
CHMUN' 19

UNGA - DISEC

Executive Board's Address

Chairperson

Greetings delegates,
I welcome you to **UNGA-DISEC** at **CHMUN'19**. As your executive board, during your time in the committee, we'll be trying to open portals for you towards a fast-paced world of international politics and diplomacy. In the committee you're not just going to be a school student. Rather, you'd be an international delegate with the responsibility of voicing the opinions of millions of civilians from your sovereign nation.

During the course of the debate, I expect that the delegates would adhere strictly to their nation's foreign interests and would only quote articles and statistics from Reuters, Al Jazeera, TeleSur, UN or National documents while making statements. Prior to your attendance in the committee, we urge you all to try understanding the complex multidimensional nature of international politics over seemingly fundamental black and white issues. Thoroughly read this background guide but keep it in your mind that this is only to kick start to your research and is not to be treated as the end-all be-all of your delegate research.

Regards,
Harshit Goyal,
Chair,
DISEC

Vice Chairpersons

Greetings delegates,
Welcome to the Disarmament and International Security Committee!

My name is Sajal Maheshwari and I will be chairing this year's United Nations General Assembly first committee- DISEC, alongside my Chair Harshit goyal and co-vice chair Prachi Tiwari. I know many of you are new to the concept of Model United Nations, but that should not stop you from researching and debating you hearts out! To make the committee sessions exceptionally invigorating, I expect the delegates to come up with innovative solutions and incisive arguments. The board is working hard to make the committee a successful and fruitful one, and we expect you to do the same. The following guide is aimed at initiating your inquiry and is by no means exhaustive. This committee guide will just provide you background information on the agenda at hand. I hope that the research you conduct as delegates is thorough; only then may the issue at hand be discussed with the propriety that it demands. Hidden inside each of you is a star-delegate and I hope that this conference is able to unveil the diplomat inside you. Feel free to contact me or any member of the E.B. at anytime regarding any doubts related to the agenda or the proceedings of the committee, and we will be happy to oblige. I am looking forward to seeing all of you in the committee as thoroughly prepared and informative delegates.

Regards,
Sajal Maheshwari,
Vice Chair,
DISEC

Greeting delegates,

My name is Prachi Tiwari. It is my pleasure to welcome you all to the Disarmament and International Security Committee! It is an honour to be serving you as Vice Chair for this committee. Prepare yourself for the three days of heated yet fruitful debates.

This year we will be discussing on 'The Right to Privacy and Security in Digital Age.'

I, along with chair person Harshit Goyal and co-vice chair Sajal Maheshwari, will do everything in our abilities to make this conference an interesting one. I look forward to have an amazing experience with you all at CHMUN 2019. I expect every one of you to be well prepared and give your very best at this conference. Feel free to contact me in the meantime if you have any queries and concerns, I'd be happy to help you out.

Regards,
Prachi Tiwari,
Vice chair,
DISEC

Disarmament and International Security Committee

The Disarmament and International Security Committee was established in 1993. It is the First and one of the main committees of the General Assembly. The role of DISEC is outlined in Chapter IV, Article 11 of the United Nations Charter which states, "The General Assembly may consider the general principles of cooperation in the maintenance of international peace and security, including the principles governing disarmament and the regulation of armaments and may make recommendations with regard to such principles to the Members or to the Security Council or to both". As per this article, the mandate of DISEC is highlighted as, "to promote the establishment and maintenance of international peace and security with the least diversion for armaments of the world's human and economic resources".

The Right to Privacy and Security in Digital Age

A. Introduction to the Agenda

As the technology advances at leaps and develops, it becomes even more important to secure private information and prevent it from being convenient to abuse. Today, the position of technology has brought the problem to a much more serious point. Thus, the

discussions upon this subject has grown in significance and become more popular around the world.

Technological devices, being a major part of our lives, store way more personal information than expected. From one's location to contacts, most apps collect very detailed personal information from devices, claiming to "provide a better experience" to users. People accept the Terms of Use without reading, and it turns out that those terms include sending personal information to third party companies. A possible stealing of personal data could lead to worse; it is not difficult for hackers to reach to a bank account or a house address if they are not safely stored.

Throughout few previous decades, foreseeing the possible danger of developing technology and the overwhelming amount of personal data being stored, several acts and regulations were signed and brought into action. Since an average person couldn't tell a safe website from a dangerous one apart, and more people got hacked every day, it was obvious that a regulation regarding the storage of personal data and immediate spread of awareness was necessary. Consequently, after the insufficient Data Protection Act, General Data Protection Regulation was adopted with great hopes by the European Union. Although it was not completely ineffective, the GDPR wasn't adequate to resolve the problem at all.

The issue now remains unsolved, with more people getting affected and harmed by various types of cybercrime day by day.

B. Important Terms and definitions.

- **Personal Data**: Any information relating to an identified or identifiable natural person ('data subject'); a identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Examples include date of birth, sexual orientation, whereabouts, religion, but also the IP personal data address of your computer or metadata pertaining to these kinds of information.
- **Data Protection**: the process of safeguarding important information from corruption, compromise or loss.
- **Privacy Breach**: the loss of, unauthorized access to, or disclosure of, personal information. Most common privacy breaches happen when personal information is stolen, lost or mistakenly shared.
- **Cybercrime**
- **Cyber attack**

C. General Overview:

1. Current Situation and Legal Aspects

Users' personal information is shared to dozens of websites from an online store to a social platform. They don't consider sharing their personal data on various platforms as dangerous, believing that it is fully private and won't be shared with third parties. Looking

at the rapidly increasing number of cybercrimes, maybe the '**cookies**' that are allowed in every website, or the personal data users give to random websites without a second thought are not as innocent as they may seem. In order to have the best understanding of the right to privacy, one must analyze the regulations correctly.

In today's world, their information being collected or even being shared to a third party company isn't really a big deal for most people. However, when examined, it can be seen that the **General Data Protection Regulation** which follows as "**Article 2**- If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.'' clearly states that the use of personal information is only possible with the full consent of the user, and by requesting it clearly and in a way that it is distinguishable from other matters.

Although there were several international laws concerning social media and digital privacy such as the "General Data Protection Regulation (GDPR)" passed by the European Union Parliament in 2016 which will be further explained and detailed under a much more comprehensive title as well as the Data Protection Act, the inadequacy of the execution and disobedience/ violation determination process of those laws was undeniable.

Users discern the disturbing and obvious violations of cyber law on a daily basis yet the consequences seem innocuous.

Furthermore, they neither contact legal authorities nor are aware of their rights nor aware that those acts are each a criminal offense in advance. As a matter of fact, depending on the type of privacy violation users experience, they officially have the right to take legal action against the person/ firm who violated their privacy.

In addition, social security numbers, addresses, phone numbers, and other personal information must always be kept confidential. Cloud computing has been one of the key innovations that is changing the landscape of technology and driving digital transformation across all industries. Despite its cost in the short run, cloud computing has been providing commanding security, flexibility, mobility, collaboration, sustainability and broad control over two decades so far when it comes to personal data protection.

2. Main Examples of Personal Data Protection Violations

Yahoo Privacy Breach

In the wake of 2013, Yahoo declared that around 500 million of their accounts had been breached. In November later that year, Word leaked that Yahoo had allowed U.S. intelligence agencies to read through its user emails in search of red flag phrases or keywords. At the end of 2013, Yahoo had stood corrected by stating the number of the "hacked" accounts as a billion. Experts still argue if the breach was really a matter of hacking which is a significantly low possibility. It is also very controversial if the number was around a billion in the manner Yahoo clarified. In such case which is them being around 3 billion as the experts estimate, it could be the biggest privacy breach in history so far.

Google EU Data Privacy Rules Violation

France's data protection watchdog fined Google 50 million euros for breaching European Union online privacy rules, the biggest penalty levied against a U.S. tech giant. The EU's General Data Protection Regulation (GDPR), the widest data privacy law in more than two decades, allows users to have a better control over their private data and gives regulators the power to impose fines.

The personal data share of Facebook

One of the most scandalous events violating the protection of personal data was when Facebook shared the data of its users without permission. Mark Zuckerberg, founder of Facebook, admitted having shared the data of eighty seven million Facebook users to Cambridge Analytica for the purpose of political profiling. Additionally, it turned out that Facebook gave 'deep access' to Apple, Samsung and other firms. Previously, Zuckerberg had stated that all Facebook users had 'complete control' over whom they share their personal data with. After great public aggression, Facebook lost many users. Consumer loss through cyber crime worldwide in 2017, by victim country is given above.

United States Government's Backdoor Demand

United States' federal government, or FBI to put it in another way, attempted to make Apple open a backdoor so it could peruse information in a suspect's smartphone. Apple CEO Tim Cook became a privacy advocate and defended the importance of the safety of personal data. The lawsuit brought up the question: If a government can bypass manufacturers in one instance, then what stops it from doing it over and over again?

3. Timeline of Important Events

1890- Fingerprints are first used to identify people; "**The right to be let alone**" introduced.

1928- US Supreme Court rules that seizures of electronic communications systems is constitutional.

1976- Public-key encryption created to prevent the stealing of personal and business information.

1980- DNA fingerprinting starts to become common.

1990- Identity theft starts to become common.

1994- **HTTPS** introduced to help secure web traffic.

1995- **Spyware** starts to become common and is transmitted through the Internet.

2000- Web bugs are introduced.

2013- Edward Snowden reveals NSA surveillance operations.

2014- EU Court approves the **right to be forgotten**.

D. Previous Attempts to Resolve the Issue

- DPA (Data Protection Act)
- GDPR(General Data Protection Regulation)
- Computer Misuse Act

E. Relevant UN Documents

As the Board, we highly encourage you delegates all to take inspiration from the past actions taken by some of the international organizations and United Nations. Thus, our aim is to come up with various original solution ideas regarding our agenda item.

- Article 12 of UN Universal Human Rights Declaration, 1948 (http://www.un.org/en/universal-declaration-human-rights/)
- Resolution 68/167 (https://undocs.org/A/RES/68/167)
- Resolutions 73/266 and 73/27 (https://undocs.org/A/C.1/73/L.27/Rev.1) (https://undocs.org/A/C.1/73/L.37)

G. Questions a Resolution Should Answer

1) What kind of actions should the General Assembly take in order to improve the current situation regarding the right to privacy and security in digital era?

2) What should be done in order to protect the international community and prevent the usage of personal information without their consent?

3) How will the process to implement possible solutions occur?

4) What kind of measures can be taken regarding the rise of awareness on data protection?

5) How can both the governments and individuals themselves assure the safety of their private data?

6) In what ways can the disobedience of international laws, illegal data transaction and/or theft be detected?

7) What kinds of enforcements or sanctions could be implemented on cyber criminal offenses?

8) What is the certain role of the media organs for this issue?

9) Should data privacy/ protection laws be rearranged, If so how?