**FORUM:** General Assembly 3

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

**SUBMITTED BY:** The People’s Republic of China

GENERAL ASSEMBLY 3,

*Acknowledging* the harmful impacts of and issues created by the World Wide Web, and the social media and other digital platforms, contained therein,

*Noting* that article 17, comment No.16 of the International Covenant on Civil and Political Rights incentivises states to apply forceful measures to intercept unlawful retention, processing and the utilisation of confidential personal data stowed by public authorities and business enterprises,

*Aware of* the Golden Shield Programme in place in China which makes use of large-scale Deep Packets of Inspection technology to block access to websites and media based on keyword detection.

*Alarmed by* the unlawful and harmful impacts of buying and selling of personal information and data by, but not limited to companies and organisations, due to the interception and surveillance of these communications by the organisations,

*Bearing in mind* the lack of laws and legislations regarding this topic globally, ensuring that the World Wide Web remains prone to attacks,

1. Urges states to impose mass surveillance and monitor internet usage and illegal activity to improve the use of the World Wide Web aiming to create a digital sovereignty by methods but not limited to:
   1. creating national and regional government branches to monitor internet usage
   2. encrypt all personal data found
   3. setting up firewalls to block any sites to meet criteria including but not limited to:
      1. affiliation with terrorists and their actions
      2. containment of content against the government;
2. Encourages states to educate the general population on their digital footprint through:
   1. media campaigns advocating about but not limited to:
      1. search history
      2. what content is categorised as illegal
      3. censored websites and networks
      4. the data that different websites often gather about their users
      5. the data that search engines often collect regarding their users which may or may not be sold to third-party advertisers
      6. virtual impersonations by criminals
   2. school courses to educate children regarding the usage of the World Wide Web to their optimal advantage;
3. Requests states to impose new legislation that serves as a disincentive to engage in unlawful hacking of personal data and against the access of censored and illegal sites through the use of VPN and hacking, such as but not limited to:
   1. the increase in the penalty given to cybercriminals to at least 12 months onward depending on the seriousness and outwardly harmful nature of said crime
   2. increasing the protection and encryption of personal data collected by states and organisations;
4. Further requests states to monitor their citizens more by methods such as but not limited to:
   1. using facial recognition technology in public places
   2. monitoring people’s shopping habits online
   3. installing robot police in public places
   4. stopping pedestrians at random to check their phones
   5. tracking people’s social media habits
   6. mandating that people download an app that allows the government to monitor the phone and see its contents at its discretion
   7. increasing the amount of CCTV cameras in public spaces;
5. Instructs states to put the Golden Shield Programme in place to censor the aforementioned kinds of websites and utilise its Deep Packet Inspections to block access based off keyword searches;
6. Suggests states to put a social credit system into place as an incentive for citizens to abide by the new laws wherein they may either be rewarded for their lawful behaviour or punished for their unlawful behaviour:
   1. such rewards and punishments that may affect their status in the social credit system would also determine the internet access they can have, such as but not limited to:
      1. websites
      2. platforms
      3. media