Senior Committee: **Human Rights Council**

Topic: **The Question of the Right to Privacy in the Digital Age**

Background Information

As per Article 12 of the Universal Declaration of Human Rights, *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation*[1]. This shows privacy as a basic human right and need, allowing one to live their lives away from unwanted scrutiny and intrusion. It is crucial to recognize that the exercise of the right to privacy is important for the realization of the right to freedom of expression and to hold opinions without interference and is one of the foundations of a democratic society[2].

Privacy has been described as the individual right to be free from intrusion, or as Warren and Brandeis affirm, *to be let alone*[3]. Most recently, privacy has been defined as being protected from intrusion as well as having control over one's information, restricting others' access to it. However, the increasing access to the world wide web at a global level has questioned and violated this right, being the cause of many data privacy and well as government surveillance scandals.

The Internet has been and continues to be the primary environment for informational privacy, as it is the place where most data is transferred, collected, and stored. Privacy concerns are

---

[1] United Nations (1948). *Universal Declaration of Human Rights*. [online] United Nations. Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights.

[2] 2013-2014, UN.G.A. (2014). The right to privacy in the digital age. *United Nations Digital Library System*, [online] 68(167). Available at: https://digitallibrary.un.org/record/764407?ln=en.

[3] Durnell, E., Okabe-Miyamoto, K., Howell, R.T. and Zizi, M. (2020). Online Privacy Breaches, Offline Consequences: Construction and Validation of the Concerns with the Protection of Informational Privacy Scale. *International Journal of Human–Computer Interaction*, 36(19), pp.1834–1848. doi:10.1080/10447318.2020.1794626.

inherent to the process of using the Internet because users' personal information is endlessly shared, both passively and actively, as users browse and share their personal details online. Be this through automated recommender systems, cookies, etc, personal details and information are stored for the widest range of purposes, including to generate suggested search results which can be sold to corporations to create targeted ads. The same data can also be easily accessed or even hacked when a breach of security occurs, and as such; due to the ubiquity of online data-sharing and storing, most research shows that users have been most concerned about how big corporations and governments have been using their personal information.

As a result, **delegates should focus the debate on trying to find measures to tackle the right to privacy online at an international level and promote it by protecting users' private information both to the government level as well as to big corporations' level**. Delegates should recognise that increasing data privacy leaks and therefore distrust of the internet, along with the growing trend in collusions in data privacy scandals, pose severe threats to the right to privacy, regardless of being online or offline.

Current Situation

The issue of data privacy has been of utmost importance as registered recently, with a special emphasis on multinational corporations, especially those related to social media and collection of data. In 2021, 3.96 billion people actively used social media worldwide, according to the reports published by such platforms, this being equivalent to about 50% of the world's population. Since the beginning of the 21st century, the use of communication technologies has increased exponentially, and with that, so have the scandals regarding data privacy, putting citizens and governments at risk of exposure of their own and personal data.

To this day, concerns are that global mass surveillance can affect the enjoyment of basic human rights, including the right to privacy. It is highly unclear the extent to which users are aware of the amount of personal data they share when using the internet, including websites and social media applications. The collection and storing of data online can interfere with privacy and lead to human rights violations, and **that should be the delegates' focus for the debate: measures to decrease the window of possibilities in which governments can allow such human rights violations to take place, including censorship of information and targeted vigilance of government oppositions**. When a user notices a data privacy leak or invasion of

his privacy, measures are needed to report such violations effectively. For instance, the European Court of Justice has declared mandatory consent to the use of cookies[4]. While cookies can be seen as important for many online services to work adequately, they can also be used to identify and track down a user's habits when navigating online. It is of extreme urgency that delegates create measures similar to this one.

International and Regional Framework

Article 17 of the *International Covenant on Civil and Political Rights* further affirms Article 12 of the *Universal Declaration of Human Rights*, already defined above. It should be noted by all delegates that the UDHR is not a legally binding document and therefore doesn't create legal obligations for countries; however, the ICCPR is legally binding on the countries who ratified it. Most recent international and regional frameworks addressing this human right are based on three main pillars: safeguarding human rights from third party abuses, corporate responsibility, and adequate access to remedies for victims of human rights violations in online settings. Delegates should focus their clauses on these three pillars, as they will build the general focus of debate, working towards more vital international legislation. The Office of the High Commissioner for Human Rights (OHCHR) has released, in 2014, a report on the right to privacy in the digital age which highlights key issues that should be addressed by delegates in this committee session.

The United Nations General Assembly first adopted resolution 68/167 on *The Right to Privacy in the Digital Age* in 2013, focused on the protection and enjoyment of human rights on the internet and privacy in digital communication, urging member states to take emergent measures to protect the right to privacy and *to review their procedures, practices, and legislation regarding the surveillance of communication, their interception, and the collection of personal data*. *The Right to Privacy in the Digital Age*, a further resolution (73/179) on the topic, adopted in 2019, asks Member States to work hand-in-hand with CSOs (Chief Security Officers) to promote ICT education within and outside corporations. Corporations are urged to provide transparent information about the methods with which they use their users' data. Further work

[4] Baker McKenzie (2019). *EU: Court of Justice of the European Union rules on Cookie Consent*. [online] Global Compliance News. Available at: https://www.globalcompliancenews.com/2019/10/25/eu-court-justice-european-union-rules-cookie-consent-20191011/.

of all stakeholders, including NGOs, the business sector, and Member States, is necessary to enjoy and maintain the right to privacy in the digital age.

In conclusion, the right to privacy in the digital age is an increasingly important topic. One of main concerns is that mass surveillance is used increasingly more by private entities, which can be deemed unlawful. Delegates should be especially worried that communication technologies can be exploited by certain policies or practices because they are vulnerable to unlawful exploitation by previously set big corporations. **Effective legal frameworks are essential to guarantee the protection of the right to privacy, and delegates should make use of existing frameworks by updating their legislative, administrative, or judicial matters to match the most recent developments of ICTs and surveillance measures.**

For the focus of the debate, delegates should essentially consider how the illegal use of mass surveillance or other communication technologies can be prevented, and how the private use of mass surveillance can be regulated. As such, delegates are strongly encouraged to devise frameworks to ensure the right to privacy in the digital age.

Bloc Positions

United States of America

In the USA, there is no single, comprehensive federal law that regulates how much most companies are allowed to collect, store, or share customer private data. In most states in the country, corporations can use, share, or sell any data collected on the users without notifying them that they are doing so. There are also no national law standards of when a company must notify the user if their data is being breached or exposed to unauthorised parties. If such company shares or sells data, potentially sensitive data included, third like data browsers can re-sell it without the user being notified. The USA has a mix of laws, including for instance HIPPA, GLBA, FERPA and COPPA[5], which target only specific types of data in special (often outdated) circumstances. At present, only the states of California, Virginia, and Colorado have comprehensive consumer privacy laws put in place.

[5] Klosowski, T. (2021). *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*. [online] Wirecutter: Reviews for the Real World. Available at: https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

Germany

As most other countries belonging to the European Union, Germany puts in place a comprehensive data privacy law named *General Data Protection Regulation (GDPR)*[6], requiring companies to ask for permission to collect, share, and store users' data, and giving them the right to access, delete, or control its use. The GDPR is applicable to companies of all sectors and sizes, and stipulates a comprehensive and detailed set of rules that aim to protect personal data and movement of such. Fines in case of non-compliance with the GDPR can reach up to 4% of total annual revenues of the business, and companies should therefore consider their compliance with assistance of legal counsel.

India

India has recently put in place a data privacy and protection bill, the *Personal Data Protection Bill*, which includes requirements for notification and consent prior to the collection and sharing of individual data, restrictions on the purposes for which personal data can be used by corporations to ensure that only the most necessary data is collected in order to provide a service with good quality[7]. However, in 2017 a judge in the Supreme Courted ruled that it was unconstitutional for corporations to use Aadhaar data, which forms the major part of India's biometric identification programme. The *Digital Personal Data Protection Bill* has been the latest attempt of the Bharatiya Janata Party (BJP)-led central government to put into practice India's first data privacy law, after previous version that was introduced in parliament in December 2019. However, it was dropped in August 2022, because opposition lawmakers, technology companies and advocacy recognise it fails to address their key concerns, including not providing adequate protection for children.

Democratic People's Republic of Korea

The DPRK has several data protection authorities, including the Personal Information Protection Commission (PIPC)[8], that, as stated in Article 1 of the Personal Information

---

[6] European Union (2016). *EUR-Lex - 32016R0679 - EN - EUR-Lex*. [online] Europa.eu. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[7] Human Rights Watch (2022). *India: Data Protection Bill Fosters State Surveillance*. [online] Human Rights Watch. Available at: https://www.hrw.org/news/2022/12/23/india-data-protection-bill-fosters-state-surveillance.

[8] Personal Protection Information Commission (2021). *Personal Information Protection Commission*. [online] www.pipc.go.kr. Available at: http://www.pipc.go.kr/cmt/main/english.do# [Accessed 1 Feb. 2023].

Protection Act, aim to *protect the freedom and rights of individuals, and further, to realize the dignity and value of the individuals, by prescribing and processing personal information*, by fixing any policies related to data access and data privacy and coordinates divergent opinions in other government agencies. Not only was the use of social media banned, but the general use of the internet was severely restricted. The general citizen does not have access to the internet, but rather only to the country's intranet, Kwangmyong.