United Nations Human Rights Council

Table of Contents

This background guide has been adopted and reformed from the London International Model United Nations 2017 background guide for the United Nations Human Rights Council.

Letter from the Secretariat

Delegates,

Welcome to the background guides for MiniMUN 2018! Whether it is your first or third Model United Nations conference, it is our hope at MiniMUN that you will continue to further expand your knowledge of MUN, world issues, and the UN itself.

The purpose of this background guide is to introduce the committee and the topic, as well as help you write your position paper. Details on position paper and submission are available under the Position Paper tab on our website: http://chsminimun.weebly.com/position-papers.html

The topics and committees were chosen to reflect the problems that our world leaders face.As a delegate, you will be stepping into the role of world leaders. You will take on perspectives different from your own, and you will push for what your country believes to be right.

We have diligently worked to make this year's topics even more captivating and advanced than previous years. If at any time, you are having trouble understanding the background guide, finding information on the topic, or writing your position paper, please contact your chairs for help. They are more than willing to assist you to make MiniMUN a productive and engaging conference!

We are very excited to see you at MiniMUN 2018!

Christine Pang and Curran Myers

Secretary-General and Director-General, MiniMUN 2018

Description of Committee

The United Nations Human Rights Council (UNHRC) is an intergovernmental body that addresses situations of human rights violations. The UNHRC strengthens the protection and promotion of human rights worldwide. It was established to be able to replace the previous CHR. The previous CHR had been criticized because it allowed countries that had poor human rights to be members of the committee. The UNHRC was established by the General Assembly. It adopted a resolution on March 15, 2006. Meetings for the UNHRC are held in Geneva and they hold only three regular sessions a year, for a total of 10 weeks. Meetings are held throughout the year on the months of March, for a total of four weeks, in June, for a total of three weeks, and in September, for a total of three weeks. In addition to this the UNHRC at any time can decide to make a special session. These special sessions mainly address any violation to human rights and immediate emergencies. The UNHRC reports to General Assembly directly. If a country engages in a gross or a systematic violation of human rights during its UNHRC membership, the General Assembly is allowed to suspend the country that made this violation to human rights. In order for the suspension of the UNHRC to be able to happen two-thirds of the members present in the GA need to support the proposal.

UNHRC: http://www.ohchr.org/en/hrbodies/hrc/pages/hrcindex.aspx

Evaluating Potential Human Rights Infringements by Technological Developments

Introduction

Technological development is a gradual process of change brought by the use of new technology. Although the term “technological development” can be rather vague, in this topic we will be focusing on technological development in the field of information technology, as well as medical and scientific technology. Information technology mainly means the sending, storing, or gaining of information through the internet. The issue of information technology innovations and their possible future effects on society has been discussed in different ways throughout history; for example, in books such as Huxley’s Brave New World to Orwell’s 1984. The idea that technology would be used by governments as a tool for surveillance (essentially spying on citizens and people) has been significantly present in books and philosophy. However, from the 1970s to today this ‘hypothetical’ debate has become a real-life issue, and more so since the National Security Agency (NSA) scandals of 2013.

The discoveries of the Snowden files and the realisation that governments were using information technology for surveillance of their citizens started the debate of security and privacy and how they violated human rights. This lead to world-wide petitions for harder restrictions, laws and more transparency (government openness and honesty). Today, government use of technology and the lack of transparency is one of the most talked about issues worldwide, with more and more information coming in every day revealing new details about surveillance activities. Relations

between world leaders, national security, and international peace have been put in danger by the discovery of technology and surveillance-related programs.

History of the Problem

Major events in the field of information technology have been happening since 1957, when Russia launched Sputnik 1, a satellite, into space. The technological race of the Cold War caused the United States to start developing the strongest communications system. A program would later give public access to the World Wide Web, changing the field of technology forever. In the 1970s, the United States' Watergate scandal revealed the Nixon Administration had been using the CIA and FBI technology to carry out surveillance and spying on communications of American and foreign citizens. This discovery initiated discussion on the legality of the use of technology that could invade the privacy of people. Although surveillance programs had existed before Watergate, since, at least, World War II, when the first intelligence alliances between the US and the UK began, these weren't revealed until decades later. In 2001, after the 9/11 terror attacks on the World Trade Center in New York, the Bush Administration created and approved the Patriot Act, a law that allowed the US Government to use these technologies at their disposal to conduct surveillance and intercept communications from individuals without needing a warrant. This caused massive controversy because it put people's constitutional rights at risk.

Breaking Point

However, the most controversial development occurred between 2010 and 2013, with the discoveries made by Wikileaks and Edward Snowden; Edward Snowden, in

particular, revealed the existence of massive surveillance programs that were being carried out by the US along with the UK, Canada, Australia and New Zealand, in what was called the “Five Eyes” initiative. The National Security Agency was using human and technological resources to collect large amounts of information not only from American citizens, but also from world leaders (such as Dilma Rousseff and Angela Merkel) and UN officials, and in the process, was obtaining information from other countries’ intelligence programs overseas. The discoveries of the Snowden files caused great chaos in the international sphere: some world leaders and politicians saw their relationships become tense because of these discoveries. The heads of these governments quickly came forward to explain, often naming ‘national security’ and ‘prevention’ policies as the reason for these programs. However, the ‘Five Eyes’ operation countries were not the only ones found guilty of using technology to invade other nations’ privacy: China is one of the countries most often accused of hacking outside its’ borders (India, Taiwan), as well as the Democratic People’s Republic of Korea (North Korea), Pakistan and Cyprus.

Aftermath

The programs revealed by Snowden started a new conversation: a discussion on technology and privacy, and the legality of governments using surveillance technology. Public protests were carried out; companies who shared their data with government agencies were criticised; and a new public poll in 2013 showed American citizens were now more worried about civil liberties and privacy than about terrorism. These feelings were echoed all over the world, particularly in countries like Brazil, Indonesia,

but also Russia and Turkey whose diplomats had been spied on during the G-20 summit in 2009. The activity that Snowden discovered was labeled as espionage by the United Nations and the EU. Within the UN and EU, espionage is illegal and goes against the human right to privacy (the Universal Declaration of Human Rights, International Covenant on Civil and Political Rights and the European Convention on Human Rights). While some countries also had pre-existing laws against espionage, there are also cases of nations with laws that allowed for it. Despite the public dislike for them, in many countries the programs were kept running.

In October 2013, the European Council released a statement that was signed by its leaders emphasizing the importance of the use of intelligence technology in the fight against terrorism. In contrast, the UN General Assembly adopted resolution 68/167 in December 2013 which was about “the right to privacy in the digital age”. This resolution strengthened the importance of this human right and called upon countries to create laws respecting this right and stop actions that violated privacy. Another resolution was later created which appointed a UN official to investigate and report various violations of this right. The latest report was published on March 8th, 2016 in the 31st session of the Human Rights Council, in which it included the obstacles that arise due to a lack of an official international definition of the term privacy as well as praise for legislation that tightened restrictions on surveillance projects. In the meantime, the Obama administration and the NSA defended their program as an important tool for counterterrorism. The Patriot Act, though practically expired and updated on more restrictive terms, was renewed in 2015 and still stands in the United

States, as well as some of the programs that were revealed by Snowden (in particular PRISM).

Statement of the Problem

In Europe, many countries have taken the initiative of creating their own new surveillance laws, such as Poland, Switzerland, the UK and the Netherlands. However, these new laws fall under the scope of the European Court of Human Rights, whose decisions on possible violations of privacy could potentially change the bias in legislation. New surveillance laws are not only a preference in Europe and the United States, but all over the world. A recent report by Privacy International showed Central Asian countries Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan and Uzbekistan had adopted heavy surveillance programs similar to those of Russia, some of them with the help of Israeli technology companies — the same companies that have also provided countries like Nigeria with an extensive surveillance system. Additionally, Privacy International has also reported the sale of British surveillance technologies in Uganda, where they were used against opposing political parties. The Ugandan surveillance operation, in particular, was used to gather critical information to later blackmail parties, under the pretense they were “dangerous to national security” – however when asked about the program, the Ugandan Government denied its existence. Ethiopia, Nigeria, and Sudan have also recently been found to carry out government surveillance. Meanwhile, countries that have pre-existing laws that allow for the use of surveillance technology have continued to use it. Countries like Singapore and Russia are legally allowed to observe the communications of their citizens without them

knowing about it. Russia now has one of the most relaxed laws in the world since July 2016, the anti-terrorist “Yarovaya package”. Although this particular law has been almost impossible to implement, the citizens of Russia have been heavily opposed to it, with online petitions to overturn it and several protests across the country.

Current Situation

Advances in technology have drastically changed the rights of each individual to privacy. By amplifying the voices of human rights defenders and promoting democratic participation, technological developments have allowed for drastic improvements in political participation in parts of the world where governments use repression and violence to stop political participation. However, with technological improvements, governments and private individuals have been able to use mass surveillance technologies to find out information which would typically violate the right to privacy. The recent trend in numerous countries surveying their populations with the excuse of preventing terrorism has allowed governments worldwide to monitor the activity of their citizens online. Monitoring systems are definitely important due to their ability to gain evidence of criminal or illicit activity for government operations and such, but they can easily be abused. Recent scandals in the United States and the United Kingdom, in which it was discovered that vast amounts of data were being collected on millions of citizens, demonstrate the need for governments to be open and transparent about the data that they are collecting and for what purpose.

In a list compiled by Reporters without Borders, it is noted that the governments of numerous countries have begun to utilize censorship and surveillance online. From Vietnam and China to Russia, the United Kingdom and the United States, mass surveillance systems have been used to find out vast arrays of information on citizens, with, or without the help of private companies such as Google, Apple and Microsoft. Tech corporations might very well be forced by governments to share information if legislation is passed against encryption. A good example of this is the case between the FBI and Apple in which Apple refused to unlock a phone which had been left by the San Bernadino shooter. These mass surveillance methods have been used by both democratic countries and authoritarian regimes. The NSA whistle-blower Edward Snowden demonstrated to great effect that even democratic countries have used spying techniques on their own citizens, techniques that are also used by countries like Iran, China, Turkmenistan, Saudi Arabia and Bahrain. From the NSA in the United States, to GCHQ in the UK, the excuse of National Security has been used without the need to ask a judge for legal permission. For example, in 2013, France adopted the “Military Programming Law” in December 2013 which allows the French government to use internet communications and spy on mobile devices without the need to ask a judge. The vagueness of this law and many other laws such as the so called “Snoopers Charter” in the UK has given governments widespread powers to intrude on the privacy of individuals. In authoritarian countries, these techniques have been used to stop public disagreement. For example, in China, authorities cut internet access for more than 48 hours to stop the circulation of reports that members of the

Chinese Communist Party were using offshore banks to avoid tax laws. The presence of vague definitions for what constitutes a crime on the online realm has resulted in the imprisonment of numerous journalists and human rights activists globally. This situation is likely to continue for a long time, as communication technologies continue develop on a drastic scale, governments will also be allowed to survey the actions of their citizens with increasing frequency and accuracy. This has made the need for legislation which limits or provides solutions to victims of internet espionage.

Bloc Positions

While the Human Rights Council has discussed surveillance and other internet issues on a regular basis, numerous countries have publically stated their support for a free and open internet in the council. However, these same countries have passed severe laws which have allowed them to survey their citizens on a massive scale. This means that certain countries may hold public positions in support of human rights, but may actually be violating these rights in their own countries. In the third committee of the General Assembly, SOCHUM, Brazil's representative to the United Nations stated that "human rights should prevail irrespective of the medium and therefore need to be protected both offline and online". While the committee passed the resolution without a vote, it was noted international human rights procedures need to be improved to ensure the privacy and freedom of expression threatened nationally and internationally by mass surveillance activities conducted by the United States.

Questions to Consider

1. What practical measures can member states take to make sure that the rights of their citizens are protected whilst also addressing security concerns?
2. How can individuals ensure that their rights to privacy are protected against large scale government programs?
3. Is it possible for the UN to protect the right to privacy of individuals without encroaching upon national sovereignty?
4. How can the internet be kept free and open whilst considering individual privacy concerns?
5. How can governments protect their civilians without encroaching their privacy online?