Committee/Council: Political Committee
Issue: The Issue of Government Surveillance
Student Officer: Nour Safadi
Position: Co-chair

Introduction:

Governments have always looked forward to maintaining security in their countries, and protecting their citizens. Surveillance has always been one way to do so. Several methods were used in the beginnings, in which countries monitored their citizens; however, technology has led us to a day where each word, move, and opinion is being monitored without the need of an actual person monitoring us. Governments around the world have developed systems that can collect data about individuals, by simply monitoring their technological devices and actions. This type of government surveillance has been rising immensely with the rise of the political conflicts around the world. Some believe that this is invading citizens' privacy without their consent and they criticize a lack of transparency in governments' acts, thus leading to lack of trust between citizens and governments. Accordingly, this issue must be prioritized globally.

Definition of key terms:

1) Surveillance:" continuous observation of a place, person, group, or ongoing activity in order to gather information." There are different types of surveillance, which are:
a. Electronic surveillance: which is done by electronic devices and means.
b. Vigil: which is the surveillance done in the purpose of guarding and observing.
c. Stakeout: which is a kind of surveillance in which the police monitors a specific place or a person.
d. Spying: which is the act of surveillance while keeping it confidential (without the knowledge of the person monitored).

2) Right to Privacy:" the right of people to make personal decisions regarding intimate matters; under the Common Law, the right of people to lead their lives in a manner that is reasonably secluded from public scrutiny, whether such scrutiny comes from a neighbor's prying eyes, an investigator's eavesdropping ears, or a news photographer's intrusive camera; and in statutory law, the right of people to be free from unwarranted drug testing and Electronic Surveillance."

3) Intelligence Agency: " An intelligence agency refers to a government institution

which collects, analyzes and exploits valuable information and intelligence to protect the national debts. The intelligence agencies help a country to cope with security matters and to protect the nation from a likely security breach; the core purpose of spy agencies is the collection of secret information to secure the country from any internal and external happening which may harm the stability of state either economically or politically. "

Background Information:

It is inevitable that monitoring methods have evolved tremendously in this digital age. The MIT Professor Gary Marx has realized the massive change of the government's surveillance nowadays as the new technologies have canceled the old surveillance means. Technology has taken away the secrecy of personal information, and it has destroyed the physical and natural ways of actually protecting information. Basically, the society now is digitally monitored.

- Governments' viewpoint:

Cameras, tracking systems and all other developed monitoring devices are being widely used by governments nowadays under the title of "Citizens' Security". Nevertheless, the benefits of surveillance are not limited to that. Surveillance expands the government's power. Surveillance leads to the collection of unlimited amounts of information, which may cause a positive impact such as enforcing needed laws which the citizens are demanding, or a negative impact which is enforcing unwanted and unneeded laws, such as banning the usage of a certain website or a social network. On the other hand, governments use the data collected to recognize, and then track their political enemies and anti-government activists. In this way, they can immune the government's power.

- Surveillance vs. Privacy

Some might argue that justice and security require surveillance and some might even argue that citizens should not be concerned about being monitored if they have nothing to fear. These issues are often brought up; nevertheless, those who believe that privacy should be placed as a priority argue that, even though surveillance can provide security and justice, it cancels a huge part of the citizens' own privacy rights. Of course, each individual wants both security and privacy. Unfortunately, as much as this world has developed, these two issues are still controversial; our aim, therefore, is to either balance between them or, democratically prioritize one over the other.
Furthermore, governments use this argument to justify their so-called "monitoring" activities. This argument might be logical, due to the fact that the majority of citizens abide by the laws and are hoping for safe and comfortable living conditions.

Nevertheless, this argument does not guarantee the total secrecy of the data collected. In fact, those who are responsible for collecting the data and protecting it might abuse it. For example, an incident took place in 2007 where Benjamin Robinson, an insider, misused the government's confidential database and systems for personal benefits, keeping in mind that he misused the database over 160 times.

In addition, if people approve of the amount of the 'limited' surveillance programs now, governments will look forward to expanding these programs and will, step by step, completely invade the citizens' privacy. On the other hand, Countries such as the UK and the USA have been collecting fingerprints of new-born children or children in school without their parents' knowledge or consent. The purpose of the personal data is not as clear as it seems.

These are two of the most important arguments, which the whole world is discussing. As explained, they both are logical, yet illogical at some point. This gives another clear reason why this issue must not be ignored, but must be taken into consideration, and measures need to be put into action in order to provide comfortable and safe living conditions for citizens.

- Criteria for Surveillance

A. The framework of data collection:
This is by far the most essential part of any data collection/monitoring activities. This framework basically controls the development of a positive or a negative relationship between governments and their citizens.
Governments must work on high levels of transparency. To achieve this, they need to provide citizens with all the information needed about their spying and monitoring activities.
First of all, citizens have the right to be aware that their data is being collected. They need to know as well who is collecting their data and if it is safe and secure. They need to know whether they have the right to review and check the data collected or not. In addition, they should know if there are laws, which provide the person the ability to sue the government for not abiding by the laws, or for misusing or not protecting their personal information. Governments must also clarify if the surveillance is on citizen or just on a specific group of people (for example: Rich people, poor societies).

B. Means used to practice Surveillance:
Citizens need to be assured that the means and the tactics used for surveillance do not cause any psychological or physical effects on them. In addition, they need to have clear information about the means used. For instance, they need to know whether these means work on personal bases (personal information, and tracking) or impersonal bases (specific groups tracking) ,or if they could lead to any kind of wrong analysis and information.

Any person, whose data is being collected and recorded, would want to know what this data is being used for.

- Risks of leaks:

The risk that can erupt if anyone illegally accesses governments' files and records thus endangers the privacy of citizens. However, some leaks have revealed highly classified information which governments have been labeling as top secret and which have not been known to the public. Disclosure of information by "whistleblowers" has always caused a very controversial debate regarding security, privacy, and freedom of speech.

Major Organizations and Countries involved:

1) USA:

The United States of America's security agency is the National Security Agency – NSA which was established by President Truman in 1952 and has been responsible for the collection of information from signals going in or out the country's borders for national security purposes.

From the beginning of the agency's establishment, the NSA had been seeking the collection of information within its borders to confront growing terrorist groups. After the 11th of September attack on the World Trade Center the government allowed the NSA to start using its previously- developed programs which collect information via phones and internet. This was considered invasive of people's privacy rights as the NSA used interceptions at all the telecom companies and recorded calls and collected all the data received. They also cooperated with Google and recorded the data of research of a certain word. They also monitored bank transactions and saved all people's personal information which was stored on their social media accounts.

Even though this is an American intelligence organization it should be taken into consideration the fact that the UK's intelligence organization, Government Communications Headquarters (GCHQ) , cooperates and shares its database with the NSA.

2) Russia:
Russia is one of the countries which has strict surveillance laws. Russia has numerous intelligence agencies and services which work domestically and globally, Including:
a. Russia's foreign intelligence service: (Global bases)
Russia's foreign intelligence service was initially established in 1991 to gather domestic information, in the purpose of making political decisions, ensuring both economic, and scientific development.

In 1996, president Yeltsin signed a law, which gave the service the authority to work on foreign bases. It is responsible of gathering foreign information and analyzing it. It collaborates with other Member States to prevent organized crime, the proliferation of weapon mass destruction and terrorism.
b. Sorm: (Domestic basis)
Sorm is a Russian system for internet and telephone communication monitoring. Sorm was developed by three stages. Firstly, Sorm-1 allowed telephone communication surveillance. In 1998, a law allowed internet monitoring, alongside the telephone communications, and this is when Sorm-2 was developed. The system had not changed until 2014. In 2014, the internet surveillance was doubled. The system now monitors all social networks, or any other messaging-websites.

3) China:
Domestically and globally speaking, the People's Republic of China has come to abnormal amounts of improvements in the territory of observation and surveillance. The Chinese government has been blamed, in 2014 after a year of inspection- for hacking US military systems. In addition, it has been spying on other nations' web content such as India.

4) EU countries:
EU nations usually offer arrangements, share policies and have comparable frameworks, yet for this situation, every nation has its own particular programs for the purpose of maintaining and keeping up the security of its government, citizens, and its national security. For instance, countries such as the UK, France, and Germany have been practicing large-scale surveillance domestically and internationally.

5) [Bahrain, Belize, Brazil, Caribbean, China, Egypt, Iran, Jordan, Kuwait, Libya, Malaysia, Mexico, Morocco, Myanmar, North/ South Korea, Oman, Pakistan, Paraguay, Qatar, Saudi Arabia, Syria, Thailand, Turkey, Tunisia, UAE, Vietnam, Yemen]:
These nations have blocked certain sites like Skype – and other Voice over IP sites- as a result, they don't have the suitable advances and created frameworks to screen such sites. Likewise, they obstructed certain web contents, which conflict with their national policies.

6) NCSL
National Conference of State Legislatures is a non-governmental organization which takes into consideration cyber issues such as Cyber surveillance. The NGO continually tracks internet privacy laws and surveillance technologies legislations in the USA.

7) ICANN
The Internet Corporation for Assigned Names and Numbers (ICANN) is a nonprofit

international agency that is responsible for the maintenance of several databases of distinctive identifiers connected to the namespaces of the Web, and verifying the Networks secure and stable process and operation.

8) The International Telecommunication Regulations (ITRs):
The International Telecommunication Union is a UN agency since 1947. It works on issues concerning communication and information technologies. The agency held a conference in 1988. It was a treaty administrative conference to set telecommunication regulations. These regulations are relevant to the issue of government surveillance since they codify the telecommunications regulations and limitations. These regulations were not reviewed until 2012, which caused many missing points in their efficiency as a UN agency due to the fast technological development.

History and Development of Surveillance:

Date	Description of Event
1791	The implementation of The Bill of Rights. 4th amendment: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."
1934	The Federal Communications Act formally addressed wiretapping and established the Federal Communications Commission (FCC). Under the Act, wiretapping legal, but information gathered must not be revealed.
1978- 2000	Many negotiations were taking place between stakeholders and member states globally, in terms of the government surveillance issue. Decisions and actions took at this phase expanded governments' mass surveillance, and limited privacy.
October 2000	Britain has been blamed for spying on its partners and allies, particularly on messages between certain individuals, which were supposedly protected by law.
11th of September- 2001	The attack on the World Trade Center.

2001	The Bush Administration issued an order to NSA to start using its spying, privacy-invading systems.
March 2003	Bugging and spying devices were found in EU offices.
December 2007	According to a London-based international watching, Britain was rated as the worst country concerning the issue of citizens' privacy protection.
2008	International fears to expand more and more, over privacy in the digital age.
June 2013	Edward Snowden reveals NSA secret data and information. This information exposed the establishment of rights-invasive, enormous surveillance program.
July 2014	The USA cooperates with Germany in order to come up with a new intelligence-sharing understanding.
August 2014	Snowden reveals that the NSA accidently caused an error in Syria's internet, while spying on it.
January 2015	Barrack Obama and David Cameroon cooperate to prevent terrorism by several methods including electronic surveillance.
May 2015	1) White House votes in favor of reforming NSA acts. 2) France expands surveillance laws after the Charlie hebdo incident.

Governments' surveillance acts are not limited to this timeline, although these events explain how surveillance evolved to reach its current shape.

Relevant UN treaties and conventions, events and resolutions:

1) World Conference on International Telecommunication
The World Conference on International Telecommunications (WCIT) took place in Dubai. It's a treaty conference, which discussed and modified the previous telecommunication treaty conference - the International Telecommunications Regulations-, so that they would be suitable with the interim advancements.

2) The International Covenant on Civil and Political Rights (ICCPR).
Article 17 of the covenant asserts to the importance of avoiding any form of "unlawful or arbitrary" interference with privacy.

4) The General Assembly's resolution 68/167 -18 December 2013- on the right to Privacy in the Digital Age.

This resolution emphasizes the harmful effect of surveillance as it might clash with basic human rights. The resolution asserts the significance of privacy rights whether offline or online and urges Member States to review surveillance legislations to ensure that the right to privacy is protected in this digital age.

Previous Attempts to solve the issue:

Numerous stakeholders including NGOs and the United Nations have been active in trying to ensure that privacy is a right that everyone should enjoy. The report issued by the UN special rapporteur Ben Emmerson noted that governments' internet surveillance is violating one of the UN promoted Rights – Right of privacy. Due to that he asked all Member States to confront the fact that the new measures of internet surveillance are not respecting the right of privacy. As mentioned earlier, the General Assembly's resolution 68/167 on the right to Privacy in the Digital Age is considered essential in highlighting the significance of privacy rights . Furthermore, two years ago, several companies including Apple, Google, Facebook, LinkedIn, Microsoft, AOL, Dropbox, Evernote, Yahoo, Twitter negotiated the issue of government surveillance. These companies have indicated the need of an international reform of government surveillance policies. They, therefore , urged governments to revise and reform laws and policies so that governments could achieve their goals efficiently in maintaining national security. These companies have supported and agreed on the following principles. They also believe that governments should put them into action urgently.

The principles:

1) "Limiting Governments' Authority to Collect Users' Information".

Governments ought to arrange sensible confinements on their capacity to urge administration suppliers to unveil client information that adjust their requirement for the information in constrained circumstances, clients' sensible protection hobbies, and the effect on trust in the Internet. Furthermore, governments ought to constrain observation to particular, known clients for legal purposes, and ought not embrace mass information accumulation of Internet interchanges.

2) "Oversight and Accountability".

Insight offices looking to gather or propel the generation of data ought to do so under a reasonable legitimate structure in which official forces are liable to solid balanced governance. Looking into courts ought to be free and incorporate an ill-disposed procedure, and governments ought to permit vital decisions of law to be made open in a convenient way so that the courts are responsible to an educated citizenry.

3) "Transparency About Government Demands".

Transparency is vital to a verbal confrontation over governments' reconnaissance powers and the extent of projects that are controlled under those forces. Governments ought to permit organizations to distribute the number and nature of government requests for client data. Likewise,

governments ought to additionally speedily unveil this information freely.
4)" Respecting the Free Flow of Information".
The capacity of information to stream or be gotten to crosswise over fringes is fundamental to a healthy and strong 21st century worldwide economy. Governments ought to allow the exchange of information and ought not restrain access by organizations or people to legitimately accessible data that is put away outside of the nation. Governments ought not oblige administration suppliers to find framework inside of a nation's fringes or work mainly.
5) "Avoiding Conflicts Among Governments".
With a specific end goal to abstain from clashing laws, there ought to be a powerful, principled, and straightforward structure to administer legitimate solicitations for information crosswise over purviews, for example, enhanced common lawful help settlement — or "MLAT" — forms. Where the laws of one local clash with the laws of another, it is officeholder upon governments to cooperate to determine the content.

Possible solutions:

In addressing the issue of government surveillance, it is necessary to keep in mind the significance of abiding by internal law, treaties, and resolutions, which Member States signed and ratified. Ensuring transparency is vital, hence governments should formulate policies and frameworks that clarify the legality and limits of data collection and make it known to the public. Each Member State should be required to report to the UN about its legislations and legality of its surveillance acts. The awareness of citizens of governments' surveillance actions and their consent must be taken into consideration too. Laws and legislations need to specify both the extent and nature of governments' power over people. Last but not least, the first and most important step in solving an issue is - as previously mentioned – prioritizing it globally.

Bibliography:

http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15200
https://www.privacyinternational.org/sites/default/files/UN%20privacy%20resolution.pdf
http://www.un.org/apps/news/story.asp?NewsID=49156
http://www.telegraph.co.uk/news/worldnews/northamerica/usa/10106504/Surveillance-QandA-what-you-need-to-know-about-the-secret-NSA-programmes.html
http://www.bbc.com/news/technology-23051248
https://firstlook.org/theintercept/2014/10/15/un-investigator-report-condemns-mass-surveillance/
https://www.eff.org/deeplinks/2013/06/internet-and-surveillance-UN-makes-the-

connection
http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx
https://www.reformgovernmentsurveillance.com/\
http://www.globalissues.org/article/802/surveillance-state
http://cs.stanford.edu/people/eroberts/cs181/projects/ethics-of-surveillance/ethics.html
http://www1.umn.edu/humanrts/usdocs/civilres.html
https://firstlook.org/theintercept/2014/10/15/un-investigator-report-condemns-mass-surveillance/
http://www.theguardian.com/technology/2014/feb/12/internet-governance-us-european-commission|
https://www.itu.int/osg/csd/wtpf/wtpf2009/documents/ITU_ITRs_88.pdf
http://www.pcworld.com/article/2020469/opponents-say-itu-treaty-threatens-internet- freedom.html
http://billofrightsinstitute.org/wp-content/uploads/2011/12/BillofRights.pdf
https://www.eff.org/nsa-spying/timeline
http://www.thefreedictionary.com/Foreign+Intelligence+Service+(Russia)
http://fas.org/irp/world/russia/svr/legis.htm
http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx
http://sputniknews.com/voiceofrussia_us/tag_110652192/
http://learningenglish.voanews.com/content/chinese-hackers-attack-us-military-command/2456083.html
http://articles.economictimes.indiatimes.com/2012-03-31/news/31266517_1_hackers-cyber-espionage-malware
http://www.theguardian.com/world/surveillance?page=81