YK '25 MUN

Antalya Private Yükseliş College Model United Nations Confrence 2025

SOCHUM

Agenda Item:

Combating Human Rights Violation in Dig

Under Secretary General:

Vigit Cirim

Academic Assistant:

Nehir Dogdu

Under Secretaries-General: Yiğit Cirim
Academic Assistant: Nehir Doğu

Agenda Item: Combating Human Rights Violations in Digital Surveillance

Table of Contents

1.1 Letter from Secretary General

Esteemed Participants,
It is our paramount pleasure to welcome you to the second installment of Yükseliş Model United Nations Conference 2025. We, Neva Nas Aydın and Ramazan Yandı, will be serving you as your Secretary General's in the upcoming three days. Our Executive Team has put not only the best Academic Team but the best Organization Team so that you can enjoy creating memories in our conference.

Essentially Model United Nations Conferences are great opportunities to improve your debating capabilities, your confidence, your foreign language level and understand how policy is implemented. We can state that Model United Nations Conferences helped us both in our academic and social lifes. For this reason it is our duty to transfer these experiences to the next generations and ensure that they affect them in a similar way.

We hope you have one of the best MUN experiences of your lifes in YKMUN 2025!

Sincerely,
Neva Nas Aydın & Ramazan Yandı

1.2 Letter from Under Secretary General

Dear Delegates,

I welcome all of you to YKMUN'25. It's a big honor to serve as Under Secretary General of Social, Humanitarian and Cultural Committee (SOCHUM), which is the third committee of United Nations.

My name is Yiğit Cirim and I am a high school student at Antalya Anatolian High School. I can not express my feelings for finding myself in that amazing academic team. Dear executive team worked for you to have good memories and experience you can be ensure of that and also we worked hard at night and morning to make you enjoy with your dear Academic Assistant Nehir Doğu in order to make you experience a wonderful committee.

For the topic; we wanted to choose a current and popular topic to make you connect the committee. We know all of you are willing to find solutions and debate about the agenda. The words ''Digital Surveillance and Violations'' are maybe the most heard of words nowadays. Our purpose is making digital surveillance more transparent and reducing violations at minimum level.

Last but not least, **I highly recommend you to read the Study Guide** which we prepared for you by mixing our nights and mornings with Nehir. It would provide you the best understanding for the topic and show you possible ways that you will follow. **If you have any and any and any kind of questions about the committee or problems with the guide please do not hesitate to get contact with me via my number:**

0542 180 48 70

Best regards,

Yigit CİRİM

1.3 Letter from Academic Assistant

Dear Delegates,

I am delighted to welcome you all to YKMUN'25 and our committee the Social Humanitarian and Cultural Committee (SOCHUM) which is the United Nation's third. My name is Nehir Doğu and I will be serving as your Academic Assistant in this conference. I am thrilled to be working with such wonderful people and very excited for you to see their hard work as well. I along with my fellow Under Secretary General Yiğit Cirim have written this study guide to assist in your research.

The Social Humanitarian and Cultural Committee will be debating on a contemporary issue of vital importance that violates human rights. As your Academic Assistant, I expect to see a lot of collaboration when it comes to addressing this issue.

I advise you to read this study guide thoroughly and expand your research on different perspectives; focusing on your allocated country. It is essential to bear in mind that each nation and every perspective holds significance if you are adequately prepared to engage with the agenda at hand.

If you do have any questions regarding agenda, procedure or MUN in general, I am always open to answering your questions and you can reach me through the Email address or my number i placed below. Lastly, I am looking forward to having a remarkable memory in my MUN journey with our committee!

nhrdogu@gmail.com

0501 036 58 09

Sincerely,

Nehir DOĞU

2) Introduction the Committee

The Social, Humanitarian, and Cultural Committee (SOCHUM) is the Third Committee of the United Nations General Assembly. It was established in 1945 in response to the Universal Declaration of Human Rights. SOCHUM focuses on issues related to basic human rights that should be enjoyed by everyone worldwide. This includes the right to life, the freedom to express cultures, the right to participate in politics, protecting children's rights, and promoting social development. SOCHUM also deals with issues concerning special groups such as the elderly, people with disabilities, crime victims, and those affected by drugs. SOCHUM aims to create peaceful solutions to social, humanitarian, and cultural problems around the world. It studies human rights issues, listens to experts, and works with other UN agencies to create resolutions that influence practices in member states. SOCHUM also

initiates studies which encourage recommendations for the promotion of international cooperation and fundamental freedoms for all.

3) Introduction to Agenda Item

Digital surveillance is one of the crucial points of today. In the globalizing world technology has been developing day by day and it brings some kind of positive sides with the negative sides at the same time. Applications, social network sites, governments, companies and more watch us step by step. This surveillance may be right to some extent, but excessive use leads us to violation of human rights. Unfortunately this critical line has been exceeded and started to cause violations. It should be stabilized at a minimum level. We do not say digital surveillance is a completely negative thing for us in some cases it can be really beneficial but especially the private sector holds a risk which should not be unspoken of.

4) What is Digital Surveillance

Surveillance is defined as the careful observation of a place or person, or the monitoring of private conversations over a period of time, typically conducted to obtain information regarding illegal activities. Surveillance is not only employed by states for purposes such as intelligence gathering, crime prevention, and protection of individuals or processes, but also by private corporations for competitive advantage, by citizens for community protection, and even by criminal organizations for illicit activities. The use of advanced technologies to monitor, intercept, collect, analyze, and store digital communications and metadata is known as digital surveillance, which is the most common form of surveillance today.

4.1) Digital Surveillance Types

Surveillance, derived from the French word 'surveiller' for 'to watch over', has seen a tremendous evolution in the era of digitization. Previously a tool primarily for control by governments and powerful groups, it has expanded to encompass electronic data acquisition and interpretation. The use of advanced technologies to monitor, intercept, collect, analyze, and store digital communications and metadata is known as digital surveillance, which is the most common form of surveillance today. The methods employed range from monitoring email and browsing history to using GPS to track physical locations, as well as conducting large-scale data mining of online activity. This form of digital surveillance utilizes a spectrum of technologies, including closed-circuit television (CCTV), biometric analysis, sophisticated tracking software, and artificial intelligence. These technologies, while raising some concerns, also offer tangible benefits such as increased security and potentially enhanced efficiency in service delivery. The table below provides some examples for surveillance technologies.

Audio surveillance	*Visual surveillance*	*Tracking surveillance*	*Data surveillance*
Phone-tapping.	Hidden video surveillance devices.	Global positioning systems (GPS)/transponders.	Computer/internet (spyware/cookies).
Voice over internet protocol (VOIP).	In-car video systems.	Mobile phones.	Blackberries/mobile phones.
Listening devices (room bugging).	Body-worn video devices.	Radio frequency identification devices (RFID).	Keystroke monitoring.
	Thermal imaging/forward looking infrared.	Biometric information technology (retina scans at airports etc).	
	CCTV.		

Computer and network surveillance is the monitoring of computer activity and data stored locally on a computer or data being transferred over computer networks such as the Internet. This monitoring is often carried out covertly and may be completed by governments, corporations, criminal organizations, or individuals. It may or may not be legal and may or may not require authorization from a court or other independent government agencies.

Computer and network surveillance programs are widespread today, and almost all Internet traffic can be monitored. One prominent form of such monitoring is corporate surveillance, which is primarily conducted by private companies.

a) ***Corporate Surveillance***

Corporate surveillance of computer activity is very common. The data collected is most often used for marketing purposes or sold to other corporations, but may also be shared with government agencies under legal obligations or specific cooperation agreements. It can be used as a form of business intelligence, which enables the corporation to better tailor their products and/or services to be desirable by their customers. The data can also be sold to other corporations so that they can use it for the aforementioned purpose, or it can be used for direct marketing purposes, such as targeted advertisements, where ads are targeted to the user of the search engine by analyzing their search history and emails (if they use free webmail services), which are kept in a database.

While corporate surveillance focuses primarily on economic gain and consumer profiling, similar technologies and data collection practices are also employed by governments and, increasingly, by individuals for various purposes.

One common form of surveillance is to create maps of social networks based on data from social networking sites as well as from traffic analysis information from phone call records such as those in the NSA call database, and internet traffic data gathered under CALEA. These social network "maps" are then data mined to extract useful information such as personal interests, friendships and affiliations, wants, beliefs, thoughts, and activities. Many U.S. government agencies such as the Defense Advanced Research Projects Agency (DARPA), the National Security Agency (NSA), and the Department of Homeland Security (DHS) are currently investing heavily in research involving social network analysis.The

intelligence community believes that the biggest threat to the U.S. comes from decentralized, leaderless, geographically dispersed groups. These types of threats are most easily countered by finding important nodes in the network, and removing them. To do this requires a detailed map of the network.

b) Policeware

Policeware is software developed by or for the authorities (e.g. police, intelligence and special services, etc.). It is intended for monitoring citizens' digital communications (e-mails and instant messengers). In the United States, the first example of this kind of software, which became known to the public over time, was the software package named Carnivore. This software was installed in the Internet providers' networks and was used for recording citizens' computer communications Switzerland and Germany, have legislation that regulates solutions, including emails. Some countries have such software. In German-speaking countries, spyware used or created by the government is sometimes called govware.

c) Malicious Software

Malicious software is any software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorized access to information or systems, deprive access to information, or which unknowingly interferes with the user's computer security and privacy. Researchers tend to classify malware into one or more sub-types such as computer viruses, worms, Trojan horses, logic bombs, ransomware, spyware, adware, rogue software, wipers and keyloggers. Malware poses serious problems to individuals and

4.2) Effects of Digital Surveillance

Surveillance is often wrongly seen to be the opposite of privacy and emphasizes this role of privacy as a nullification mechanism for surveillance but at the most basic level, surveillance is simply a way of discovering and noting data that may be converted to information.
The aforementioned information can be used for advancing surveillance technologies to improve the quality of daily life for individuals or provide crucial information for governments in preventing terrorism and malicious acts on a mass scale.
Digital surveillance is one of the keys to reduce loss, theft and vandalism using Closed-Circuit Television (CCTV) also known as security cameras. In this matter it may be used for remote monitoring houses, workplaces, roads and stores for safety and efficiency reasons.

Thus, depending on the context and role played, individuals or groups may be required, find it optional, or be prohibited from engaging in these activities, whether as subjects or agents of surveillance and communication.

Surveillance practices can significantly impact digital rights, privacy, freedom of association, and freedom of expression, which are some of the most fundamental human rights, leading to the fulfillment of many other important rights.

Such surveillance practices can cultivate an atmosphere of fear and mistrust and can amplify discriminatory practices. Moreover, the misuse of digital ID systems can further compromise individual privacy. Governments and organizations may use these systems to track people's

movements, purchases, and even political beliefs without their knowledge or consent, creating an additional layer of human rights infringement. Similarly, abuse of counter-terrorism plans poses another threat, as seen in some instances where such measures have been used to target activists under the guise of national security, thereby suppressing dissent and infringing upon the freedom of expression.

5) Legal Frameworks Related to the Issue

The right to privacy, central to the debate on surveillance, is protected under the The Universal Declaration of Human Rights (UDHR), adopted in 1948, which laid the foundation of modern human rights law . However, it is under threat due to digital surveillance practices. Other affected rights include freedom of expression and association, which are stifled due to surveillance-induced fear. The ongoing debate revolves around achieving the balance between national security requirements and individual rights. Surveillance technologies are governed by frameworks, which are yet to be rooted in international norms and standards. This suggests that there is a lack of emphasis on the balance between enhancing security and respecting human rights internationally. This area has been closely monitored by the United Nations, as the UN Human Rights Council has underscored the right to privacy in the digital age, noting that intrusive surveillance can infringe on human rights. The UN Guiding Principles on Business and Human Rights (UNGPs) these Guiding Principles provided the first global standard for preventing and addressing the risk of adverse impacts on human rights linked to business activity, and continue to provide the internationally accepted framework for enhancing standards and practice regarding business and human rights.The Special Rapporteur on the right to privacy has issued directives, advising states to ensure their surveillance activities comply with international human rights law. The International

Covenant on Civil and Political Rights (ICCPR) also provides a strong international normative framework against unlawful or arbitrary interference with privacy.

5.1) Regional Frameworks

Interpretation and application of these standards can vary, influenced by regional and national contexts. The Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights or ECHR) is a supranational international treaty designed to protect human rights and political freedoms throughout Europe.

The European Convention on Human Rights has played an important role in the development and awareness of human rights in Europe, the General Data Protection Regulation (GDPR) also offers strict rules for data collection and usage, with the aim of protecting the privacy rights of European Union citizens. The European Commission and the Council of Europe have made substantial strides in this area, with instruments such as the Convention 108 on the Protection of Individuals with regard to Automatic Processing of Personal Data. Some have even proposed extending Convention 108 into a global treaty to address the digital privacy challenges worldwide. The non-member states that have ratified Convention 108 are Argentina, Cabo Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia, and Uruguay. These countries, despite not being members of the Council of Europe, have committed themselves to the standards set by Convention 108 for the protection of individuals with regard to the automatic processing of personal data. This reflects the convention's significance in setting international standards for data protection and privacy. The Organisation for Economic Co-operation and Development has also contributed significantly, establishing a landmark agreement on safeguarding privacy in cases of law enforcement and national security data access. However, as discussed in the International Journal of Human Rights, these international norms only effectively apply within the domestic legal frameworks of individual states. Additional measures include export controls such as the Wassenaar Arrangement, which restricts the trade of certain surveillance technologies. The European Union is additionaly developing guidelines on the export of cyber-surveillance items, seeking to prevent the misuse of such technologies. Apart from Convention 108, several regional frameworks such as the African Union's Malabo Convention, Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines, Organization of American

States (OAS) Principles on Privacy and Personal Data Protection in the Americas, and the Association of Southeast Asian Nations (ASEAN) Framework on Personal Data Protection aim to regulate data protection and limit arbitrary surveillance practices. These frameworks emphasize state obligations to uphold the right to privacy and ensure that digital surveillance is conducted in accordance with human rights principles

6) Historical Background

6.1) Pegasus Case

Pegasus is spyware developed by the Israeli cyber-arms company NSO Group that is designed to be covertly and remotely installed on mobile phones running iOS and Android NSO Group developed its first iteration of Pegasus spyware in 2011. The company states that it provides "authorized governments with technology that helps them combat terror and crime." NSO Group has published sections of contracts which require customers to use its products only for criminal and national security investigations and has stated that it has an industry-leading approach to human rights. While NSO Group markets Pegasus as a product for fighting crime and terrorism, governments around the world have routinely used the spyware to surveil journalists, lawyers, political dissidents, and human rights activists.

The sale of Pegasus licenses to foreign governments must be approved by the Israeli Ministry of Defense. As of September 2023, Pegasus operators were able to remotely install the spyware on iOS versions through 16.6 using a zero-click exploit. While the capabilities of Pegasus may vary over time due to software updates, Pegasus is generally capable of reading text messages, call snooping, collecting passwords, location tracking, accessing the target device's microphone and camera, and harvesting information from apps. The spyware is named after Pegasus, the winged horse of Greek mythology. Cyber watchdog Citizen Lab

and Lookout Security published the first public technical analyses of Pegasus in August 2016 after they captured the spyware in a failed attempt to spy on the iPhone of a human rights activist. Subsequent investigations into Pegasus by Amnesty International, Citizen Lab, and others have garnered significant media attention, including in July 2021 with the release of the Pegasus Project investigation, which centered on a leaked list of 50,000 phone numbers reportedly selected for targeting by Pegasus customers. Citizen Lab and Lookout discovered that the link downloaded software to exploit three previously unknown and unpatched zero-day vulnerabilities in iOS. According to their analysis, the software can jailbreak an iPhone when a malicious URL is opened. The software installs itself and collects all communications and locations of targeted iPhones. The software can also collect Wi-Fi passwords.The researchers noticed that the software's code referenced an NSO Group product called "Pegasus" in leaked marketing materials. Pegasus had previously come to light in a leak of records from Hacking Team, which indicated the software had been supplied to the government of Panama in 2015.Citizen Lab and Lookout notified Apple's security team, which patched the flaws within ten days and released an update for iOS. A patch for macOS was released six days later.

6.2) Edward Joseph Snowden Case

Edward Joseph Snowden is a former National Security Agency (NSA) intelligence contractor and whistleblower who leaked classified documents revealing the existence of global surveillance programs. Born in 1983 in Elizabeth City, North Carolina, he attended a community college and later enrolled at a masters programme of the University of Liverpool without finishing it. In 2005 he worked for the University of Maryland, in 2006 he started working for the Central Intelligence Agency (CIA) and then switched to Dell in 2009 where

he was managing computer systems of the NSA. In 2013, he worked two months at Booz Allen Hamilton with the purpose of gathering more NSA documents. In May 2013, Snowden flew to Hong Kong and in early June he revealed thousands of classified NSA documents to journalists Glenn Greenwald, Laura Poitras, Barton Gellman, and Ewen MacAskill. His disclosures revealed numerous global surveillance programs, many run by the NSA and the Five Eyes intelligence alliance with the cooperation of telecommunication companies and European governments and prompted a cultural discussion about national security and individual privacy. Yet despite the fact that he broke the law, Snowden argued that he had a moral obligation to act. He gave a justification for his "whistleblowing" by stating that he had a duty "to inform the public as to that which is done in their name and that which is done against them." According to Snowden, the government's violation of privacy had to be exposed regardless of legality. Journalists were conflicted about the ethical implications of Snowden's actions. The editorial board of The New York Times stated, "He may have committed a crime…but he has done his country a great service."

On June 21, 2013, the United States Department of Justice unsealed charges against Snowden of two counts of violating the Espionage Act of 1917 and theft of government property, following which the Department of State revoked his passport. He stayed in Moscow's Sheremetyevo International Airport for a month, then was granted asylum in the country. He became naturalized as a citizen of Russia in 2022. In early 2016, Snowden became the president of the Freedom of the Press Foundation, a San Francisco–based nonprofit organization that aims to protect journalists from hacking and government surveillance. He also has a job at an unnamed Russian IT company. On September 17, 2019, his memoir *Permanent Record* was published. On September 2, 2020, a U.S. federal court ruled in *United States v. Moalin* that one of the U.S. intelligence's mass surveillance programs exposed by Snowden was illegal and possibly unconstitutional.

6.3) Mother of All Breaches Case

The term "Mother of All Breaches" (MOAB) refers to one of the largest known data compilations in history, includes records from thousands of meticulously compiled and reindexed leaks, breaches, and privately sold databases. Bob Dyachenko, cybersecurity researcher, together with the Cybernews team, has discovered billions upon billions of exposed records on an open instance. Even though at first the owner of the database was unknown, Leak-Lookup, a data breach search engine, said it was the holder of the leaked dataset. saying the problem behind the leak was a "firewall misconfiguration," which was fixed. According to the team, while the leaked dataset contains mostly information from past data breaches, it almost certainly holds new data that was not published before. The MOAB contains 26 billion records over 3,800 folders, with each folder corresponding to a separate data breach. While this doesn't mean that the difference between the two automatically translates to previously unpublished data, billions of new records point to a very high probability, the MOAB contains never seen before information.

Researchers believe that the owner of the MOAB has a vested interest in storing large amounts of data and, therefore, could be a malicious actor, data broker, or some service that works with large amounts of data.

"The dataset is extremely dangerous as threat actors could leverage the aggregated data for a wide range of attacks, including identity theft, sophisticated phishing schemes, targeted cyberattacks, and unauthorized access to personal and sensitive accounts," the researchers stated. The supermassive MOAB does not appear to be made up of newly stolen data only and is most likely the largest compilation of multiple breaches (COMB). While the team identified over 26 billion records, duplicates are also highly likely. However, the leaked data contains far more information than just credentials; most of the exposed data is sensitive and, therefore, valuable for malicious actors. A quick run through the data tree reveals an astoundingly large number of records compiled from previous breaches. The largest number of records, 1.4 billion, comes from Tencent QQ, a Chinese instant messaging app. However,

there are supposedly hundreds of millions of records from Weibo (504M), MySpace (360M), Twitter (281M), Deezer (258M), Linkedin (251M), , Adobe (153M), Canva (143M), VK (101M), Daily Motion (86M), Dropbox (69M), Telegram (41M), and many other companies and organizations. The leak also includes records of various government organizations in the US, Brazil, Germany, Philippines, Turkey, and other countries. According to the team, the consumer impact of the supermassive MOAB could be unprecedented. Since many people reuse usernames and passwords, malicious actors could embark on a tsunami of credential-stuffing attacks.

7) Fundamental Rights at Risk

A human rights violation is the disallowance of any of these basic rights and freedoms. When human rights aren't protected, or are blatantly disregarded, they are violated. Digital surveillance carries substantial risks to human rights, particularly in terms of privacy. Consequently, digital surveillance often affects a broader spectrum of internationally protected rights, the most notable of which include the following.

UDHR Article 12 -

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

ECHR Article 8 -

Everyone has the right to respect for his private and family life, his home and his correspondence.

ICCPR Article 17 -

No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

European Union Charter of Fundamental Rights Article

7- Everyone has the right to respect for his or her private and family life, home and communications

8. 1 - Everyone has the right to the protection of personal data concerning him or her

8) Questions to be Addressed

1) **What kind of agreements can be made that countries and companies can join?**
2) **How can digital surveillance by the private sector be controlled?**
3) **What sanctions can be imposed on those who exceed the limits of digital surveillance?**
4) **How can we improve digital surveillance systems in a positive way?**
5) **What kind of futuristic scenarios might occur if precautions are not taken?**

9) Bibliography

SURVEILLANCE AND HUMAN RIGHTS

https://www.echr.coe.int/documents/d/echr/convention_ENG

https://www.un.org/en/global-issues/human-rights?gad_source=1&gad_campaignid=20126487822&gbraid=0AAAAAD9kiAep725fghhYKEb_PX0ycbqFr&gclid=Cj0KCQjwn

ovFBhDnARIsAO4V7mA222YMtbaFkZq8kOPGmH6OUIQFlldX11E4jY2WDOEj5goQL12EGjUaAq9XEALw_wcB

https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

https://digitallibrary.un.org/record/4031525?v=pdf

https://docs.un.org/en/A/HRC/41/35

https://ghostarchive.org/archive/iTghC

Greengard, Samuel. "Pegasus (spyware)". Encyclopedia Britannica, 14 Aug. 2025, https://www.britannica.com/topic/Pegasus-spyware. Accessed 18 August 2025.