

SAHINKAYA MODEL UNITED NATIONS 2019

GROUP OF TWENTY

- THE ISSUE OF DIGITAL SECURITY AND PRIVACY

Group of Twenty

Letter from the Secretary-General

Most distinguished participants,

If you are reading this letter, I am more than happy to announce that the Şahinkaya MUN team has achieved every single objective that it had put forward when founding this society in 2012. On behalf of the most honorable Deputy Secretary-General Mr. Eren Mermer, Director-General Ms. Bilge Derin and Deputy Director-General Ms. Derin Aydın, it is an overwhelming honor for me to welcome you to the Şahinkaya Model United Nations 2019. As the Secretary-General of the sixth edition of the Şahinkaya Model United Nations conference, I have been endowed with the honor of this position in order to serve you and create the most esteemed Academic Team, so that you the participants will leave with an unforgettable experience. With my friends and colleagues, we have always looked for greatness and academic sufficiency. Our main purpose in Model United Nations is to guide you in your journey to acquire a diplomatic perspective in your future careers, all while experiencing an entertaining conference.

In this edition of Şahinkaya MUN 2019, G-20 will simulate an important topic being digital privacy and data protection. Şahinkaya Model United Nations 2019 offers you a new diplomatic perspective to current and historical global issues with challenging events and instant crises. Agenda items range from the chronic issues that the world has been fighting for decades. As a consequence of the agenda items being so important and relevant, the Secretariat expects all of the participants to read this document intensively, prepare thoroughly in advance, and understand their given countries' point of view.

In the end, I would like to thank my Academic team, Organization Team, PR and Press Teams for their cooperation and their relentless support in making this conference unforgettable for delegates, committee directors, and observers alike.

With respects and regards,

Gökhan Şeheri

Secretary-General of Şahinkaya Model United Nations 2019

Letter from the Under-Secretaries-General

Honourable participants,

It is an utmost pleasure to welcome you all to the G20 committee. Our names are Cahit Cem Kıryak and Yekta Can Tursun and we will be taking the role as Under-Secretaries-General in G20 committee.

We are sophomores at Istanbul Technical University and we are studying computer engineering in there. We have been participating in MUN conferences since 9th grade and we love doing this job. With our hardworking assistant Ömer Can Öztürk, we will do our best for you to have a great conference.

G20 committee will be about data privacy and freedom of information. Delegates will be discussing this issue and find new ideas also solutions for data privacy issues and freedom of information problems.

We highly suggest and encourage all the delegates to read and understand the study guide before the conference. We also suggest delegates do extra research to get much more prepared for the conference.

We cannot wait to see all of you in the conference.

tursun@itumun.org

cemkiryak@gmail.com

Best Regards,

Under Secretary Generals of Group of Twenty

Cahit Cem Kıryak – Yekta Can Tursun

Table of Contents

I) Introduction to the Committee

a. History of Group of Twenty

b. Purpose

c. Today's Structure of G20

II) Agenda Item: The Issue of Digital Security and Privacy

a. Cyberspace

b. Data

c. Privacy

d. Information types

III) Authorities by Countries

IV) Legal protection of right of privacy

V) Issues

VI) Conclusion

VII) What should the resolution cover?

I. Introduction to the Committee: Group of Twenty

The Group of Twenty, abbreviated as G20, is an international forum that mainly focuses on economic cooperations and consensus decision-making between the participant countries. The members of the group consisting of 19 countries and the European Union. The members of The G20 retain %90 of the global GDP,%80 of global trades and now two-thirds of the world population. Any member state can also invite several guest countries to the forum. The leaders of the Group of Twenty meet annually on a “chair country” which essentially is the country that will host the forum that year. The chair countries are decided via a grouping system, which divides all nineteen members of the forum, with the exception of the European Union, into 5 groups. After negotiations between and in the groups, the chair country has the presidency of the summit starting from 1st of December to 30th of November.

There are also regular meetings in the G20 throughout the whole year between the Finance Ministers and Central Bank Governors of the member states and the meetings are made on topics.

Regarding ways to strengthen the economic cooperations between countries, the global economy, reforming the international financial institutes, an improvement on financial regulations, implementation of the economic reforms to the member states, etc.

G20 is an apt model, and a key factor in economic and global cooperation in the world we are living today. The actions taken against the global financial crisis by the G20 is a resemblance of the effect of the G20 members when they are working and cooperating as a whole. The G20 provided trillions of dollars in fiscal stimulus packages, saving and also creating many job opportunities which otherwise would be destroyed or even be extinct.¹

a. History of the Group of Twenty

The Group of Twenty is the latest installment of post World War 2 institutions aiming international coordination of economic policy, such as The Bretton Woods Twins, The International Monetary Fund and the World Bank. G20 was first talked upon at the Cologne Summit but it was foreshadowed by other topics in June 1999. Later on that year, on 25th of

¹ <http://g20.org.tr/about-g20/>

September, the G20 was formally established at the G7 Finance Ministers' Meeting and an inaugural meeting was also held between 15-16th of December 1999 in Berlin.

For a 5 year stretch, there have been talks on who was the primary influencer and supporter of the establishment of The G20. There have been reports made in 2004 about Hans Eichel, the host of the inaugural meeting aforementioned before, was the main initiative of the forum. However, later the reporter also stated that Paul Martin, Canada's future Prime Minister, also played a crucial role in the formation of the forum. Many Canadian academics and journalistic sources supported the idea. In the end, though, members acknowledge that Germany and The United States had a key role in bringing their ideas and opinions into reality.

b. Purpose

The Group of Twenty was established as a response to many financial and economic crises that have occurred in many emerging economies of the 1990s and also aimed to help certain countries gain recognition and be adequately represented in global economic talks and governance. The group's primary attention, focus, and power is on the governance of the global economy. But it's far from saying that there have not been various topics that have been debated on before. As an example, the 2006 Summit's main theme was "Building and Sustaining Prosperity". This was discussed to achieve "sustained growth", reforms to the World Bank and the International Monetary Fund, as well as the effects of demographic changes created by an aging population throughout the globe. The Group of Twenty's main objectives consists of Policy coordination between its members in order to achieve global economic stability, sustainable growth; promoting financial regulations that reduce risks and prevent future financial crises and lastly; creating a new financial architecture.²

c. Today's Structure of the G20

After every G20 summit, a new chair country is selected to host the next summit in their country. The country that is selected and declared as the host, is called the "chair" country. This chair rotation is executed annually among the members of the forum and is selected from different regional groupings of the member states. The chair is a part of a revolving

² <http://www.mea.gov.in/Portal/ForeignRelation/g20-august-2012.pdf>

management group consisting of 3 members as the past, present and future chairs, named as the “Troika”.

The G20 has not bound a permanent secretariat nor a staff member. The secretariat is established by the incumbent chair country of that year to organize the meetings of the forum and provides the coordination of the work done by the forum. The secretariat is valid in the same time period as the chair country.

The preparation part of the G20 summits is executed by two established tracks named as “The Sherpa” and “The Finance” Tracks. These tracks prepare and continue on commitments and issues that have been adopted in previous summits.

The Sherpa Track mainly focuses on non-economical topics, namely as development, food security and anti-corruption and so on. It also addresses internal attributes such as the rules of procedure of the G20 process.

On the other hand, The Finance Track, as it is in its name, focuses mainly on financial and economic situations. Both of these tracks rely heavily on technical work of a series of expert working groups. On top of that, the agendas that will be discussed in the summits are developed through many ministerial meetings. One example of it is the Joint Meeting of Finance and Development Ministers.³

II. Agenda Item: The Issue of Digital Security and its Privacy

Technology, has been a huge part of daily and basic human life for decades now and it is growing and improving itself day by day and it seems like there’s just nothing that can stop it from happening. Technology brought us many life-changing devices such as cellphones, televisions, computers and an invisible web that connects the entire world together named as the internet. With the internet, you can search, find, ask anything you want and it will be there for you before you can even blink your eyes. Internet’s evolution also resulted in what we call “social media” where billions of people can chat, talk, message, send or receive photos or videos and post them online for people to see even to like or share them. However,

³ <https://worldview.stratfor.com/article/structure-g-20>

improvements are not always positive. Every information and data installed to the internet and people's personal cloud is under risk of being exposed via many expert hackers worldwide. Hackers are not limited to social media though, as there have been numerous cyber attacks against governments. In July 2009, The United States and South Korea have been victims of a series of cyber-attacks to their governments, financial websites and news agencies. Up to 240000 computers have been hijacked via DDoS (overload on servers caused by flooding in the internet traffic). Such acts lead to political and economic damages on the government affected by the cyber-attacks as well. The technology and knowledge they use can be unparalleled sometimes and that leads to the exploitation of data and privacy of information. There have been many attempts to improvise the reinforcements of the security systems in websites and applications the public uses in their phones, yet the hackers adapted to the changes and exposed data anyway.

The risk doesn't end there though. not only do these attacks have a mass effect on social, personal and even governmental data, they also affect non-governmental branches such as the private sector. The private sector is the part of a country's economy run by individuals independent from the government, mainly with the intention of making a profit. Private sector is more common in countries with larger free enterprise economies, like the United States, where it makes most of the country's Gross Domain Product, also known as GDP. In countries such as China, where the government has a bigger power on the economy, the private sector is less effective and the public sector, which is under governmental authorities, is more common. Since private sector plays a big role in a country's economic state, growth and development in most of the cases, a cyber attack that would transmit information and data of companies and facilities that contribute to the private sector would damage the economic status of the country significantly.

These, combined with the ever-growing technology, becomes a much more serious situation with every day passing. Thus, our committee has to find enduring ways of preventing such acts and decide how to take such actions against these cyber attacks.

a. Cyberspace

The term cyberspace is used to refer to the virtual computer world and more specifically, is an electronic medium used to form a global network for online communication. The network itself

Consists of many worldwide computer networks that use TCP/IP Protocol (A suite of protocols established to create a network of networks with a host providing access to the internet.). This way, the cyberspace space provides a free area for data transmissions and communication.

Cyberspace is also the virtual ground for users to share their personal information, interact and swap ideas with one another, play games, conduct a business, engagements in many social forums and discussions and so on. The term was first used by William Gibson and in his book “Neuromancer” and nowadays, the term is still being widely used among anything that has a connection with the internet.

According to many IT specialists and internet experts, the word cyberspace became more commonly known as a medium for social media and interactions, rather than its technical implementation.

Although cyberspace has allowed us to stay in touch with the world and other people any time of the day we want to and also gave us many options to interact with it, this also results in huge data exchanges and a big percentage of it freely running in the global cloud of the internet, which essentially makes the internet a gold mine for hackers. Every information and knowledge that has been put to the cloud, is at risk of getting hacked and transmitted to cyber-attackers. These data exchanges and information can result in a variety of different ways such as exploitation of privacy of a person and even to the hijacking of the codes of nuclear weapons which would create a serious tension environment around the world.

To summarize, cyberspace has become a term that we use in our daily lives now and is a part of our life already. There's no way of going around it. The interactions it provides have also become necessities in our businesses, forums and websites. However, all the data and media

we share and put on the web is at great risk. Thus, solutions and reinforcements that the whole world could input and use, would be a game-changer against cyber attacks.⁴

b. Data

Data essentially means a set of values with quantitative and qualitative values. While data is generally used for scientific research ratings, it is also being used in a variety of different branches including finance, transport, nature, meteorology, geography, culture, etc.

The terms data, information and knowledge are commonly being used in the same meaning but there are some key things that differentiate these three words. For instance, data becomes information or knowledge when data is viewed in post-analysis reports.

We can analyze, view, report, measure and collect data additionally, we can visualize the data by using graphs, images and other analysis tools. Data's main concept revolves around information or knowledge being represented as coding in a viable form for better using and processing.

Data can also be unstructured (also know as human readable) and structured (machine readable). The key difference between structured and unstructured data is that unstructured data cannot be read or encrypted by the technological machines. They can only be read by humans. On the other hand, structure data can be read, coded and encrypted by machines which help the human force used on certain jobs and projects since now machines can do it without any tire. For a program to be able to perform its instructions on the data, it has to be structured. When the program applies the instructions, we get software out of it.

As an example of how this affects the business and transport branches, US Naval Officer Matthew Maury took aged, hand-written shipping logs and turned them into coordinate routes which then he processed these routes to reduce the average naval journeys by 33%. This is crucial as now the Navy consumes less fuel and resources throughout their journey, staying far more sustained than before.

⁴ <https://www.techopedia.com/definition/2493/cyberspace>

i. Personal Data

This kind of data has only the users information and keeps it specific to the user him/herself. It covers the user's location, email address, demographics and any identification the user owns. At normal conditions, this kind of data is not exploited to any kind of foreign user on the internet. Yet that does not mean that this information cannot be leaked via cracking of certain codes and hacks. There have been many scandals of celebrities (such as the Ashley Madison Scandal) cause of the leakage of their personal info and privacy. Many companies and websites collect your personal data (especially social media websites like facebook, twitter, Instagram, etc.) via when you log in to your account with your email address, or when you are writing your credit card information. Often times these sites use your knowledge to make suggestions and advertisements depending on your personal liking, selections and preferences. However, these companies can aggregate (depersonalize) your personal data and then sell it to other companies for advertisement and competitive research reasons. This is one of the reasons why people get targeted advertisements that they are not genuinely interested in.

ii. Transactional Data

Transactional is basically the data that requires any kind of action to collect. Clicking on an advertisement, making a purchase in a website, visiting certain links are just a few examples of what it is. Pretty much every site collects transactional data from the users via certain analytics, 3rd party systems or a data collector of their own.

Transactional data is very important for businesses, since it provides exposure of variability, optimizes the business operations to the highest quality. With the examination of huge data, the possibility of uncovering hidden patterns and correlations in the data is there and the patterns allow big advantages to businesses such as effective marketing and higher revenues.

iii. Web Data

Anything that you search, click, watch, listen, view on the internet can count as web data. It can be governmental data and also the score of a football match. It's a catchall for anything you can find on public facing (not stored in an internal database.). Studies on this data can be really beneficial as it can be informative, especially when communicated well.

Web data has a big role in the virtual world because its one way for businesses to access and interact with information that is not generated by themselves. Businesses need internal, external and global knowledge of what is going on with their organizations and the wider market before making serious BI decisions.

The usage of web data can vary. It can be used to monitor other competitors in the business, traction of potential customers in the web, also keeping the traction of their channel partners, building apps and many more. However, web data's usage is not limited to these, as with the ever-growing technology, new ways of using web data are discovered every day and it seems like there will be many more to come in the following years.

iv. Sensor, Environment Data

Sensor data is created by objects and is often called as "The Internet Of Things". It covers every device you can imagine ranging from your smartphone that you use every day to anti-air military defence systems.

So far, the sensor data has been used in many different branches, but it is really effective on optimizing processes. As an example, an airline company named AirAsia saved around 30 to 50 million US Dollars with the usage of GI sensors. This helped them reduce operating costs and increase flight rates. This shows us that machines can help human life by increasing productivity in various sectors and in the near future, sensor data is expected to be used more commonly than the current time.

v. Collection of data, Big Data

Technically, every category of data that has been aforementioned before (personal, transactional, web and sensor data) can be counted as big data. There isn't a certain or consensus criteria of what makes a data "big". The term relates to the increasing amount and the varieties of data that we use and gather into a data collection.

As a bigger percentage of the world's information goes online and is digitalized, analysts can use this information to create data out of it. Social media, online books, music, videos, etc. Have all added up to the huge increase in the current data that can be analyzed.

The difference between the “big data” and the “regular data” we were analyzing before however, is the tools that we use to collect and conserve it had to evolve and revolve around the increase in the size and complexity of the data. This helps us process datasets that we can use for a more complete perception of the globe and web around us.

vi. Importance of Data Collection

Data collection is a process that consists of the measurement and gathering of the data. The collection is usually done via software and there are many techniques, strategies and ways to collect data. Since most of the collection is classified as “electronic data” and since this kind of data encompasses such information, it counts as “big data” as well.

Data collection provides businesses and management with the quality information and knowledge to make a decision from further research and analyses. Without it, many companies would be at the back of the technology and marketing race, using outdated methods and information. With data collection, companies can lead the race and analyze the issues easier and faster than other competitive markets.⁵

c. Privacy

Privacy is humanity’s fundamental right for the protection of dignity and its autonomy. It also is the cornerstone of other human rights such as accommodation, travel, etc. Privacy enables us to create barriers and manage the boundaries of our information to defend ourselves from unwarranted interference of our personal lives, which also creates our perception to the world and how we won't to interact with other people around us. These boundaries also determine who can interact with our private information and also who cannot.

The laws and rules that protect privacy give us the opportunity to assert our rights against significant power imbalances.

Thus, privacy is an essential way for humans to seek self-protection and also the society, against unjustified usage of power, by eradicating available knowledge and information about ourselves and also what can be done against us while also gaining protection against people who may try to exert control.

⁵ <https://www.import.io/post/what-is-data-and-why-is-it-important/>

Privacy is a must have in human life. It essentially reflects our perspective of life via our selections and restrictions we put and it changes day by day sometimes even involuntarily. It is a free space where we can feel truly as ourselves without any sort of judgement, creates a place where we can think and cognitive independently and gives us the authority of who will know what about our identities.

i. Right of Privacy

The right of privacy refers to the concept of one's personal information is under protection against public scrutiny. This right of privacy is generally protected by statutory laws. An example is the Health Information Portability and Accountability Act, abbreviated as HIPAA, conserves the citizens' health information.

The right of privacy must always be balanced and harmonic with the public's interests with the inclusions of public safety promotions.

ii. Right of Publicity

Just like a person has the right to keep their personal knowledge hidden from the public, he/she also has the right to use their identity as promotional commercials. Yet an unauthorized use of the identity is recognized as infiltration of privacy.

iii. Right of access to Personal Informations

A citizen has the right to determine what kind of personal information and knowledge will be collected and how will the information be used. The Privacy Act of 1974 is the obstacle that holds back the governments from unauthorized disclosure of a citizen's personal information. The people also have the right to review their personal information that is conserved in the system and request corrections if needed.

Related to the right of privacy, The Financial Monetization Act of 1999, has financial requirements and request institutions to provide the customer with a privacy policy that shows

what type of personal information is being collected from them. The requirements are also needed to have a safeguard that protects certain information collected from the citizens.⁶⁷⁸⁹

iv. The Importance of Privacy in Human Life

Data collection is a process that consists of the measurement and gathering of the data. The collection is usually done via software and there are many techniques, strategies and ways to collect data. Since most of the collection is classified as “electronic data” and since this kind of data encompasses such information, it counts as “big data” as well.

Data collection provides businesses and management with the quality information and knowledge to make a decision from further research and analyses. Without it, many companies would be at the back of the technology and marketing race, using outdated methods and information. With data collection, companies can lead the race and analyze the issues easier and faster than other competitive markets.¹⁰

d. Information Types

Information is referred to as facts provided or learnt about something or someone, which is really a meaning that just scratches the surface of what information essentially means considering all the different kinds of information flowing throughout the globe via world-wide-web. There are so many things to type, search and learn in the global cloud that, we could fill books with billions of pages, and the books would fill thousands of libraries by writing down every data found in the network.

Today, we can find information about anything that has been discovered, invented and implemented to people’s daily lives. There are many tools we can use to get information, whether it is a book, a magazine, an encyclopedia, a painting or a photo and etc. Although all of these are good sources to find information, the most efficient way of getting more

⁶ <https://www.livescience.com/37398-right-to-privacy.html>

⁷ <https://www.justipedia.com/definition/2750/false-light>

⁸ <https://dictionary.cambridge.org/dictionary/english/appropriation>

⁹ <https://dictionary.cambridge.org/dictionary/english/intrusion>

¹⁰ <https://www.import.io/post/what-is-data-and-why-is-it-important/>

information in a shorter time span can easily be recognized by everybody nowadays as the internet itself.

i. Interconnected Networks, Internet

The internet has been in development for nearly 30 years before its initial invention starting in 1965 and being officially released in 1991 as “World Wide Web” and since the day it entered our lives it instantly changed human life in an enormous way. Via the internet, people were able to get any information that has been coded or registered into the World Wide Web with the snap of a finger. Years have passed and technology has evolved. So did the internet. Many computer engineers and IT technicians have started to create their own software and websites on the internet. Some names include Microsoft, Facebook, Youtube, Reddit, Amazon, etc. These names have contributed to the evolution and improvement of the internet and they have also spread the popularity of the internet to global scales. Almost every person in the world is aware and somehow connected to the World Wide Web. It became an inseparable part of our lives in a really short time. The cumulative knowledge collection inside the internet cannot be valued or measured since the knowledge inside the cloud is at a constant change and the knowledge it contains is beyond imagination.

ii. Geolocation

People are free to travel and visit wherever they want to as this is one of the humans’ key rights. The transportation sector has seen a lot of revolutionary changes and has been in development for many years and counting. This allowed people to travel quicker and more. Nowadays people can go anywhere they please to.

With these increases in travel rates, the surveillance of people also has seen a significant uprise. As technology developed, many more devices and systems such as GPS (Global Positioning Systems) Satellites were implemented for traction of millions of people and also products in the world.

Although the surveillance brings a lot of goods to our lives, it wouldn’t be genuine to say that there are no negative effects of it. The overuse of surveillance devices (CCTV’s, tape recorders, unmanned drones, etc...) by the government can lead to the discrimination of people’s right to privacy. This can lead to the public’s role in the country to weaken as people

would question if they are really safe and secure under their own government if authorized people can perform such acts on them.

As an example of such acts, many companies like Google and Apple, collect and store their users' data, knowing where the user is occupied at, which stores they visit, what transactions they make in the digital markets and so on. Via this data, the company sends advertisements accordingly to the information that the data holds in it.

iii. Medical

Technology's one other blessing to our world comes at the medical branch. With new systems and devices, people's medical and health information can be collected and stored for quicker diagnoses of certain diseases and illnesses, more efficient supplements of medicine, eradication of errors in certain surgeries and operations, etc.

Further detailed studies on genetics granted us insight upon storable encodation of human DNA, thus resulting in better recognition of genetic diseases altogether.

Amniocentesis, for instance, is a medical procedure that is used to identify possible genetic disorders and chronic abnormalities that may occur in the fetus' genetic information. To execute this process, a certain amount of amniotic fluid, which contains fetal tissues, is extracted from the amniotic sac that surrounds the developing fetus. After the extraction of the fluid, fetal DNA goes through an examination to indicate if there are any chromosomal abnormalities. This gives people the opportunity to prevent genetically disordered births and abort them.

This is one of the many cases that benefit the health sector through exemplary usage of medical information. With such knowledge, we can now indicate disorders that occur and actually prevent them from happening before it is too late.

iv. Financial

The global market of the world has been on the uprise as technological developments on data transformations and information transmitting have been implemented continuously, mostly throughout the last decade. With these upgrade and implements, the transactions made through the virtual world have become more efficient and reliable with certain security

reinforcements which inevitably increased the popularity of microtransactions through the internet and amount of credits stored into the cloud.

With these revolutionary developments, people are now able to check their funds, make transactions, obtain more funds from bank accounts if needed, see their purchase history and so on. It really created a new dimension of marketing and set a new level of accessibility and security for the financial data storages.

Many businesses and financial markets have started to focus more on financial data storage and information since many economists believe that in the foreseeable future, the world finance is likely to be dependent on digital concepts and work through financial data encryption of funds and credits.

v. Protection of Information System

Information Systems (IS) are formal, sociotechnical, organizational systems that are designed to process, collect, store and distribute information. The information systems mainly composed of 4 elements named as:

-Task

-People

-Structure (or Roles) and

-Technology

Any specific information system's goal is to support operations, management and decision-making. An information system is also the information and communication technology (ICT) of the organization that uses, and also the way in which people interact with this technology in support of business processes.

As such, information systems inter-relate with data systems and activity system separately. It is also a form of a communication system in which data represent and are processed as some sort of social memory. Such systems can also be considered as a semi-formal language which supports human decision-making and actions.

There are many types of information systems such as transaction processing systems, decision support systems, knowledge management systems, learning management systems, database management systems, and office information systems. The critical factor for information systems is information technologies, which are designed to process actions that the human brain and will is not capable of doing, such as handling huge amounts of information, calculating complex calculations, controlling many processes at once and so on.

The six main components of an information system are listed below:

- Hardware (Machinery)
- Software (Computer programs and manuals)
- Data (Information)
- Procedures (Policies that operate the system)
- People
- Feedback (Not necessary for the system to function)

Information systems have earned an important and unique spot in our lives as we can legitimately store every information we want to write to the cloud freely. Nevertheless, we must keep in mind that everybody shouldn't know everything about ourselves and some things should be kept precisely and securely. Yet many information systems are able to be decoded, hacked and cracked through by many cyber attacks and it results in the invasion of privacy. At times, people even are not aware of their privacy getting infiltrated, thus they do not take any actions to prevent it. This is a serious issue that will continue to grow as the technology develops since there will be many more devices and programs that the hackers can use to invade the personal information of people. Hence, the security systems and reinforcements implemented to the information systems should be reviewed, repaired and improved after a certain time span passes without any latency for the systems to be able to keep up with the developing hacking systems.¹¹

¹¹ <https://www.britannica.com/topic/information-system>

III. Authorities by Countries

Day by day the importance of private life is getting stronger. Since there are so many hackers who use their knowledge for stealing data, the privacy of information is now one of the trending topics around the world. Countries and some organizations are starting some campaigns to show their support for data privacy also they establish or change their laws to prevent data theft. Some of the members of G20 committee has established organizations in their country in order to protect their citizen's private data's and fight against hackers and so.

a. European Union

European Union is one of the biggest supporters of data protection. All of the members gathered and wrote a directive about data protection in 1995. The name of the directive is the Data Protection Directive. This directive includes harsh and exact rules about processing period of personal information. It basically mentions that managers of any place have to inform their customers if they collecting data from them also they cannot share customers data without customers consent. The directive also says that managers have to tell the aim of data collection which means where will they use data and which companies or persons will know about their personal data. This directive was adequate but with the developing technology, circumstances have changed and the European Union decided to adopt new legislation named as General Data Protection Regulation(GDPR). Acceptance process took some time but in 2018 European Union members recognizes this new law and it is currently in practice within the borders of EU.

b. Personal Data Protection Authority (Turkey)

Personal Data Protection Authority (PDPA) is an organization which is located in Turkey. It has been established on January 30, 2017. Protection of Personal Data Law officially announced on April 7, 2016. After the establishment of law, 3 candidates have been elected by Grand National Assembly. The current president of PDPA is Professor Faruk Bilir who works constitutional law and political science. The mission of PDPA is to protect citizens personal data, ensure security for data privacy and raise the knowledge about the importance of data privacy. PDPA depends on current Turkey constitution and takes acts respect to laws. The

second mission of PDPA is to create and develop competence in the area of data-driven the economy for private companies. Their biggest aim is having a great effect on public awareness about data-information privacy also becoming the biggest data protection authority in the world.

c. Federal Commissioner for Data Protection and Freedom of Information(Germany)

Federal Commissioner for Data Protection and Freedom of Information(BfDI) is the authority for data-information protection in Germany. BfDI also supports the freedom of information and encourage all of the persons for speaking independently. It established on January 1, 1978, and it still continuing their presence since that time. The current commissioner of BfDI is Ulrich Kleber. Since January 1, 2006, BfDI follows German Freedom of Information. With the European Union regulations which have been made in 2016, BfDI is an independent federal agency. German Federal Ministry of the Interior and judicial oversight of the German federal government are the supervisors of BfDI and technical supervision is not using for this federal commissioner. Federal commissioner provides total data and information security for government and companies also for telecommunication and mailing service. Every half of a year, federal commissioner writes a report about the situation of data and information privacy. A privilege to deny to give proof is accessible to the Federal Commissioner concerning people and certainties with which comes into contact in his ability as Federal Commissioner. He is likewise approved to choose about his representatives' refusal to give proof.

d. Office of the Australian Information Commissioner (Australia)

Office of the Australian Information Commissioner (OAIC) is an Australia based commissioner which is trying to provide full security for data privacy and freedom of information. It has been categorized as a government agency which works independently and it acts as a national authority which provides data security for their whole nation. It formally established and recognized by the Australian Government in 1989, and until 2010 it was known as Officer of the Australian Privacy Commissioner. The current commissioner of this organization is Angelene Falk. Three main functions can be seen the office has, which are private functions, freedom of information functions and government information policy functions. Just like the other data privacy organizations, it has a couple of missions and responsibilities. These responsibilities can be defined as performing some investigations,

controlling agency management, informing and educating citizens, companies, some other government agencies about data-information privacy issues and so.

e. Information Commissioner's Office (United Kingdom)

Information Commissioner's Office (ICO) is an independent organization that protect and control the United Kingdom's information rights. It has a couple of office in different cities for doing that work in the United Kingdom. Current head commissioner of this structure is Elizabeth Denham since July 15, 2016. History of ICO is based on 1984. In 1984, after the establishment of Data Protection Registrar, ICO showed up and started to do their jobs. Firstly they started with 10 people, then it grew up and now more than 500 people work for this organization. Their prior role in the UK is protected information rights of their citizens and handle the data privacy problems. Their duties, in general, are taking some amount fee from who process their customer's information, follow the legislation which are valid right now, handling citizens problems about data-information related issues and organizing some programs for enhancing people's awareness about information issues and develop new brand new solutions.

f. Office of the Privacy Commissioner for Personal Data (PR China)

Office of the Privacy Commissioner for Personal Data (PCPD) is a body of Chinese Government which works for the protection of information and data privacy of citizens. It is a subsidiary organization of Hong Kong. The current minister of this commissioner is Stephen Wong since August 4, 2015. He will act as head commissioner until 2020. PCPD is being divided into six divisions which are Complaints Division, Compliance Division, Legal Division, Policy and Research Division, Communications and Education Division and Corporate Support and Enquires Division. These different departments have various duties and fields. Having that kind of different divisions make the commissioner's works much easier. Complaints Division's duties are basically taking complaints from citizens or organizations, helping them about their problems and gives them advice about information issues. Compliance Division's duties are following breaches and notifications about data privacy, check compliances and make investigations and make suggestions about upgraded compatibility for data users. Legal Division makes legal suggestions to citizens about data issues, watches improvements of data protection laws in foreign countries and monitors also

controls the legal process of data privacy-related issues. Policy and Research Division's duties are making some policy recommends about personal data issues and contributing with their suggestions to investigations also compliance checks. Communication and Education Division's duties are making some programs about information-data related issues for citizens, making suggestions to companies about corporate communications strategies and organizing some press conferences. Corporate Support and Enquires Division's duties are supplying governing of resources and strategic planning, taking some questions and problems from citizens also organizations and producing some answers for them, giving and keeping up the bookkeeping, finance, obtainment and money related planning frameworks.

g. National Commission on Informatics and Liberty (France)

National Commission on Informatics and Liberty (CNIL) is an independent organization of France Government. The reason for establishing this organization is SAFARI program. SAFARI program is an old program that made French people very angry. French Government tried to develop a program to identify the French public with the usage of government services such as hospitals and agencies. Citizens did not remain silent against that kind of move and made a riot. After these situations, CNIL showed up to took to control about data privacy and information freedom. CNIL started to take real actions at the beginning of the 1980's. Since 1980's CNIL is fighting for data privacy and information freedom. The current president of this organization is Isabelle Falque-Pierrotin. CNIL mission is recording the information systems which operates personal information. Also, they control and monitor laws that related to this area and if CNIL sees a person or company did not obey the rules-laws, they can warn the lawbreakers.

IV. Legal Protection of Right of Privacy

Every person is living their own life. They live with some secrets and their own stuff. Sharing their information or secrets are depends on them. No one can get into their lives and share their information without one's consent. But nowadays with the growing technology, some serious problems emerged. Hacking someone's cloud is becoming usual and people's private life does not mean anything for anyone no more. Even some big social networks such as Facebook sold their users' data to different kind of companies. In order to prevent that

governments taking some actions and establishing new organizations such as but not limited to Personal Data Protection Authority. But this kind of organizations cannot act according to their wishes. Organizations must act in accordance with the laws of their respective countries or international laws. In this context, some major organizations just like the European Union and some countries have enacted laws on data privacy.

a. Laws

1. General Data Protection Regulation (European Union)

General Data Protection Regulation is an information privacy law that countries follow in the borders of Europe. It is an enhanced version of the Data Protection Directive. European Union's member countries gather and debate upon this new data privacy law and in 2016 they finished it. But the implementation date of this law is 25 May 2018. On 25 May 2018, the General Data Protection Regulation took the place of Data Protection Directive. The GDPR contains 99 articles and extra 173 expressions about data privacy. The prior mission of GDPR is to let people control their personal information and enhance the relations in the field of international business by improving the administrative condition. This current law includes the requirements of data processing structure in the borders of Europe and every single company that process the data of persons have to do their job within the framework of this law.

2. Privacy Act (Canada)

Privacy Act of Canada has been established in 1983. History of Privacy Act starts in 1977 with the emerging of Office of the Privacy Commissioner of Canada. After six years of works, in 1983 Bill C-43 was passed during the Parliament and then Privacy Act officially established. That act contains some important points like if one is not allowed access his/her personal data, he/she can apply to the court and with the decision of Federal Court, one can be able to reach his/her personal data. Articles of law continue with if it is not related with foundation or operational schedule, government institution cannot receive the personal data and if some company or foundation is collecting a citizen's data, they have to inform this citizen and explain why their personal data is being collected. Also, act says that every single citizen of Canada have right to access their personal data and if there are some mistakes about his/her personal data citizen can apply for a correction about his/her information.

V. Issues

Great improvements of technologies create many solutions to today's world; however, these abilities create many numbers of issues. This part of the study guide provides some number of issues in order to discuss in the committee. There is no doubt that issues are not limited and further issues can also be discussed through the conference.

a. Safety vs Freedom

The first question is what is the right balance of safety and freedom. About this issue, Benjamin Franklin stated, "They who can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety."¹² This statement from Franklin supports the idea that without liberty, it is not possible to have both safety or freedom. However, today's world it is a very debatable topic. Due to the complexity of two concept, freedom and safety, it is necessary to understand what are they. Kavi Shah defines these concepts as Freedom and safety have a great connection between them. Freedom and safety are truly symbiotic words meaning that they are both affect each other.¹³ However, what is the ideal balance of safety and freedom? How much freedom should be sacrificed in order to have a safety? These questions have been debated since the first modern civilizations emerged. The same debate is now observing in the digital age.

i. Mass Surveillance

The first issue of safety vs freedom debate occurs in the area of mass surveillance. Today's governments now can able surveillance their citizen by any mean due to technological abilities in order to protect their citizens as they stated. However, this mass surveillance creates many debates and privacy issues. How much governments can monitor their citizens. Should be a limit or not. According to some supporter of mass surveillance, the freedom should be sacrificed for safety. During these debates are being discussed, the Government of PR China introduced a national social credit system for their citizens. The system aims to rate each citizen, and gives rewards and also punishments. These punishments include travel ban,

¹² Franklin, Benjamin. "3929. Benjamin Franklin. 1706-1790. John Bartlett, Comp. 1919. Familiar Quotations, 10th Ed." Bartleby. N.p., 1755. Web. 25 Aug. 2013.

¹³ International Journal of Scientific & Engineering Research, Volume 4, Issue 10, October-2013 ISSN 2229-5518

exclusion from private schools, and adding to the public blacklist. Furthermore, citizens can share their credit scores with other companies such as China's dating service, Baihe in order to demonstrate social credit score as social status. The system allows to monitor every citizen's action and if they did "bad" actions, their credit score can be lowered. These system rises many criticisms, people have banned domestic flight due to their low scores, and some low score citizens can be denied if they attempt to rent hotel and such. Furthermore, the reasons for lowering someone's scores include excessive online gaming, personal shopping habits and many other actions that do not affect society much. Besides, PR China claims that this system will increase the safety of its citizens thus will reduce crime. However, some people believe it will reduce to freedoms including freedom of speech.

ii. Prediction Calculation

Thanks to the new method for analyzing big data, it now possible to predict what is going to happen in future. The system scans the big data and understands the patterns, from these patterns the system can give the probability of a possible event. For example, as a usage case, from a person's personal data, it is possible to guess that same person has a great risk of committing a crime. These situations rise many questions, should governments can act from these predictions or not?

b. Censorship

Censorship is one of the major issues for data. One of the sides claims that that, every person should have the right to access all data, others claim there should be a limit. There is no consensus about this issue.

c. Radicalization in Social Media

Another issue is radicalization, there is no doubt that radicalization creates great risk for human civilization and mostly for civil order. According to Robbin Thompson, since mobile devices become more popular day by day, more people get access online contents every day, the usage of social media start to involve radical movements including political movements thus, create a more open environment for radical acts. Due to these, social media can be used

as a platform for recruiting members for radical actions. ¹⁴ Governments can limit the access to social media, or ban certain content for this action but, some countries believe that any banning action can be a direct violation for freedom of free-speech thus, they are not open for limiting these social media platforms.

d. Debatable Usage of Personal Data

Another issue come from the debatable usage of personal data, at that point, there is no consensus about how sensitive personal data should be used. As an example, should big cooperation that stores personal data have right share personal information if there is urgent national need? This question has been asked many times. For instance, when FBI demanded to unlock a captured a terrorist's iPhone from its manufacturer. Apple rejected this demand due to right of privacy¹⁵. Should Apple have the right to protect its users' data even there is official demand from responsible government institution?

e. Safety of Data

i. Safety of Personal Data

Since personal data have great importance, it is critical to protect. There is no doubt that personal data should be protected. However, the leak of personal data has been observed throughout history. Illegal selling/sharing create great risk for civil order. One of the recent scandals is Cambridge Analytica Scandal for this issue. In early 2018, it is surfaced that Cambridge Analytica had accessed millions of people's personal data from Facebook and used as their political aims. Cambridge Analytica use these illegally accessed data for election campaigns includes but not limited to, 2016 Donald Trump's and Ted Cruz elections campaign, 2016 Brexit Referendum, and 2018 Mexican general election. These personal data used to create an individual campaign for each Facebook user by using artificial intelligence. This scandal clearly demonstrates how important to protect personal data and its privacy.

¹⁴ Thompson, Robin L.. "Radicalization and the Use of Social Media." *Journal of Strategic Security* 4, no. 4 (2012): : 167-190.

DOI:
<http://dx.doi.org/10.5038/1944-0472.4.4.8>

¹⁵ <https://www.cnet.com/news/fbi-asked-apple-to-unlock-iphone-before-trying-all-its-options/>

VI. Conclusion

It is absolute that data has great importance in today's world. The importance of protection of personal data will increase day by day. Governments and decision makers should consider this importance and act according to. There are many issues that are required to be answered. Some of possible questions are provided in the next section of this study guide.

VII. What should the resolution cover?

- What is the role of governments for issues?
- What is the right balance for safety and freedom?
- How much governments should access private data in the sake of national defence?
- What is the right way to do mass surveillance?
- Do governments have the right to censor any data?
- What kind of acts should be taken against data thief companies?
- What kind of regulations can be done for freedom of information and data privacy?

