Research Report

Model United Nations Oud-Beijerland 2026

General Assembly 2 - ECOSOC

Addressing the question of digital surveillance and privacy rights

Rafael Roos & Max den Boer

Introduction

Digital surveillance means that governments or companies store and analyse personal data from online activity. Privacy is the right to keep your personal information private without other bodies collecting it. This right is protected by the law of the Universal Declaration of Human Rights (Article 12). Technology nowadays makes it possible to monitor millions of people with low effort and low costs. This often happens secretly. For example, some states say that this is necessary for security, while other critics say that it threatens rights such as freedom of expression and association. This is why the UN member states need to find new ways to protect privacy without ignoring security needs.

General Overview

In 2013, Edward Snowden revealed that the American National Security Agency, together with other countries such as the United Kingdom, was collecting huge amounts of internet and phone data; this data also contained information about people who weren't suspected of anything. This made people furious. The same year, a resolution was accepted on the matter, which states that the rights people have offline should also be protected online. However, these matters were not legally binding, which is to be seen as a lot of members are still gathering information online about their citizens.

Surveillance is not only done by governments. Private companies sell advanced spy technology to countries too. A good example is Pegasus, which is made by an Israeli company, NSO Group and can take over a phone without the owner clicking on anything. In 2021, an international investigation found that Pegasus had been used against journalists, human rights defenders and politicians in many countries. Because these tools are sold internationally and are hard to trace, it is difficult to find the perpetrator.

Governments say that surveillance helps to prevent terrorism and crime. This is a legitimate claim, but international law says that restrictions on privacy must be lawful, necessary and in line with international law. Collecting data about everyone is hard to defend under these criteria. Human rights groups also say that surveillance has a “chilling effect”: when people think they are being watched, they speak and organise less freely. Groups such as activists and journalists are affected by this the most.

Countries handle data protection differently. The European Union uses the General Data Protection Regulation (GDPR), which was adopted in 2018. This agreement gives people the right of privacy over their data and limits how companies can/may use it. For example, Brazil and several other countries have followed this model as well. China, on the other hand, uses facial recognition and online monitoring, which is presented as a “tool for public order”. In the United States, there is no single data privacy law. There are programs such as Section 702, which allow the collection of foreign communications, but this can also include data about American citizens. These differences in law make it difficult to make global rules on this topic. For example, data transfers between the EU and the US have been struck down by the European Court of Justice a lot of times.

Artificial intelligence, biometric data and smart cities increase the amount of data that can be collected by governments or companies. In 2024, the General Assembly adopted a convention on cybercrime which allows the collection of this data in some cases. Human rights organisations criticised it because it could be misused without strong regulations.

Major Parties Involved

- United States. The US runs some of the largest intelligence programs in the world and was at the centre of the Snowden revelations. It has taken steps to limit commercial espionage by its own government, and it has put the NSO Group (Pegasus) on a trade blacklist in 2021, but it still defends a lot of surveillance for national security.

- China. China has one of the most advanced digital monitoring systems in the world, which includes facial recognition and strict internet control; for example, they use a different browser to monitor their citizens' online actions better.

- Israel. Israel is home to NSO Group and other cyber surveillance companies. The government

says it controls the export of these tools that the companies produce, but investigations have shown that these products have been abused in other countries, which makes Israel an important party in this matter.

- OHCHR & UN Special Rapporteur on privacy. The Office of the UN High Commissioner for Human Rights promotes and monitors human rights worldwide and the Special Rapporteur was created to report on privacy violations. They publish reports and guidelines on the matter of privacy.

Possible Solutions

Clear rules for surveillance. Members could agree on minimum standards which weigh of the need for security and the right for privacy. Surveillance should have a legitimate goal and be limited to what is necessary. Independent companies should approve it in advance, and people should be informed afterwards if possible.

Controlling the spyware trade. The committee could call for a non-governmental body to oversee the export of spyware technology, and it should be able to ban countries when they have a record of abuse. Members could also be asked to carry out checks for Human rights organisations.

Strengthening the UN framework. The UN could ask the OHCHR to develop guidelines for members and to create a reporting system to be able to ban countries in case of misuse.