HUMAN ASIA 휴먼아시아

I-Model UN UPR

TECHNOLOGY AND THE RIGHT TO PRIVACY

THE 2019 I-MODEL UN UPR

THEMATIC ISSUE GUIDE

Whilst advances in information communication technology are dramatically improving real-time communication, information-sharing and ordinary peoples' lives in numerous ways, it has become clear that new technologies are vulnerable to and can facilitate electronic surveillance and interception. This makes users of such technologies at risk of having their **right to privacy** violated. The right to privacy is a fundamental human right which is guaranteed under Article 12 of the UDHR and Article 17 of the ICCPR. Within the context of the I-Model UN UPR, privacy can be considered as the presumption that individuals have an area of autonomous development, interaction and liberty, free from State intervention and excessive unsolicited intervention by other uninvited individuals (see, for example, A/HRC/13/37, para. 11, and A/HRC/23/40, paras. 22 and 42). In 2013, the UN General Assembly called upon all States to respect and protect the right to privacy in digital communication, and reenforce Article 17 ensuring that citizens are not 'subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence,' and 'unlawful attacks on his or her honour and reputation'. Key issues include **mass surveillance, the collection of personal data, censorship** and **the role of businesses.**[1]

1. MEASURES TO PROTECT THE RIGHT TO PRIVACY VIS-A-VIS (MASS) SURVEILLANCE

Recent developments and revelations about digital mass surveillance have raised questions within the human rights community around whether such measures are consistent with existing legal standards and whether stronger safeguards are needed to uphold the right to privacy. The UN General Assembly noted that some may consider the very usage and exchange of personal information via digital means to be a kind of consensual compromise, for the return of digital goods and information. Yet firstly, technological surveillance may be undertaken without any kind of knowledge from those surveilled, and secondly, consumers may be unaware as to the extent, the exact nature, or the purpose for which their information is being collected. Furthermore, whilst many States continue to utilise forms of mass surveillance under the pretext of national security, the UN has determined that this is 'not permissible under international human rights law' (see A/HRC/33/29, para. 58). Issued identified by the UN vis-à-vis state

[1] **Please note that the provided topics within the overall thematic issue are a general guide only. Participants are encouraged to explore other topics related to the thematic issue aside from the ones outlined within this guide.**

surveillance include: **governmental access to user data of business enterprises, offensive intrusion software (hacking), attempts at weakening encryption and anonymity,** and **intelligence-sharing**. Some issues that delegates may wish to consider for the four States Under Review include:

- **Measures against harmful and/or hidden surveillance tactics**
  - **Spycams in public bathrooms in the ROK**
  - **Wiretapping of smartphones and the national intranet in the DPRK**
  - **Big data, QR codes, biometrics, artificial intelligence, and phone spyware technology in China**
  - **The use of FinFisher technology in Japan**
- **Public access to encryption and anonymity tools in online spaces**

2. MEASURES TO MONITOR THE COLLECTION OF PERSONAL DATA

Personal data typically refers to: data which can be used to identify a person, data which contains personal private information, and/or data which reflects personal use of services. States increasingly collect and use steadily available amounts of data related to the private lives of individuals, both through private and public mechanisms. Immense data streams from millions of individuals are being collected by personal computers, smartphones, smartwatches, fitness trackers and other technological wearables. The range and depth of the information collected and used are vast, from device identifiers, email addresses and phone numbers to biometric, health and financial data and behavioural patterns. Across various countries this commonly occurs without the knowledge of the persons concerned and without meaningful consent. The OECD has outlined eight recommendations for governing the protection of privacy and transborder flows of personal data: **1) collection limitation; 2) data quality; 3) purpose specification; 4) use limitation; 5) security safeguards; 6) openness; 7) individual participation; and 8) accountability.** Delegates are encouraged to review present policies and legislation towards businesses by States regarding these eight principles, and whether these have resulted in State citizens being rendered in positions of powerlessness on controlling their own personal data. Areas for the States Under Review could include:

- **Compulsory registration systems**
- **Collection of data through digital footprints on SNS/the Internet**
- **Biometrics (DNA, facial geometry, voice, retina or iris patterns and fingerprints) and data scanning devices**

- Protection of private communications
- Workplace surveillance
- Monitoring and collection of personal data by markets
- Protection of medical records and protection of confidentiality

3. MEASURES AGAINST FURTHER EXPLOITATION OF OTHER HUMAN RIGHTS CONCERNS

Other issues which may be explored regarding States' responsibility to respect and protect the right to privacy in the digital age, and whether adequate safeguards are in play, may include:

- Unrestricted Internet access and issues of censorship
  - VPNs
- APEC Cross-Border Privacy Rules
- The roles and responsibilities of businesses and their relationships with delegations
- The protection of medical data and medical records (including mental illnesses)
- Cyber Security Laws
- Crackdowns and equal access to technology and the Internet

OTHER USEFUL RESOURCES

- **UPR Database:** recommendations to the ROK, the DPRK, China, and Japan
- **UN Human Rights Council Report A/HRC/39/29:** The right to privacy in the digital age
- **Korean Progressive Network (Jinbonet):** Guide for Human Rights in the Information Society
- **Asia Pacific Data Protection and Cyber Security Guide 2018**
- **Law Reviews:** The Privacy, Data Protection and Cybersecurity Law Review
- **New Zealand Human Rights Commission:** Privacy, Data and Technology - Human Rights Challenges in the Digital Age
- **UNRISD:** Time for a Fourth Generation of Human Rights?
- **The Right to Privacy UPR Report:** The Philippines 2016