**FORUM:** Special Conference 2

**QUESTION OF:** Protecting civil privacy while maintaining national security

**SUBMITTED BY:** Iraq

THE SPECIAL CONFERENCE,

*Defining* civil privacy as the privacy of citizens, which is a responsibility of all governments, meaning governing bodies have to respect and support citizens’ privacy and limit their interference in these matters,

*Stating* national security as the utmost necessary protection of a nation from any internal or external threats,

*Indicating* data as the content of online or wireless communication and the history of information accessed online,

*Specifying* metadata as the information of the context of data communication, such as location and time,

*Recognizing* the right to privacy as being a right for people to make decisions independently and without unwarranted publicity and acknowledging such as being a fundamental human right,

*Recalling* the Universal Declaration of Human Rights (UDHR) adopted by the General Assembly on the 10th December 1948 as a great stepping stone in consolidating the fundamental right to civil privacy and establishing it as a universal human right that should be respected on the global scale,

*Acknowledging* that 168 states have signed the International Covenant on Civil and Political Rights in which Article 17 states that “no one shall be subjected to arbitrary or unlawful interference with his privacy”,

*Noting* the European Convention for the Protection of Human Rights as a further attempt to secure the protection of civil privacy within nations,

*Bringing to light* that the UN General Assembly resolution on the 18th December 2013, concerning the right to civil privacy in the digital age, was a key component of civil privacy in modern times,

*Reaffirming* the UN General Assembly resolution on the “Promotion and protection of human rights” on the 19th November 2014 as being another stepping stone to enhance this fundamental right among citizens worldwide,

1.     Implores that the UN create a separate body by the name of the UNNSO (United Nations National Security Organisation), composed of one elected representative for each UN Member State, which decides by majority vote, for the sole purpose of ensuring that the national security needs of each nation are met whilst not obstructing the civil privacy of its citizens by:

a) allowing all member states to collect private data independently, provided that their private data surveillance programmes are monitored and approved by the UNNSO through:

i.      a comprehensive analysis process of each state’s private surveillance programmes,

ii.     collaboration between the UNNSO and each state to achieve the ratification of surveillance programmes,

iii.   all necessary information, including files of surveillance records, from a member state being placed at the body’s disposal in order to prove that the state is abiding by international law,

b) facilitating ethical and necessary collection of metadata by:

i.      enforcing that all states come directly to the UNNSO to receive permission to collect metadata which can only be used to stop a threat to national security,

ii.     setting specific guidelines regarding what a country may consider a threat to national security, which is considered to consist of threats pertaining to terrorism and extremism

iii.   developing a decision-making process for all members of the UNNSO to determine whether the nation in question’s threat is of enough gravity to warrant their collection of metadata,

iv.   helping nations to collect metadata should a reasonable threat and need for help be proven and agreed to by three-fourths of the members of the UNNSO,

v.     requesting that private corporations do not provide metadata to states who have not been approved by the UNNSO to collect and receive metadata,

c) creating an algorithm which takes into account a country’s population and GDP in order to aid the UNNSO in assessing the national security needs of a state,

d) ensuring that all states go through the UNNSO should they wish to alter their national security policy regarding the collection of digital data;

2.     Calls upon the international judicial system of the United Nations to be responsible for the administration, adherence, and implementation of the decisions of the UNNSO, which could be enforced by, among other means, the intervention by the Security Council, to which degree can be decided by them, in the case of failure by said judiciary branches to administrate and implement the UNNSO’s decisions;

3.     Suggests that the UNNSO access the data in question by means of but not limited to:

a)     drawing on the resources of data collection programmes including PRISM and other similar domestic surveillance groups,

b)    the creation of a global data surveillance network owned and operated by the UNNSO,

c)     negotiating agreements, preapproved by the UNNSO, with data and internet providers to gain access to private data and metadata;

4.     Condemns the independent mass data collection of UN member states without permission and due process of the UNNSO and full awareness of the United Nations;

5.     Encourages citizens of all Member States to evaluate and protect their own online security to ensure the safety of a citizen’s data from a malicious organisation, which could then possibly leak a large database of a nation’s citizens’ personal information, by means such as:

a) providing better education on online security matters through inclusion in national education systems,

b) raising awareness on malicious cyber threats by a nation’s government at the earliest convenience through public service announcements, on the same level as a physical security threat,

c) establishing communication between national security and law enforcement forces on a local level and UNNSO representatives in order to cyber threats and invasion of a citizen's civil privacy as a local security issue on the same level as physical threats;

6.     Strongly recommends that member states actively participate in the extradition of persons who have violated national security laws and sought refuge in the territory of said member state, in order to ensure that said persons are tried under the legal system in the nation in which the crime was committed and to deter future agents from attempting to put the integrity of sovereign nations at risk, except in cases when the violator has discovered information and intelligence which proves to break international law, in which case the violator will not be tried in the country where the crime was committed, but by the international judicial system of the United Nations;

7. Urges all the immediate recognition by the UNNSO of organizations such as: Interpol, Europol and other international law organizations that deal with online data so as to not prevent them working for an assessment period should the UNNSO come to existence.