or

(c) establish, operate or use any radiocommunication service on board any ship, aircraft, or other vessel in the territorial waters or territorial airspace of Trinidad and Tobago, other than a ship of war or a military aircraft or satellite registered in Trinidad and Tobago, without a licence granted by the Authority.

40. Radio-communication equipment shall not be operated in a manner likely to cause harmful interference to any other means of telecommunication.

48. (1) The Authority shall, for the purpose of certifying or approving terminal equipment and other equipment to be installed or used for a public telecommunications network or telecommunications service or broadcasting service determine whether such equipment fulfils the criteria stipulated in section 32 and such other requirements as the Authority may prescribe.

(2) For the purpose of a determination made pursuant to subsection (1), the Authority may require that such equipment be submitted for testing by an inspector.

(3) The requirement for testing may be waived by the Authority, after consultation with the concessionaire or licensee, if the Authority is satisfied that the equipment has been certified in accordance with international standards.”

***4) Remedies available in the event of undue restrictions on Internet and telecommunications access or undue access to customer data.***

**Interception of Communications Act, Chap. 15:08, Section 18 ss. (8) & (9) and Section 23 ss. (2)-(6)**

18. (8) An authorised officer shall not disclose any communications data obtained under this Act, except—

(a) as permitted by the notice;

(b) in connection with the performance of his duties; or

(c) if the Minister directs such disclosure to a foreign government or agency of such government where there exists between the State and such foreign government an agreement for the mutual exchange of that kind of information and the Minister considers it in the public interest that such disclosure be made.

(9) A person who contravenes subsection (6), (7) or (8) commits an offence and is liable on summary conviction to a fine of three hundred thousand dollars and to imprisonment for five years.

23. (2) A person who intentionally discloses the contents of any communication—

(a) obtained by means of a warrant, to a person to whom he is not authorised to disclose the

communication;

(b) obtained in the course of the interception of communication to a person to whom he is not authorised to disclose the communication whether the interception occurred prior to or after the commencement of this Act; or

(c) obtained in contravention of this Act,

commits an offence and is liable on summary conviction to a fine of two hundred and fifty thousand dollars and to imprisonment for three years.

(3) Subsection (2) shall not apply to the disclosure of the contents of any communication obtained by means of a warrant which is made, in any criminal proceedings, to a person charged with an offence or to the attorney-at-law representing that person in those proceedings.

(4) A person who intentionally has in his possession communications intercepted under this Act and who is not authorised to have such communications commits an offence and is liable on summary conviction to a fine of one hundred thousand dollars and to imprisonment for two years.

(5) A person who intentionally has in his possession communications intercepted under this Act and who is not authorised to have such communications and who discloses such communications commits an offence and is liable on summary conviction to a fine of two hundred and fifty thousand dollars and to imprisonment for three years.

(6) No action shall be brought in any Court against a person or entity for any act done in good faith in pursuance of a warrant under section 8 or 11 or a direction under section 6(2)*(b)* to provide information, facilities or technical assistance.

1. Other relevant laws, policies or initiatives to promote or enhance internet accessibility and connectivity, including measures to promote network neutrality

* Universal Service Framework for Trinidad and Tobago

<https://tatt.org.tt/Portals/0/ConsultativeDocuments/Universality%20Framework/Universal%20Service%20Framework%20June%202012.pdf>

* Telecommunications Universal Service Regulations 2015

<https://tatt.org.tt/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=519&PortalId=0&TabId=222>

* Revision and Update of National ICT Plan for Trinidad and Tobago

<http://www.mpac.gov.tt/publications/smartt-national-ict-plan-2014-2018>

* Electronic Transactions Act, Chap. 22:05

<http://rgd.legalaffairs.gov.tt/laws2/alphabetical_list/lawspdfs/22.05.pdf>

**---oOo---**