



Students for the Promotion of International Law (SPIL), Mumbai



Treaty Appreciation Competition 2019

Module



**REVIEW CONFERENCE OF THE INTERNATIONAL COVENANT ON CIVIL AND
POLITICAL RIGHTS**

ARTICLE 2, ARTICLE 17 AND ARTICLE 19 OF THE ICCPR

Putania is a prosperous democratic nation-state, which has been at the forefront of the development of several critical modern communication technologies, including the internet. The enterprising citizens of Putania have developed groundbreaking technologies including search engines, social media networks and video sharing websites which have proven to be some of the most popular around the world. A number of major corporations like Zero Search and BasicallyFree which provide these services are concentrated in the Emoticon Valley located on Putania's West Coast.

Many around the world are jealous of Putania's prosperity, and routinely threaten to destabilize the Putanian Government by any means possible. As a result, Putania's government zealously attempts to fight these perceived threats by any means possible. One of the key components of its national security programme is the secretive Signals Intelligence Unit ("SIU"), which aims to predict and prevent foreign threats to Putanian national security.

Recently, nations around the world woke up to leaks to international media, from within the SIU, which exposed a sinister underbelly of the SIU's operations. According to these leaks, the SIU had been routinely collecting personal data of foreign nationals who utilize the services of Emoticon Valley firms. This data included personally identifiable private messages, emails, profiles and search histories, based upon executive orders and without any independent judicial review or oversight.

Additionally, citizens of Putania were (even more) shocked to learn that the SIU was collecting 'meta-data' on them. The collection of meta-data was authorized by a law, which allows for the SIU to make requests to a special Supreme Court of Surveillance ("SOS") for any information which is relevant to any 'national security investigation', which can force any company running an internet or communication service to provide data to the SIU. The SOS does not allow the Emoticon Valley companies to object to surveillance, and the decisions and proceedings of the SOS are highly confidential and not available outside of the SIU. The metadata information available under this program does not include the content of communications, but reveals information such as the name and location of the senders and receivers, the duration of the communication, and similar information that is not personally identified.

In the face of significant backlash from their users who were outraged at such invasions to their privacy, the companies of the Emoticon Valley began to balk at the information requests from

SIU, and began to create technologies that utilize end-to-end encryption, where the content of messages would be encrypted to every person except the sender and the receiver. While the SIU was indifferent to the mounting public pressure, it found that end-to-end encryption employed by some Emoticon Valley firms thwarted their efforts at collection of data at scale. In response, the Government of Putania hurriedly passed the Special Hacking Act (“**SHA**”) which requires all companies providing communications facilities to ensure that information can be technically made available to specified law enforcement authorities upon procurement of a warrant to that effect, without the knowledge of the users. Further, the SHA bans the import of any encryption tools except those specially licensed by the SIU. The SHA itself does not authorize the collection of information by any agency, but only mandates the creation of the so-called ‘backdoor’ to end-to-end encryption technologies.

While Putania is often the most visible country in terms of such developments, similar scenarios are playing out in the rest of the world. The Member States of the United Nations, concerned about the implications of such technologies and techniques on human rights, shall be convening to conduct a review of the relevant provisions of the International Covenant on Civil and Political Rights (“**ICCPR**”), to which they are contracting parties, in order to assess its relevance in light of the SIU disclosures. The member states are particularly concerned about the ambiguity of the ICCPR in light of the actions of the Putanian government. Specifically, the member states wish to clarify, through the review:

- 1) Whether Putania’s surveillance of non-citizens and foreign nationals violates the ICCPR in light of its scope under Article 2 of the ICCPR.
- 2) The applicability of Article 17 of the ICCPR to the surveillance of Putanian citizens by the SIU.
- 3) The applicability of Articles 17 and 19 of the ICCPR to the restrictions on the development of end-to-end encrypted communications technologies under the SHA.

Member States are expected to examine the applicability of the provisions of the ICCPR to the fact scenario described above, using available interpretive aids. The member states are expected to take a clear position on the applicability of the provisions of the ICCPR, and, if required, suggest appropriate measures for clarifying the scope of the applicability of the ICCPR to the acts in question. The member states may also argue that the acts in question are governed by other relevant provisions of the ICCPR or customary international law.

ANNEXURE

ARTICLE 2, 17 AND 19 OF THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS

Article 2

1. Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.
2. Where not already provided for by existing legislative or other measures, each State Party to the present Covenant undertakes to take the necessary steps, in accordance with its constitutional processes and with the provisions of the present Covenant, to adopt such laws or other measures as may be necessary to give effect to the rights recognized in the present Covenant.
3. Each State Party to the present Covenant undertakes:
 - (a) To ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity;
 - (b) To ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy;
 - (c) To ensure that the competent authorities shall enforce such remedies when granted.

Article 17

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

Article 19

1. Everyone shall have the right to hold opinions without interference.
2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
 - (a) For respect of the rights or reputations of others;
 - (b) For the protection of national security or of public order (ordre public), or of public health or morals.

