General Assembly
The United Nations Big Data Committee

Study Guide

Singularity Model of United Nations
SMUN2030

SINGULARITY FOUNDATION

SMUN2030

Table of Contents:

Dear Delegates,

We would like to welcome you to S'MUN 2030, as well as the Big Data committee. This year's conference will explore the effects of the implementation of Artificial Intelligence into everyday life in the year 2030, especially concerning data protection. In 2030, as anyone would probably expect, technology has evolved and entered every sector of one's life; smart devices are everywhere and AI programs are as prevalent as they have never been, with new problems however arising with it. In this MUN conference, you are given the opportunity, using your imagination, to figure out solutions to the possible dangers to personal data that you think it would emerge that year, especially due to AI. To tackle though effectively the issue, it is essential that the whole world follows the same path towards protecting data. To achieve that, the only solution are the United Nations. As you probably are aware, the UN is an organization where countries are striving to solve the worlds' biggest issues through international cooperation. As delegates of the 2030's UN, you will need to exchange opinions and solutions, debate upon them and compromise, in order to find the most suitable resolution for this arising problem. To achieve that, this study guide will help you initiate your research on the topic. Nevertheless, you should also research the topic on your own focusing on your countries' specific policy, so as to be fully prepared for the heated debates we expect. If you have any questions do not hesitate to contact us via email. We are looking forward to meeting you all and providing you with an unforgettable MUN Experience.

We wish you the best of luck in your research,

Evangelos and Nicole

The Chairs of the Big Data Committee

Introduction to the Chair

My name is Nicole Hanani and I will honorably hold the position of the chair director of the Big Data Committee. I am a 16 year old student from Vienna, Austria, and go to Danube International School. During the conferences, I will be assuring that our debates are well ordered, productive, and exciting at all times. I am an open-minded person and am always welcoming disagreement and at the same time consensus. I am delighted to be a chair at SMUN2030 and addressing the global issues that have to be resolved by then. I highly encourage all of the delegates to express their opinion and point of view and for everyone to contribute. I hope we all will have an amazing time and create great memories together. Together with my deputy chair, we will be making sure that everybody participates in the discussions and we will always be here to help in any way. Do not hesitate to contact us about any questions you might have about either the topic itself or even the rules of procedure. I am looking forward to meeting all of the delegates. We wish you all a successful preparation before the conference.

Excited to meet you all at the conference,

Nicole Hanani
nhanani@danubestudent.com
Chair Director in the Big Data Committee

My name is Evangelos Tasios and I am a 17 year old student from Thessaloniki, Greece. I have taken part in many conferences, either as a delegate or as a chair and am delighted to be serving as a Chair Assistant in S'MUN-2030's Big Data Committee. I am a very hard-working person, especially when it comes to achieving my goals and can make the most out of any situation. MUN for me means unforgettable memories and incredible people. Apart from diplomacy, I love history, playing football and listening to and playing music, while I also aspire to study Mathematics and maybe get involved with Cryptography, AI, or even Big Data. Last but not least, I am looking forward to meeting you all and advise delegates to take that difficult first step; to raise their placard, get the floor and talk, as soon as possible. As I say 'a deep breath and a decision is all it takes to embark in a magnificent journey and discover the magic and the additivity of MUN'.

Evangelos Tasios
evaggelost@outlook.com
Chair Assistant in the Big Data Committee

History:

1890

Two lawyers in the United States of America, Samuel D. Warren and Louis Brandeis, write the Right to Privacy, which is a text that argues for the right to have privacy.

1948

The Right to Privacy is accepted from the Universal Declaration of Human Rights, known as the 12th fundamental right.

1967

The Freedom of Information Act (FOIA) provides every citizen in the United States the right to ask for permission to documents from state agencies, which then other countries follow suit.

1980

Guidelines on data protection are issued by the OECD, which is reflecting the increase of usage of computers for processing of business transactions.

1981

Data Protection Convention (Treaty 108) is adopted by the Council of Europe, which renders the right to privacy as a legal obligation.

1995

The European Data Protection Directive is fully developed, which reflects technological advances and launches new laws that include processing, sensitive personal data and consent, among others.

2002

The Directive on Privacy and Electronic Communications is adopted by the EU

2009

In response to email addresses and mobile numbers, evolution of the EU Electronic Communications Regulations becomes vital in guiding marketing and sales campaigns.

2014

An overrule in the Court of Justice in the EU, regulated a new law which gives people the right to request Google to remove results that involve their name. Also known as “the right to be forgotten”.

2016

The EU parliament approves the General Data Protection Regulation (GDPR), after a 4 year discussion.

2018+2019

Replacing the Data Protection Act, GDPR is enforced. Till now there is a controlling management of personal data by IT governance, transparent processes as well as modern applications.

Further optional Reading: https://www.dataversity.net/brief-history-data-storage /

Countries in the real-life committee:

Australia, Bangladesh, Brazil, Cameroon, Canada, China, Colombia, Denmark, Egypt, Georgia, Germany, Indonesia, Ireland, Italy, Mexico, Morocco, Netherlands, Oman, Pakistan, Philippines, Poland, Republic of Korea, Saudi Arabia, Switzerland, United Arab Emirates, United Kingdom, United Republic of Tanzania, United States

International Organizations in the real-life committee:

African Development Bank, CARICOM, Eurostat, FAO, IMF, OECD, GCC-Stat, ITU, UN Global Pulse, UNECA, UNECE, UNESCAP, UN Statistical Institute for Asia and the Pacific, UNSD, Universal Postal Union, World Bank

Key Terms:

Data Protection: the process of keeping prime information safe from corruption, compromise or loss. As the amount of data increases, data protection becomes more required. Making sure that data is easily and quickly restored after any corruption or loss, is a great portion of the data protection strategy. As well as, making certain that the data is protected from compromise and guaranteeing data privacy are also necessary for data protection. Important principles of data protection are ensuring safety as well as having available data under all circumstances. Data protection is utilized to outline the operational backup of data and business continuity/ disaster recovery. Its strategies evolve around two main parts: data availability and data management.

Data Privacy: (also known as information privacy) is a part of data security, which concerns with the genuine handling of data. Data privacy revolves around: If and how the data is published to third parties, Legal ways of how data is collected and stored, and Regulatory restrictions. Data privacy is extremely vital since data os the main asset a company can have. It is necessary for a business, due to the fact they have to build trust and accountability with their customers and partners, who expect privacy, as most of them request their data to be kept private and not shared nor passed further on to third parties.

Big Data: this term is used for certain database systems. It is a great amount of structured and unstructured data that is too massive to process by using the usual database and software techniques. It is utilized for a number of technologies that assist in organizing data. For data to be categorized as big data, the following must apply: it has a massive amount of data, it changes frequently, it is tough to assemble in a structure that other models can be used easily.

Data Storage: a general term for data that is archived in electromagnetic devices or other forms by a computer or different devices. Data storage refers to the usage of recording media, in order to hold on to data using these devices. There are different types of data that are being stored differently and the most frequent ways of data storage are: file storage, block storage, and object storage, with each way having a different function and purpose. Besides having various forms of hard data storage, nowadays there are new options for remote data storage, for example cloud computing, which can advance the ways that users access data.

GDPR: The General Data Protection Regulation is the strongest privacy and security law in the whole world. Those who violate the GDPR, reach penalties up to the tens of millions of euros.

Database: the collection of data, which is organized. A database is stored and accessed electronically from a computer system. Often formal design and modeling techniques are used where databases are more complex.

Current Situation:

Cambridge Analytica:

It is widely known that Facebook is linked to many other apps, meaning when one downloads an app, they can sign up through Facebook. From that there was an app developed, which is a quiz app, and was originally made for Facebook. 300,000 people downloaded the app and logged in through their facebook account. Aleksandr Kogan (the creator of this app) could access the information about users that downloaded the app as well as their friends. The problem with this was that the information was sent through this quiz app and saved into a private database, which was not deleted. Over the years, the private database eventually collected an excessive amount of information about over 50 million Facebook users. This information was then sent to a voter-profiling company called Cambridge Analytica. The data that has been sent to the third party, goes against any ethical standards. Cambridge Analytica made use of this information by making psychographic profiles about these people, which got their personal data sent. Cambridge Analytica has ties to Trump, and is pro republican and therefore used those profiles to make targeted ads for the 2016 presidential campaign of Trump, which they also did with Brexit. This was a huge issue, as they manipulated voters with an indirect influence through advertisements

which affected one's thoughts. The users of this app thought that their information was kept private, however, it was shared with third parties without their consent. Facebook received great amount of criticism and their shares were decreasing to a low point after the scandal went out. The Cambridge Analytica scandal reshaped the UK´s and US´s laws for data privacy. Currently there are a lot of investigations against Facebook and Cambridge

Analytica, not only by the US, however, also by the UK and Canada. Many countries, like Colombia, blocked access to apps that are in relation to Cambridge Analytica to not influence any upcoming elections.

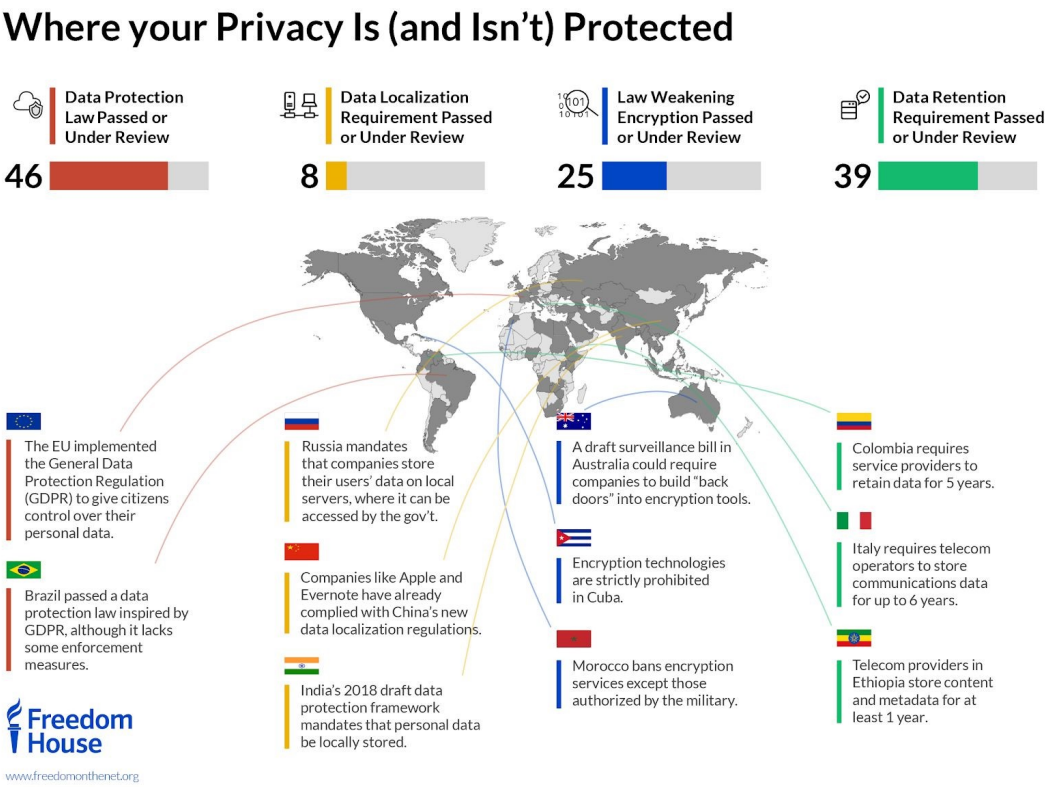
Further reading:

https://www.theguardian.com/uk-news/2019/mar/17/cambridge-analytica-year-on-lesson-in-insti tutional-failure-christopher-wylie

ZAO

There was a Chinese app invented called ZAO, which allowed users to swap faces with celebrities and TV shows. In September 2019, it was revealed that the app was mainly used to create deep fakes, which is the fake pornography of celebrities. The issue was that the user agreement, which no user read on the app, stated that the user agrees to let the app use any videos or photos taken in the app for free at all types. After a public protest the company clarified that the app would not store any user's facial recognition and that as soon as the user deleted the account, the app would delete any data about them.

Block Positions:



US

The legislation in the US varies from state to state, meaning there is no unified law about data privacy in the whole country. States like California and New York are more leaning for consumer data rights, but this causes a dissent due to the fact that the country cannot impose a unified law for data privacy if some states are more to the extreme than others. This also causes a confusing legal environment at risk that companies can get away with a lot of data privacy and security breaches without being noticed because the state does not have the capacity to catch them as much as the federal government has. The first state to take the stand was California with the California Consumer Privacy Act, which came to the effect at the start of 2020 and it allows consumers control what personal information is collected online. New York has passed a privacy

act as well, which is much stricter than the Californian one in the sense that New Yorkers can sue the companies if they think they violated the data privacy laws.

China:

The status of china has been confirmed as the world's worst abuser of internet freedom, for the fourth year in a row. With every passing year, the government enhances its information control, in order to prepare for the 30th anniversary of the Tiananmen Square massacre as well as the widespread anti-government protests. China has imposed more information control on the internet and so, have removed hundreds of thousands of accounts on social media, that is classified as “harmful” as it provokes the government or medical research. They control the data so that the government's initial plan could not be damaged.

EU:

The EU has updated their general data protection laws, which are based on the 1995 bdata protection laws. The updated version consists of two main objectives. One objective is to facilitate and stimulate free movements of personal data in all EU countries. The second aim is to protect the fundamental rights of the users based on the protection laws. The data controllers are people that do the data processing and control what data goes in and out of the system, while the data subjects are the people that the personal data belongs to.

Russia:

Russia has imposed a highly similar data protection laws and regulations like the EU. However, Russia emphasizes strongly on the technical measures of the data protection

Treaties about Data and Privacy Protection

1. Universal Declaration of Human Rights

The Declaration was proclaimed by the U.N. General Assembly in 1948, with the right to privacy found in Article 12: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks”. Even though countries are not forced to abide by the Declaration, many of its principles have been incorporated in international treaties, regional human rights instruments, and national constitutions.

2. International Covenant on Civil and Political Rights (1966)

In Article 17 of the Covenant, the right to privacy is protected, stating that: “1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks”. The Covenant has 173 state parties and 74 signatories.

3. Convention for the Protection of Human Rights and Fundamental Freedoms

A treaty by the Council of Europe (also known as the European Convention on Human Rights) states in Article 8 that: “Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”.

4. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

The convention was the first legal document protecting personal data. It came first in effect in 1985, and was later amended in 2001 with the Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows. Also, in 2018, a new amendment was drafted set to take effect in 2023 (Protocol Amending the Convention for Protection of Individuals with Regard to Automatic Processing of Personal Data).

5. African Union Convention on Cyber Security and Personal Data Protection

Drafted in 2011 and adopted in 2014 by the African Union (A.U.), the convention tackles the issue of Cyber security, a subsector of which is data protection mentioned in chapter II of the Convention. However, it is only ratified by just 5 A.U. members, while it is only signed by 14 more.

6. EU Charter on Fundamental Rights

The European Union protects personal Data in article 8 where it is stated that:

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent Authority

Guiding Questions

What is your country's view on data protection and data privacy?

Are there any laws in place that enforce data protection and privacy in your country? Are there any significant historic points that have happened in your country that affected data protections and data privacy?

How much internet access do citizens of your country have?

Are there any current events happening in your country relating to data protection and data privacy?

Is your country part of any treaties relating to data protection and data privacy?

Has your country faced any problems relating to data protection and data privacy?

Do the citizens of your country find this issue important and what do they want done about it?

Is your country moving towards an international custom in international law on data privacy, and how would that affect other countries?

How would having more coherent policies relating to data protection and privacy affect other countries?

Bibliography (Further reading - optional)

History of Data Storage - https://www.dataversity.net/brief-history-data-storage/

The difference between data privacy and data protection -

https://www.forbes.com/sites/forbestechcouncil/2018/12/19/data-privacy-vs-data-protection-und erstanding-the-distinction-in-defending-your-data/#2854249150c9

Why privacy protection is a losing game - https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-tochange-the-game/

Why data protection is important

https://www.fsb.org.uk/resources-page/why-is-data-protection-so-important.html

Cambridge Analytica Case explained -

https://www.theatlantic.com/technology/archive/2018/03/the-cambridge-analytica-scandal-in-thr ee-paragraphs/556046/

Data privacy after Cambridge Analytica -

http://jtl.columbia.edu/international-data-privacy-in-a-post-cambridge-analytica-world/

Interesting article on a new perspective of data privacy - https://www.livemint.com/mint-lounge/features/what-the-great-hack-tells-us-about-data-privacy-1 565946607143.html

Did the case really change anything - https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-change d-the-world-but-it-didnt-change-facebook

What is GDPR and why it is important - https://gdpr.eu/what-is-gdpr /

What has been done since GDPR -

https://www.techradar.com/news/whats-been-done-for-data-privacy-since-gdpr

https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

https://www.brinknews.com/the-us-is-leaving-data-privacy-to-the-states-and-thats-a-problem/