

WISMUNC I

The First Iteration Of Washington
International School's Model United Nations
Conference



United Nations Human Rights Council
General Assembly
Background Guide

Table of Contents

Pg. 3: Letters from the Dais

Pg. 4: Topic One

Pg. 7: Topic Two

Pg. 12: Citations

Letters from the Dais

Dear Delegates,

My name is Liam McCuaig, and I am a senior at Washington International School. I have done Model UN throughout high school, and am honored to be serving as your chair. Recently I won an outstanding delegate award at Boston Model UN (BOSMUN), and I have participated in many conferences over my high school years. Outside of MUN, I enjoy sports such as soccer (last year we won States) and basketball, both within and outside of school. Gughi and I play on the same basketball team and we have known each other for a few years now. I am looking forward to a fun and exciting conference.

Best,

Liam McCuaig

Chair, UNHRC

Dear Delegates,

My name is Gughi, and I am a junior at WIS. I have done MUN throughout high school and have participated in many conferences, including BOSMUN with Liam, which through the years has strengthened our friendship. Outside of MUN, I enjoy playing basketball, playing Varsity since freshman year and also AAU basketball. Beyond school and sport, I am interested in engineering and have a passion for cars. Growing up internationally has shaped all of my interests in many global issues including AI, Disinformation and National Security. I am looking forward to an interesting and exciting conference.

Best,

Gughi Sarzi-Braga

Vice-Chair, UNHRC

Topic One: Artificial Intelligence and Disinformation

Introduction

False information has existed for centuries, with governments, political groups, businesses, and individuals using rumors, falsified documents, or propaganda to influence the manners in which people think. Recently, the internet has amplified this problem by allowing disinformation to have the ability to be spread to millions of people in mere seconds. Furthermore, Artificial Intelligence has made it easier than ever to produce disinformation by allowing users to create convincing, deepfake images, text, and videos quickly and easily.

Despite these risks, however, artificial intelligence also has a variety of benefits, ranging from text translation to helping professionals process and analyze large amounts of data in a short period of time. These benefits associated with AI serve as reasons for its global, widespread use, in turn expanding AI's knowledge and data base, as AI uses global information provided to it online.

The central issue of this committee is not to decide if a simple social media post is true or false, but rather to ensure that there are many easy, suitable, and universal ways to determine what information online is factual. People need to have access to accurate and reliable information, understand its origin, compare information across different sources, and produce their own thoughts and opinions about it. The United Nations (UN) uses the term "information integrity" for an environment in which people can access reliable information, express different views, and make informed choices. The increased prevalence of disinformation (specifically that made and supported by AI) is a problem for younger generations, and thus delegates must consider ways in which countries can reduce the spread of disinformation without giving entities complete control over public discussions. A balance must be struck between rules that are too strong and rules that are too weak, with the primary goal of this committee to protect information integrity while respecting universal freedom of expression.

Background

For most of history, spreading information to a large population required access to printing presses, radio stations, television channels, or other costly systems. This meant governments and major media organizations had the ability to control and filter much of what reached the public. These entities had the ability to spread false or prejudiced information, while expending much time, money, and workers in the process. Recently the internet has made publishing much easier, so that anyone with an internet connection has the ability to share media to a large audience in mere minutes. Users of social media are also able to propagate information immediately, such that instead of individuals having to manually search information, platforms can decide what media to place in front of users. These platforms study the habits of users to keep them hooked. While this strategy is primarily intended to make the platforms more money, they also have the side effect of forming echo chambers in which a user will be continuously offered more similar, misleading videos. Disinformation is particularly effective because it builds off feelings, divisions, or stereotypes that already exist. They often evoke a strong reaction in the viewer, who then shares what has now become misinformation with their friends and family without ever checking the original source, leading to further damage. Disinformation is harmful in that it can damage public trust, social peace, and even human rights. False claims may target specific minorities or individuals, leading to increased fear between communities, discrimination against specific groups of people, or even harming specific people's reputations. At the national level, disinformation may increase political, ethnic, religious, or social divisions. At the international level, it may increase tension between countries. A false recording or image could be presented as evidence of another government carrying out a hostile act. This creates a risk that leaders or the public will react before the material has been properly checked.

The Impact of Artificial Intelligence on Disinformation

AI has reduced the time, money, and skill needed to create convincing misleading content. Large tasks that once required comprehensive teams can now be completed by individuals with minimal skills. AI has also brought about a new form of disinformation: Deepfakes. These fakes are dangerous not only because their

depictions can be viewed as real before they are verified, but also since they lead to genuine recordings being dismissed as AI generated. At this stage AI does not create disinformation on its own, but rather humans are still the ones choosing the messages and targets, each with their own motive. Nevertheless, AI has the capability of amplifying existing problems such as political divisions, minimal public trust, and social media by making them easier to scale. UNESCO's Recommendation on the Ethics of Artificial Intelligence calls for transparency, human oversight, accountability, and stronger media literacy. The Global Digital Compact also recognizes the risks of AI-generated content. It calls for cooperation on methods such as identifying AI-created material, proving the origin of content, labeling, and watermarking. However, none of these methods is perfect. Labels may be removed, detection systems may make mistakes, and real content may be falsely described as AI-generated.

Past UN Actions

Artificial Intelligence is a very new, innovative technology. Due to that, there hasn't been too much past UN action in response to its existence and usage, but its threats still loom. In 2021, UNESCO's Recommendation on the Ethics of Artificial Intelligence was the first global standard on AI ethics. It calls for transparency, accountability, human oversight, media literacy, and action against AI-driven misinformation and disinformation while protecting freedom of expression. In 2023, the UN Secretary-General's Policy Brief on Information Integrity on Digital Platforms called for coordinated international action, greater platform transparency, stronger protection for independent media, researcher access to platform data, and warned against broad censorship measures that lack a legal basis. In 2024, UN Member States adopted the Global Digital Compact, committing to an open, safe, and human rights-based digital environment. It promotes platform transparency, media literacy, independent and fact-based information, researcher access to data, and international cooperation to combat information manipulation.

Topic Two: Digital Surveillance and National Security

Introduction

Governments have the responsibility to protect their populations from terrorism, organized crime, foreign threats, and other dangers. Digital surveillance aids authorities in investigating crimes, identifying threats, protecting borders, and finding people who may be planning or have already committed violence or crimes. Modern technologies are able to collect more information than older modalities. Governments now have the ability to track where people travel, whom they contact, which websites they visit, and even the public events they visit. In certain cases, cameras have the ability to identify faces automatically and larger systems can connect data from phones, airports, and government records. These powers can support national security, but they can also influence privacy, freedom of speech, journalism, protests, as well as other rights. People may also change their behavior when they believe they are under surveillance. Journalists also may struggle in protecting confidential sources of information, and citizens may avoid political or religious activities altogether. Not all countries follow uniform rules for digital surveillance. Some require judges to approve intrusive monitoring, while others give intelligence and security agencies broader authority. Some also permit collection of data on a large scale, while others heavily limit it. It is crucial that countries in this committee establish minimum rules for what levels of government should be allowed to be utilized, balance is key, as security needs to be balanced with privacy and civil rights.

Background

Before digital surveillance came into use through computers, government surveillance was still occurring. Authorities used to type letters, use informants, follow suspects, and tap into home phone calls, methods which required much effort, equipment, and time. Due to technological advancements, new possibilities were born, such as listening and recording calls and even seeing who contacted who. This led to the introduction of the use of warrants and other approvals before authorities could intercept private communication, methods now possible due to the internet and mobile phones.

One device connected to a server could reveal someone's communications, location, contacts, interests, purchases, and even their daily routine. Metadata could show this even without authorities reading the contents of a message. Modern surveillance also relies on information held by private companies. Phone companies, internet providers, social media platforms, banks, even transportation services and online stores. This is done by collecting large amounts of user data. Governments may request this information through court orders (warrants), national security procedures, and emergency powers, which could be in the best interest of national security or may be considered a breach of privacy. This issue is made international due to cloud computing. Information about a citizen of one country may even be stored in another country and controlled by a company in yet another country. It is for this reason that questions about which laws apply and how governments should request information across borders arise. The cost of storing said information has also fallen, allowing governments to hold databases containing information about millions of people. This causes governments to possibly collect information first and then leverage it in a way it sees fit for society. Artificial Intelligence (AI) has also helped reduce cost and time as it examines databases quickly. AI searches for patterns, compares faces, translates messages, and can assign risk scores to people. This helps investigators, but also may produce false matches and unjust prosecution. UNESCO states that AI should not be used for mass surveillance or for scoring citizens: they say it should be mixed with human responsibility and final human clearance, and can only be used for a legitimate aim.

Governments and other external intelligence and security agencies have different regulations. Governments may possibly use surveillance to investigate terrorism, organized crime, human trafficking, kidnapping, foreign spying, cybercrime, and serious violence. Communication record, location data, and camera footage are frequently used methods for this. Intelligence agencies may also monitor threats from outside the country, while border authorities may check travel records and identify wanted citizens. From this, however, the issues of "who decides and enforces the rules of who may be monitored", "what evidence is needed to initiate the monitoring of someone", and "which methods are permitted along with how long they can be monitored" arise.

Human rights organizations strive to narrow down the rules and regulations put into place in order to protect global citizens. Conversely, security agencies may strive for more flexible powers in order to prevent and mitigate threats which can now develop and be disseminated quickly. A drawback to this, however, is that there must be someone who decides whether an event is indeed an emergency, and whether certain emergency powers can be used. There is also the issue of powers being abused after the end of an emergency, another prominent issue.

Different Levels and Rules About Digital Surveillance

Different levels of surveillance influence privacy differently. At the lowest level, digital surveillance is observing information which is available to the general public. This includes news reports, public websites, and public social media posts. This is less intrusive, although collective public statements made by citizens and placing it in government files still affects privacy and freedom of expression. Secondly, the next level is basic accounts or limited metadata, helping investigators connect a person to a device or account. This does not reveal the content of messages, but it shows time, relationships, and patterns. A step above this includes private messages, emails, photographs, location history and live communication. This is intrusive and often requires strong evidence and possibly a court order. The fourth level is when authorities continuously track, monitor, and use facial recognition in public spaces. This helps them follow a person's movements and identify others around them, which can be limited to serious threats, and short periods of time. Lastly, the highest level is mass surveillance. This involves collecting information from large populations without first identifying a suspect. Governments argue that this is useful in finding unknown threats, although many argue that it poses a serious risk of abuse, and data leaks. As the levels become more intrusive, some nations argue that they should be more heavily regulated, such as needing stronger evidence, a warrant, shorter time limits, and greater limits on storage and sharing.

There are multiple articles in the Universal Declaration of Human Rights (articles: 12 and 19) which restrict surveillance and protect human rights, freedom of opinion and expression, and a citizen's privacy, family, and home. This is important as people may be less willing to speak or communicate when they believe they are being watched.

Stemming from this, Article 17 of the International Covenant on Civil and Political Rights also protects people from unlawful interference with privacy, creating a legal duty for the countries which have joined. Due to these articles, surveillance must follow some principles. It must follow legality, meaning that surveillance must be based on a clear law, which should explain which agencies use the power and who and what may be monitored, as well as how long it lasts. It must also follow necessity, meaning that authorities must show that that level of surveillance is truly needed to achieve a legitimate purpose, which is another principle that states that surveillance must have a proper public goal, such as investigating a serious crime or protecting national security (for example monitoring peaceful protests would not be legitimate). Lastly, it must also have proportionality, which means that the method used matches the seriousness of the threat, and authorities should aim to use the less intrusive method to achieve the goal. Before surveillance begins, the agency should comply with all of the above, and identify the person, account, device, or location involved. This should explain the suspected threat, the connection between the suspect and the threat, the methods used, and how long it will take.

Past UN Action

To start, in 2013 the UN General Assembly (GA) adopted a resolution on the right to privacy in the digital age. It deemed that states should respect privacy in digital communications and review their surveillance laws and practices. Also in 2013, the UN Special Rapporteur on freedom of expression reported on communication surveillance. The report explains that surveillance can affect both privacy and freedom of speech and expression, calling for new laws, independent authorization, oversight, and more transparency. The UN GA and Human Rights Council have continued to study privacy in the digital age. A 2022 report written by the Office of the High Commissioner for Human Rights focused on surveillance, encryption, and the need for states and companies to follow human-rights standards. Specifically on AI-based surveillance, UNESCO recommends that it should support privacy, transparency, proportionality, human oversight, and review. It also warns against mass surveillance, as per the Ethics of Artificial Intelligence.

The first legally binding international agreement was the Council of Europe's

Convention 108, which focused on protecting people when personal data is processed automatically. It was then modernized (Convention 108+), and that strengthened rules on data protection and oversight. Although it is not a UN agreement, it is an example of internationally shared privacy standards.

Charge to Delegates

Despite all of these past actions, there is still no single rule explaining exactly which levels of surveillance is acceptable. That is the goal of this committee. The resolution should define each level of surveillance and connect each level to the appropriate safeguard. The framework should cover authorization, collection, access, analysis, sharing, storing and deletion. It should also require legality, and necessity as well as access to remedies. Lastly, it should protect amendments, civil laws, as well as religious or political practices, and journalism. Delegates should determine and argue for whether upholding national security is a satisfactory reason to monitor ordinary citizens without cause, or targeted citizens with cause. Delegates must also consider whether, and to what extent, countries who abuse power should be held responsible.

Citations

Human Rights Committee. General Comment No. 34: Article 19, Freedoms of Opinion and Expression. United Nations, 2011.

<https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no34-article-19-freedoms-opinion-and>

Khan, Irene. Disinformation and Freedom of Opinion and Expression. A/HRC/47/25, United Nations Human Rights Council, 2021.

<https://digitallibrary.un.org/record/3925306>

UNESCO. Recommendation on the Ethics of Artificial Intelligence. 2021.

<https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence>

UNESCO. Guidelines for the Governance of Digital Platforms. 2023.

<https://www.unesco.org/en/articles/guidelines-governance-digital-platforms>

United Nations. Universal Declaration of Human Rights. 1948.

<https://www.un.org/en/about-us/universal-declaration-of-human-rights>

United Nations. International Covenant on Civil and Political Rights. 1966.

<https://www.ohchr.org/sites/default/files/ccpr.pdf>

United Nations Secretary-General. Our Common Agenda: Policy Brief 8, Information Integrity on Digital Platforms. 2023.

<https://digitallibrary.un.org/record/4012857>

United Nations. United Nations Global Principles for Information Integrity. 2024.

<https://www.un.org/en/information-integrity/global-principles>

United Nations. Global Digital Compact. 2024.

<https://www.un.org/pact-for-the-future/en/annex-i-global-digital-compact>

United Nations. “Information Integrity.”

<https://www.un.org/en/information-integrity>

United Nations. “Resources on Information Integrity.”

<https://www.un.org/en/information-integrity/resources>

Council of Europe. “Convention 108 and Protocols.” Council of Europe, 28 Jan. 2021, <https://www.coe.int/en/web/data-protection/convention108-and-protocol>.

Council of Europe. “Modernisation of Convention 108.” Council of Europe, <https://www.coe.int/en/web/data-protection/convention108/modernised>.

La Rue, Frank. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. United Nations, 2013, <https://digitallibrary.un.org/record/756267>.

Office of the United Nations High Commissioner for Human Rights. The Right to Privacy in the Digital Age. United Nations, 4 Aug. 2022, <https://digitallibrary.un.org/record/3985679>.

Office of the United Nations High Commissioner for Human Rights. “UN Treaty Body Database.” United Nations Human Rights Treaty Bodies, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?DocTypeID=11&Lang=en&Treaty-ID=5.

UNESCO. “Recommendation on the Ethics of Artificial Intelligence.” UNESCO, 23 Nov. 2021, <https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence>.

United Nations. International Covenant on Civil and Political Rights. Office of the United Nations High Commissioner for Human Rights, <https://www.ohchr.org/sites/default/files/ccpr.pdf>.

United Nations. Universal Declaration of Human Rights. 1948, <https://www.un.org/en/about-us/universal-declaration-of-human-rights>.

United Nations General Assembly. The Right to Privacy in the Digital Age. 18 Dec. 2013, <https://digitallibrary.un.org/record/764407>.