**FORUM:** Human Rights Council

**QUESTION OF:** Examining human rights implications of mass surveillance in the digital age

**MAIN SUBMITTER:** People’s Republic of China

**CO SUBMITTERS:** Democratic People’s Republic of Korea, the Russian Federation, the Islamic Republic of Pakistan, the Federation of Malaysia, the Kingdom of Saudi Arabia, the United Arab Emirates, the Republic of Sudan, The Islamic Republic of Iran

HUMAN RIGHTS COUNCIL,

*Acknowledging* the transformative potential of digital technologies in fostering global development and innovation,

*Deeply Concerned* about the lack of surveillance currently present in European MEDCs that justify their lack of action,

*Keeping in mind* the role of surveillance practices in national safety, security, counter-terrorism, and sovereignty,

*Reaffirming* the principle of state sovereignty as outlined in the United Nations Charter, emphasizing that each nation has the sovereign right to implement measures to ensure its national security,

*Recognizing* that privacy is a capitalist socially constructed notion that arises out of the entitlement of the rich,

*Affirming* citizens’ right to privacy must not abrogate the right to life and safety,

*Recognizing* countries’ right to national sovereignty and involvement in their affairs,

1. Establishing stronger surveillance units within the nation to prevent crime and criminal activity that infringes on a nation's sovereignty in ways such as but not limited to:
   1. implementing surveillance devices provided by the People’s Republic of China in:
      1. public spaces,
      2. rural areas,
      3. areas at high risk of crime,
   2. moving towards increased development and usage of Artificial Intelligence (AI) technologies in the interest of:
      1. profiling individuals with malicious intent,
      2. monitoring online activity regarding counter-terrorism,
      3. automating and expediting the process of responding to threats in real time;
2. Creating an international organization that can be known as the Organization for Watchful and Efficient Network Surveillance (OWENS) to prevent confidential data theft and increase national surveillance in ways such as, but not limited to:
   1. refraining from further implementing illegal surveillance that violates the sovereignty of other nations,
   2. encouraging MEDCs to share their technological research on surveillance devices such as drones, closed-circuit television (CCTV) cameras, and AI profilers with LEDCs to improve surveillance in a beneficial manner,
   3. tracking individuals who seek to theft and interrogating them thoroughly by:
      1. tracking their location,
      2. invading and seizing any stolen information, while punishing the perpetrators for the sake of national security by following the existing laws,
      3. using advanced interrogation methods to deter any further violations of data breaches by other individuals,
      4. utilizing facial recognition technology developed by governments to identify individuals that threatened national security and safety effectively;
3. Securing the firewall of all surveillance units to prevent human rights violations from the unjust seizure of surveillance data via illegal means in ways such as, but not limited to:
   1. requesting global firewalls that the People’s Republic of China will provide due to their existing technological prowess to secure other nations from unfair national data theft while ensuring the following:
      1. creating non-disclosure agreements (NDA) between producers of firewalls and the governments of each nation to prevent data stealing,
      2. actively tracking and examine all producers and supporters of the global firewall to prevent any illegal and unjust usage,
   2. collaborating with the organization OWENS to detect any individuals who attempt to data steal and swiftly deal with them before trouble arises,
   3. preventing the collaboration of big tech companies and the government due to their notoriety for data theft;
4. Encourages the development and implementation of advanced domestic data security protocols to ensure that data collected through surveillance remains within national boundaries, including but not limited to:
   1. establishing secure, government-regulated data centers to store surveillance information, preventing unauthorized access through:
      1. encouraging the usage of virtual private networks (VPNs) to secure remote access to the organization’s data infrastructure preventing unexpected cyberattacks,
      2. standardizing an internet protocol (IP) that facilitates government data storage use only,
   2. using end-to-end encryption technologies to protect sensitive information during data transfer within the country through ways such as:
      1. verification processes ensuring safety during data transfer processes such as multi-factored authentication,
      2. periodically auditing data storage systems by national cybersecurity agencies to identify and address potential vulnerabilities;
5. Proposes increasing funding and resources for research and development in domestic cybersecurity technology, with a focus on:
   1. using artificial intelligence systems to identify and prevent hacking attempts in real-time through ways such as:
      1. utilizing machine learning algorithms to detect unusual patterns and anomalies in online network traffic,
      2. deploying real-time monitoring tools to identify and neutralize potential threats before they escalate,
      3. continuously updating and innovating AI models to adapt to emerging cybersecurity threats and hacking techniques,
   2. employing blockchain-based systems to ensure secure, tamper-proof storage of surveillance data,
   3. suggesting NGOs such as the United Nations Development Programme (UNDP) to fund nations in developing surveillance technologies;
6. Calls for the establishment of a robust cybersecurity education program aimed at the general public, which will pertain:
   1. organizing regular training sessions collaborating with the UN on recognizing cyber security hazards and social engineering tactics, such as keylogging, invasion of malware, and phishing attempts,
   2. establishing public awareness campaigns educating citizens on the importance of safeguarding personal information online through ways such as:
      1. implementing courses in school curriculums targeting the youth,
      2. encouraging the usage of various media forms such as radio, flyers, advertisements, newspapers, and short videos in the general communal environment;
7. Promoting the usage of facial recognition technology to combat terrorism, increase national security, and effectively identify individuals through ways such as but not limited to:
8. recommending MEDC countries to aid LEDCs in the construction and establishment of facial recognition technology infrastructures,
9. encouraging nations to facilitate domestic corporations to utilize such technology for enhanced national security,
10. implementing and developing AI algorithms to effectively and efficiently identify and profile individuals suspected of malicious intent.