**FORUM: General Assembly 1**

**QUESTION OF:  Protecting individual rights to privacy in the digital age**

**SUBMITTED BY: Hungary**

**CO-SUBMITTER: The Slovak republic, Brazil, The Netherlands, Croatia, Ethiopia, Libya, Holy see, Cuba, Ethiopia, Turkey, Rwanda, USA, New Zealand, Czech republic, Libya, Lithuania, Turkmenistan, Argentina, Zimbabwe**

THE FIRST GENERAL ASSEMBLY

*Recalling* the previous relevant United Nations resolution 69/166 (2013) which illustrates the growing attention the United Nations are paying to the issue but also that this has not yet led to significant change on a national level,

*Understanding that* human rights are the basic rights and freedoms to which all humans are considered entitled: the right to life, liberty, freedom of thought and expression, and equal treatment before the law,

*Deeply concerned* about the wellbeing of whistleblowers,

*Bearing in mind* that the Internet is commonly used for personal communication purposes due to its easy accessibility and availability,

*Deeply disturbed* by the adverse impact of surveillance and/or interception of communications including the collection of personal data that it may have on the action and adherence of the human rights,

*Declaring that* information online can never be fully kept private and that Internet corporations such as Google, Facebook or Microsoft are not decreasing the vulnerability of this information,

*Conscious that* as technology develops, so should the level of privacy of the information of the people using the technology,

*Aware that* keeping individual rights to privacy intact and the fact that no personal information on the digital media should be violated,

*Recognizing that* the technological world advances each and every day as improvements are made to invent and discover more sophisticated technology,

*Recalling* article 12 of the United Nations declaration of human rights which states that “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks,

1. Suggests the creation of a UN branch, named United Nations Council for the Protection of Digital Rights (UNCPDR) dedicated to the handling of international cyber surveillance programs which will:
   1. be a branch directly under the OHCHR, and report any incidences of mass surveillance that are deemed unethical to the public
   2. govern a body of technical professionals which are allowed to interfere in a country’s digital situation if:
      1. that country is violating human rights by damaging the digital privacy of its citizens so severely that infringing on its national sovereignty is in the best interests of the citizens of this country
      2. a ⅔ majority of the members of the UNCPDR agree on making use of this body
   3. consist of a selection of the council members, where:
      1. The UNCPDR will consist of 50 members from 25 member states, elected within their own country;
      2. The UNCPDR will have 5 semi-permanent members, and 20 cycling members where permanent members serve for 3 years before reevaluation cycling members serve for 1 year before reevaluation
      3. the cycled member states and the permanent member states directed at the discretion of the OHCHR
      4. countries that are non-members of the UNCPDR will be allowed to participate in debate on topics that lie in their direct interests, but will not have a vote;
2. Calls upon all member states to declare all current operations in place for mass surveillance of their respective populations through which the UN sets a 6 month review period in which individual projects are reviewed and if deemed necessary, kept classified until the operation has ended or the information no longer poses a risk to a person’s physical well being;
3. Acknowledges the need for individual member states to increase the level of online surveillance on the population which will be done by monitoring individuals as soon there is a threat made them by an online post, it will assess threat level and take early action if needed if these statements;
   1. explicitly allude to physical violence or bodily harm or repeated dangerous behavior
   2. mention improvised explosive devices;
4. Recognizes that certain concessions must be made for cultural differences in regards to what may be posted online, as:
   1. the regulation and censorship of the internet is deeply tied into a country's respective culture, which the UNCPDR will take into account when reviewing the censorship employed by member nations, the UNCPDR will also be in charge of negotiating with states if the censorship level is deemed unreasonable,
   2. the right to free speech must be respected by individual governments, however terrorist accounts such as I.S on twitter must be targeted on behalf of all member nations;
5. Urges all states to reduce bulk collection of metadata inside & especially outside national borders through:
   1. asking member states to declare current surveillance programs in place to the UNCPDR for review on ethical grounds
   2. asking member states to take national action to prevent unnecessary use of this tool by establishing protocol and guiding principles regarding who should be observed and when;
6. Asks that interception of the communications in foreign territories be treated with the same graveness as unauthorized breaches of airspace, where:
   1. a warrant must be granted by the UNCPDR and the nation of which the person being observed is in
   2. the host nation must be made aware of whom is being observed within their own country by the outside organization
   3. the host nation will need to be provided with adequate reasoning for this surveillance and must sign off on the same warrant
   4. asks that special branches be set up especially to handle these warrants so as not to defeat the purpose of surveillance by slowing it down due to bureaucratic hold-ups;
7. Proclaims to protect the rights of the Multi national corporations (MNC) in terms of protecting and encrypting their information to stop surveillance outside of official government branches, which will:
   1. give MNC’s power to not hand over information with simply a national warrant for information if the person observed is of a different nation and a person who is of more than one nationality may be observed by all the respective nations they are officially a part of
   2. grant MNCs power to ask for rationale before granting access to a person's data unless it is a matter of immediate national security however governments may refuse to provide this information if the information receives the top 4 security ratings of their intelligence system;
8. Strongly suggests that an international covenant regarding mass surveillance in domestic & international contexts be established and that the International Covenant on Civil Rights & Political Rights be used as a legal principle until the International covenant on mass surveillance is established;
9. Proposes the recognition of whistleblowers and helping them by the following but not limited to:
   1. providing economic help
   2. ensuring personal protection;
10. Further asks that all member states strive to pass legislation regarding the rights of foreign nationals under their own mass surveillance policies by:
    1. establishing rights such as the right to privacy, unless previous patterns of substantially dangerous actions have been proven; or the right to association with the same conditions applying
    2. requesting that such legislation be passed in a span of 3 years, or by 2018;
11. Further urges that legislative steps be taken to support and inherently protect the right to information (specifically in the media context) and counsel (in the legal context) in relation to mass surveillance, such as:
    1. furthering existing laws pertaining to breaches of attorney-client privilege by  state actors, specifically to adapt to the new platform of cyberspace
    2. developing further laws that support journalistic endeavors, and adapt them to protect interviewees to make them immune to fear of government surveillance and its resulting repercussions to a certain extent;
12. Supports the increase in oversight of national intelligence agencies, their budgets and capabilities by conducting bi-yearly surveys and checks to prevent unchecked developments of capabilities, and power;
13. Urges nations to increase transparency on all forms of surveillance by:
    1. disclosing the findings of surveys and checks found in Clause 12 in yearly reports to a certain extent, so as not to endanger military and security operations
    2. mandating internet-based corporations and conglomerates to summarize their terms of use, and emphasizing those elements that can be interpreted to infringe on the human right to privacy before the user utilizes the services for the first time where current users will be notified at length of any changes to the aforementioned terms of use by the corporations or conglomerates
    3. urging governments inform their citizens of ways to improve their privacy themselves.