



Model United Nations

*2020*

*Structuring sustainability*



Secretary-General's Address

Dear Delegates,

Thank you for taking the first step on your journey into the most underrated aspect of MUN: **research**.

Given below are the background guides, starting points for learning about your agendas, and briefs on the basic information that is pertinent to the UN regarding them. These guides serve mainly as a *launch pad* to explore your topic in detail, and not an end to your research.

ADMUN has only one agenda per committee, while most MUNs have 2 to 3. The reason for this is simple: we want a highly qualitative, serious, in-depth discussion on the agenda, and that means we expect a relevant amount of research. For the coming conference, I'd like to give a short list of the most important areas of knowledge regarding an MUN agenda, and I'd highly recommend that you prepare a research binder containing this information.

Firstly, understand the background of your issue, and be able to cut it up into small, *specific* problems to solve. The Kashmir issue, for example, pertains to terrorism, legality, and peace between the relevant countries.

Secondly, understand the role your country plays in this issue. Regardless of whether you are in the WTO, look at your major trading partners, allies, rivals, and understand what your country wants from this issue.

Thirdly, understand what the UN wants to accomplish, and what has already been tried. Past resolutions, private sector initiatives, and even military methods are all often relevant. Check why they worked - or didn't.

Finally, find out what exactly the innovative solutions for this issue are. This can be ideas you have come up with yourself, siphoned from opinions of academics and politicians, or it can be detailed policy proposals from think tanks like Demos.

Remember to genuinely try to take an interest in what's going on, as these issues could affect you directly the next time you try to get a visa for a trip, or even explain why the job market for specific fields is booming (or stagnating). Remember that you can always mail your chairs at their given email IDs if you have any doubts on research, and that you will do the vast majority of your work in committee with other delegates in person.

Our chairs have worked very hard on these guides, and they are of the utmost quality in terms of content, and they are invested in these topics both academically and personally. Please look over them with the care they deserve. I hope to see you all well prepared and sharp on the days of the conference. Have fun researching! :D

Regards,  
Shaurya Chandravanshi  
Deputy Secretary General



Program Director's Welcome

Dear Delegates and Faculty Advisors,

On behalf of the Secretariat, I would like to welcome all of you ADMUN 2.0. With ADMUN '19 being a huge success, we hope to see the same amount of enthusiasm among all those who are involved in this year's ADMUN.

This year's background has been tailored in a way that delegates gain enough knowledge regarding their agendas but at the same time are asked questions which require them think critically. To start with, the chairs have written a letter to the delegates, outlining what is expected from the committee, followed by a brief summary of what the committee does. After this, a few key terms are discussed, and the agenda is introduced. The background of the issue is described along with its current situation and to conclude the major parties involved and problems the resolution must address have been given. A few starter links have also been provided by your chairs to make it easier to research your topic further. Do keep in mind that the issue goes far beyond what has been discussed in the background guides and delegates must research more than what has been given.

The theme for ADMUN 2.0 is Structuring Sustainability. The need for sustainability is growing each year and as we move closer to 2030, it is important that we start acting on the Sustainable Development Goals.

To conclude, a big thank you to all those who were involved in making and researching for the background guides. I am sure that these background guides will help you see what really needs to be discussed regarding your agendas. All the best!

Veena Madhu

Program Director

ADMUN 2.0



## United Nations Human Rights Council

### Agenda:

Right to Privacy in the Age of Digitalization

## Letter to Delegates

Greetings delegates,

It's our honor and pleasure to formally welcome you all to the United Nations Human Rights Council at Al Diyafah Model United Nations. We hope each and every one of you leave the committee room with more knowledge, more confident in your self and most importantly an experience you will remember.

MUN is a platform of expression, where each and every word you say matters, where your voice matters, Where you can make a difference in the world, it might be hypothetically but this is what will build the leaders of the future.

MUN is a forum of expression and a platform for each and every one of you to develop and sharpen debate skills, gain new knowledge, effectively cooperate, solve issues and most importantly create new memories and friends along the way.

The topic chosen for this committee is Right to Privacy in the Age of Digitalization. We chose the topic keeping in mind its relevance in our lives today as well as its future development. We hope to see extensive and fruitful debates leading to constructive resolutions.

We wish you all the very best and can not wait to meet you.

Warm Regards

Fatma Ghayyour and Waleed

Chair and Co-Chair of UNHRC

## About the Committee

The United Nations Human Rights Council was established on 15 March 2006 after resolution A/RES/60/251 was passed. The committee was formed to be the successor of the United Nations Commission on Human Rights. This committee consists of 47 nations based on regions for a term of three years after which new members are elected. UNHRC directly reports to the General Assembly. The Office of the High Commissioner of Human Rights is responsible for the proper functioning of the committee in terms of administration, logistics and ensuring its functions in the most effective manner. The committee, with a comprehensive Human Rights mandate addresses issues of Human rights violations, reviewing nations records on Human Rights, responds to human rights emergencies and acts as a medium for international dialogue. In 2007 the committee established its very first Institutional Building Package which aimed at combating the flaws of its predecessor and ensuring the committee is as efficient as possible. Through establishing three bodies of the committee. The first one was the establishment of a system whereby the committee's working is reviewed every 5 years by the general assembly to ensure the best outcomes from the committee. Secondly, the advisory committee which advises the committee over a multitude of issues while also providing expertise and advice to the committee. Thirdly, the complaint procedure the process through which organizations and individuals can bring to the attention the different Human Rights Violations taking place across the world.

The UNHRC is also the main principal body of the United Nations which looks into Human Rights Research, Education and Awareness and advocating for Human Rights across the world and the UN.



## Key Terms

- **Digitalization**

The conversion of text, pictures or sound into a digital version which is processable by a computer.

- **Big Data**

A large and diverse set of data which grows at increasing rates. It includes the volume, speed of collection and scope of the data.

- **Right to privacy**

Right of an individual to not have interference from any external body in terms of personal matters.

- **Data Breaches**

It is security violation where protected data is accessed or disclosed by unauthorized personnel.

---

## Introduction

In today's Modern Society a lot of us have a tendency to share our personal information whether it be to government authorities for services such as healthcare or on digital platforms such as social media. This information that we share on digital platforms can be easily misused by governments or other third parties for illegitimate reasons. This is done through detection software where these softwares track one's activity online, the data collected from these tracking softwares can further be used for illegitimate actions ranging from hacking and robberies to governments detaining individuals or a group of individuals based on their online activity.

Data breaches are one of the most common type of violation of the Right to Privacy. This type of violation by a firm can not only have legal and reputational implications but also impact the productivity due to financial losses and major operational disruptions. This lack of productivity is a loss of to the economy especially if such an event takes place on a large scale, which is very possible in today's time.

The Right to Privacy is a fundamental human right according to Article 12 of the Universal Declaration of Human Right, and probably one that gets exploited the most on a daily basis. This right gets exploited not only by businesses or individuals but there have been incidents where the government has violated the right to privacy for reasons such as national security.

## **Background**

United Nations has a specialized agency, International Telecommunication Union (ITU) whose main purpose is to look into issues regarding Information Technology. They have recently taken the issue of cyber security into due consideration with an emphasis on the misuse of Information Technology and its implication and discussed multiple resolutions such as 55/63, 56/121, 57/239, 58/199, 64/211. The United Nations General Assembly has taken this matter with seriousness. In the past the P5 nations have collaborated with other nations such as India, Germany, Tajikistan and Uzbekistan.

The United Nations Cyberspace and International Peace and Security, an autonomous body of the UN, has looked into this matter. It has released multiple reports on Cyber Security and nations can promote it in today's time. The United Nations General Assembly has discussed the topic on multiple occasions and established the Open-ended Working group (OEWG) and the Group of Governmental Experts (GGE) under General Assembly Resolutions 73/27 and 73/37 respectively. The OEWG has published multiple reports with the main focus on Cyber Security and its implications on the international level. GGE has worked closely with the OEWG conducting multiple meetings with nations across the board to resolve the issue..

## **Current Situation**

Currently many governments have taken advantage of the security implications and violated the rights to privacy in the nation. There are many examples where governments have violated the right to privacy of individuals, one such incident taking place in Mexico. Federal Authorities in Mexico have purchased more than 80 million dollars worth of tools for spying from an Israeli software manufacturer, Pegasus. These authorities claim that these tools are used to monitor and combat crime and terrorism in the nations, but there have been multiple cases reported where they have been used as spying devices and tracking every aspect of government

officials, lawyers and journalists who stand against corruption, human rights violations and abuse. There have been cyber-attacks launched on individuals one such being when one of the most influential journalists in Mexico, who stands up for anti-corruption, Carmen Aristegui and his wife were targeted using these spying tools.

One of the largest national level Cyber Attacks that took place in Bulgaria. In this case, a group of hackers hacked into the systems of the Bulgarian Tax Revenue Office and stole all the data. Data of almost 5 million individuals was hacked into and this personal information was made private on multiple platforms. Taking into consideration that Bulgaria has a population of 7 million people, we can say that every household in the country was impacted by this attack. It is speculated that these small group of hackers who conducted this cyber attack were not even trained in the field, but gained access to advanced hacking technology through the dark web.

In 2018, one of the biggest data breaches took place in India. India has the world's largest government database of its citizens in the Aadhar registry. The Aadhar contains information of up to 1 billion individuals. This Registry was hacked by a group of individuals and used for illegitimate purposes.

Another incident which took place was the British Airways Data Breach that took place in 2018. In this case the personal information of 500,000 British Airways customers including credit card information and personal details was taken through a fraudulent website. Before this event took place British Airways had not taken any action towards making their systems more secure despite being warned in the past. The Information Commissioner's Office (ICO) fined the airline 183 Million Euros.

Another major breach which came shortly after the British Airways case was with Marriott International, an international chain of hotels. This time the personal information including name, phone numbers, emails and passport numbers of more than 500 million individuals was lost by Starwood, a subsidiary of Marriott International. The ICO fined Marriott International 99 million Euros under the claim that the company did not take proper measures, especially in terms of security, when they bought Starwood. The company was further fined another 265,000 dollars by the Turkish Data Protection Authority for the same.

One of the best data scandals that have taken place in the past few years has been committed by a data firm, Cambridge Analytica. This firm has close ties with the Trump Administration in the United States of America and with the Brexit Campaign in the United Kingdom. In the United States of America, Cambridge Analytica had taken data of 50 million Facebook users, and taking

into consideration that the firm has ties with the Trump administration, it had been speculated that it affected the results of the 2016 US elections. According to an ex-official of Cambridge Analytica, it was revealed that the data firm had intervened yet again in a political matter. This time it was the Brexit referendum held in 2016. In both these cases the collected data was used to spread political propaganda for the benefit of the parties involved.

There are policies in place but in most cases they are not up to date with the advancements of hacking systems available on the dark web today, resulting in cyber-attacks on government databases. Another major stakeholder to take into consideration is the tech companies and with emphasis on social media companies as these are the major sources for such crimes to take place. Tech companies have the capability to either aid this type of human rights violation or side in the protection of the right to privacy, they are one of the most important stakeholders to take into consideration. Despite loopholes nations have put an effort to strengthen their policies and laws. Some nations have even established a separate organ which looks into matters related to digitalization, ensuring it is carried out in the most effective and safe manner. These agencies have proven to be very effective as well.

## **Major Parties Involved**

### **Tech and software development companies**

They play the most important role as they are the ones majorly involved in digitization specifically with the development of new and more advanced technologies.

### **The United Nations and the international community**

The UN and the international community is another major stakeholder as we have seen from the above mentioned examples there are cases where nations use data in illegitimate ways for personal benefits of the parties involved.

### **Nations**

Now nations need to cooperate and come to a solution that is implementable and at the end of the day resolving of the issue at hand will only benefit nations and its citizens. The way

digitalization is implemented in the nation can impact the productivity of the nation and in turn can also aid in growing the economy which will eventually help the nation.

## **Problems a Resolution must address**

- Prevention of cyber-attacks on government databases
- To what extent is the government intervention into personal information acceptable in cases of national security threats? What will be the defining factor for the same
- Creation of international law to protect the right to privacy in terms of digitalization
- Regulation of Businesses to avoid data breaches from taking place

## Bibliography

Goldstein, Keith, et al. *The Right to Privacy in the Digital Age. The Right to Privacy in the Digital Age*

<https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/PrivatePartiesInternational.pdf>

"<https://www2.ohchr.org/>" [https://www2.ohchr.org/english/press/hrc/kit/hrcs\\_fs2.pdf](https://www2.ohchr.org/english/press/hrc/kit/hrcs_fs2.pdf).

Por Azam Ahmed y Nicole Perlroth. "Somos Los Nuevos Enemigos Del Estado': El Espionaje a Activistas y Periodistas En México." *The New York Times*, The New York Times, 19 June 2017, <https://www.nytimes.com/es/2017/06/19/mexico-pegasus-nso-group-espionaje/>.

Albright, Jonathan. "The Graph API: Key Points in the Facebook and Cambridge Analytica Debacle." *Medium*, Tow Center, 21 Mar. 2018, <https://medium.com/tow-center/the-graph-api-key-points-in-the-facebook-and-cambridge-analytica-debacle-b69fe692d747>.

"Fundamental Rights Report 2017 - FRA Opinions." *European Union Agency for Fundamental Rights*, 1 Aug. 2019, <https://fra.europa.eu/en/publications-and-resources/publications/annual-reports/fundamental-rights-2017#data-protection>.

Ahmed, Azam, and Nicole Perlroth. "Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families." *The New York Times*, The New York Times, 19 June 2017, <https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html>.

Scott, Mark. "Cambridge Analytica Did Work for Brexit Groups, Says Ex-Staffer." *POLITICO*, POLITICO, 31 July 2019, <https://www.politico.eu/article/cambridge-analytica-leave-eu-ukip-brexit-facebook/>.

"Are Big Data and Analytics Actually Able to Increase Productivity?" *University of Liechtenstein*, <https://www.uni.li/en/topics/information-systems/news/are-big-data-and-analytics-actually-able-to-increase-productivity>.

"Right to Privacy in the Digital Age." *OHCHR*, <https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx>.

"British Airways Faces Record £183m Fine for Data Breach." *BBC News*, BBC, 8 July 2019, <https://www.bbc.com/news/business-48905907>.

Swinhoe, Dan. "The Biggest Data Breach Fines, Penalties and Settlements so Far." *CSO Online*, CSO, 31 Oct. 2019,

<https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html>.

Kottasová, Ivana. "An Entire Nation Just Got Hacked." *CNN*, Cable News Network, 21 July 2019, <https://edition.cnn.com/2019/07/21/europe/bulgaria-hack-tax-intl/index.html>.

CSTadmin, Author: "The Complete List of Cyber Security Breaches Around the World." *CloudSecureTech*, 30 Aug. 2019, <https://www.cloudsecuretech.com/the-complete-list-of-cyber-security-breaches-around-the-world/>.

"Welcome to the Human Rights Council." *OHCHR*, <https://www.ohchr.org/EN/HRBodies/HRC/Pages/AboutCouncil.aspx>.

"Right Of Privacy Legal Definition." *Merriam-Webster*, Merriam-Webster, [https://www.merriam-webster.com/legal/right of privacy](https://www.merriam-webster.com/legal/right%20of%20privacy).

Brooks, Ryan, et al. "What to Know about a Data Breach: Definition, Types, Risk Factors and Prevention Measures." *Netwrix Blog What to Know about a Data Breach Definition Types Risk Factors and Prevention Measures Comments*, 29 Nov. 2018, <https://blog.netwrix.com/2018/11/29/what-to-know-about-a-data-breach-definition-types-risk-factors-and-prevention-measures/>.

A/RES/68/167 - E - A/RES/68/167, <https://undocs.org/A/RES/68/167>.

"Arms Control Today." *The UN Takes a Big Step Forward on Cybersecurity | Arms Control Association*, <https://www.armscontrol.org/act/2013-09/un-takes-big-step-forward-cybersecurity>

UN Resolutions, <https://www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx>.

"New U.N. Debate on Cybersecurity in the Context of International Security." *Lawfare*, 31 Oct. 2019, <https://www.lawfareblog.com/new-un-debate-cybersecurity-context-international-security>.