**Forum:** Human Rights Council

**Issue:** Addressing the violations of human rights to privacy caused by electronic surveillance

**Student Officers:** Natalie Tiller and Jean Daniel Kadadihi

**Position:** Chairs of Human Rights Council

---

## Introduction

Governmental departments and intelligence agencies are primarily responsible for the most widespread electronic surveillance. They hold the resources and capabilities to track large groups of people in or out of their country. The government also has the right and responsibility to respond to concerns about threats and attacks to protect its citizens. Many governments claim it is necessary to collect as much information as possible to keep their citizens safe from harm and track those who do certain actions that rebel against a government. One common government justification is for preventing "terrorism". In the last decade, it has been increasingly normal for government agencies to spy on citizens after many governments have had heightened concerns about terrorism after 9-11. Especially in this digital era, a significant increase in technology has made it more effortless.

The NSA created the Terrorist Surveillance Program to protect citizens; however, the program has detained people, resulting in serious human rights violations.

Innocent people are sent to prison with no trial and are interviewed by the FBI. Some cases even involve implemented disappearance, where the individual's whereabouts are entirely disguised. This unlawful detention leaves individuals at a heightened risk of torture or other inhuman acts prohibited under international law. Edward Snowden was able to leak information from NSA to the media in 2013. This event was only the start of many scandals where citizens found out the government had taken unauthorized information among them, which astounded the world. It exposed how the NSA could demand information about users from firms and their collection of civilian internet traffic. Instead of focusing on criminals, governments have increasingly turned their attention to everyone.

In 2016 the FBI revealed that they had hacked devices, which questions how trustworthy spy agencies are in reality. It's also essential to keep in mind that NSA holds the capability to turn on and activate microphones and cameras on devices without you noticing. Even facial recognition technology strives to capture and detect an individual's facial characteristics, profiling individuals based on their characteristics such as ethnicity, national origin, race, gender, and others, which are often the basis for unlawful discrimination. However, other groups will use the internet to track what people do besides governments. For instance, companies with large collections of data generate revenue for the company's benefit by providing other companies with individuals' browsing histories so ads can be targeted more accurately towards these tracked

people. These types of tracking techniques invade the privacy of internet users. In many states, some laws stipulate who can use surveillance techniques and how they can use them. Electronic surveillance laws are stringent as there are numerous ways they can be used to invade privacy. Electronic surveillance can be traced back to 1791 with the implementation of the bill of rights, the fourth amendment, which declares a right to be free from unreasonable searches.

However, there are a lot of improper uses for all this information, and the question often comes to mind. Does all of this tracking actually make us safer? When all this data is collected about people's personal lives, governments and other parties can use this information against a person. Governments are also using dangerous and sophisticated technology to read activists' and journalists' private messages and remotely turn on cameras/microphones on devices to secretly record their activities. Invading this privacy it's seen as an abuse of power. The need for individuals to keep certain parts of their lives private is essential; privacy amongst individuals continues to be violated anyways, even after laws were placed. Electronic surveillance is meant to keep citizens safe, but it does quite the opposite in many ways. It causes harm. Mass surveillance negatively affects human rights and freedoms, including freedom of assembly, freedom of expression, freedom of movement, as well as the principle of non-discrimination.

## Definition of Key Terms

### Electronic Surveillance

The monitoring of a home, business, or individual, usually secretive or unobtrusive, uses various devices such as cameras, microphones, tape recorders, wiretaps, and other electronic digital, and audio-visual means. It can also refer to surveillance done through a computer or mobile phone.

### Mass Surveillance

Mass surveillance systematically monitors people's lives through technology to monitor large groups of people instead of only surveilling individuals suspicious of crime.

### Terrorism

The threat of violence, especially against the state or the public, is a politically motivated means of attack or coercion.

### The Right to Privacy

An individual's legal right to privacy and freedom from unjustified publicity. An element of legal traditions intended to constrain government and other behaviors that endanger people's privacy.

### Freedom of Expression

The ability of an individual or a group of individuals to freely communicate their opinions, ideas, and views on various topics without fear of government censure.

### Principle of Non-Discrimination

The necessity for equal treatment amongst individuals even with their specific characteristics. The avoidance of discrimination.

### The Fourth-Amendment

One of the amendments to the United States "protects people from unreasonable searches and seizures by the government."

### The Digital Age

This period began in the late 1970s up until the present time, where increasingly advancing technology is being introduced, allowing us to store and transfer information quickly and freely on digital media.

### Internet Censorship

The control or suppression of what can be accessed, published, or viewed online. Governments or private organizations may carry it out at the behest of the government, regulators, or their initiative.

**The National Security Agency**

(NSA) a federal government intelligence agency part of the United States department of defense.

## General Overview

Privacy is a crucial human right protected by the UN and violations of privacy go unnoticed or generally ignored by governments for their benefit. Governments tend to track citizens and control what they see or do, violating their privacy. It is hidden by the excuse of national security but, in reality the private information of the average citizen is barely relevant to national security. In the USA the FISA amendment enables the US government to carefully track citizens' private online information without any sort of permission or warrant.

The spread and misuse of information by the government is concerning for humanity as sometimes information is used to favor a government or benefit them politically or economically. In North Korea, China, and Russia Electronic surveillance is implemented heavily and knowingly violates citizen human rights. There can even be criminal charges for slandering the government in private conversation. This extreme vigilation can lead to more human rights being violated such as freedom of speech.

The right to privacy is the right to be free from undue surveillance by the Government or anyone else. Surveillance by the State should only occur if absolutely necessary and where authorized by an independent judicial officer. Personal information should only be collected and kept by the State and anyone else for a legitimate purpose authorized by law. Once collected, personal information should be destroyed as soon as it is no longer required. Not only would this protect privacy, it would also improve security. If personal information is only collected when absolutely necessary, it is less likely to fall into the wrong hands. If it is destroyed when it is no longer required, it is less likely to become incorrect and out of date. Privacy laws have expanded in recent years, but are still fundamentally flawed. They lack uniformity, they fail to recognize a right to privacy, and they do not apply generally to individuals or small businesses. This means that private individuals and small businesses are largely unregulated when it comes to the collection and use of personal information about other people. The majority of democratic countries have recognized that privacy is a fundamental human right which needs to be protected. Article 17 of the ICCPR recognizes privacy as a basic human right, but Australia, despite being a signatory to the ICCPR, does not recognize privacy as an actionable human right.

**Rights to privacy**

An actionable right to privacy would enable individuals to take action against the inappropriate and illegal collection, use or disclosure of their personal

information. It would not prevent the lawful collection and use of personal information for legitimate purposes. The spread of new technologies such as CCTV and GPS presents new threats to privacy which have outpaced the law. It is futile to try to stop the spread of many of these technologies. However, the legal environment in which they spread should discourage the misuse of personal information. The most effective deterrent to the misuse of personal information would be a liability to compensate people whose privacy has been compromised for no legitimate purpose. The right to privacy is associated with the rights to freedom of speech, freedom of movement, freedom from discrimination and the principle of government accountability.

## Major Parties Involved and Their Views

### United States

**Most important agencies in the United States:**

Intelligence Agency - CIA

National Security Agency - NSA

Federal Bureau of Investigation - FBI

The constitution claims to protect people from unreasonable searches and seizures by the government through the fourth amendment. For years, the main idea was that the government would only intend to focus on criminals. However, a leaked and secret court order and other documents reveal that the National

Security Agency has been collecting phone records on millions of Americans for months at a time, spying on email communications with the knowledge of large internet providers, and collecting a vast catalog of Americans credit card transactions, going against their law. The US Intelligence System constitutes elaborate intelligence organizations, each with a specific role and a carefully defined area of expertise and responsibilities. The first is The Central Intelligence Agency, responsible for coordinating all the separate intelligence units. The biggest of the country's intelligence organizations is the National Security Agency. The NSA was exposed to also being responsible for code-breaking in the following years. The NSA focuses overseas rather than domestic, which means it focuses more on spying on foreign countries than the USA (international). The role of the CIA and the NSA has been questioned on numerous occasions due to numerous accusations of illegitimate interventions and support to authoritarian regimes. The FBI leans more towards domestic intelligence, while the CIA and NSA lean more towards international intelligence.

## United Kingdom

**Most important agencies in the United Kingdom:**

Governmental Communication Headquarters - GCHQ

(military intelligence) **MI5**

(military intelligence) **MI6**

GCHQ is the UK's official security and intelligence organization, working closely with the British Government and subject to Parliamentary and judicial control. It is a secret organization, and its existence was not officially admitted until 1983. MI (military intelligence) numbered agencies up to 19 at different times. Most were folded into MI5, MI6, or GCHQ after the war. MI5 deals with threats inside of the UK. It investigates national security matters in the UK, such as investigating terrorists. On the other hand, MI6 combats overseas threats (international) spying on other countries. British mass surveillance and intelligence-gathering practices breached the human rights laws. The European Court of Human Rights found some aspects of British surveillance activities violated provisions in the European Convention on Human Rights to safeguard Europeans' rights to privacy. The court stated that sufficient safeguards had been placed to protect against abuse of power and ensure that the UK authorities from foreign intelligence partners; however, some judges disagreed with this statement.

## Russia

**Most important agencies in Russia:**

Federal Security Service - FSB

FSB holds the responsibility for counterintelligence, antiterrorism, and military surveillance. It is exceptionally effective at counterintelligence and human rights

activists. President Putin has informed the National Security council Agency that Russia is not carrying out mass surveillance programs of the kind exposed in the US. When Russia was asked if they stored, intercepted, or analyzed the communication of millions of individuals. In response, Agencies are controlled by law. This means you have to get court permission to put a particular individual under surveillance. Russia does not have mass permission, and its regulations make it impossible for that kind of mass permission to exist. Russia has access to technical means to respond to terrorist nature, but not mass control; also, it is essential to notice that Russia has a deficient economy and doesn't have as much money as the united states.

## China

**Most important agencies in china:**

Ministry of state security- MSS

China holds accountability for having the world's largest surveillance network, deploying over half of the worldwide surveillance cameras. China's government claims the project aims to improve public safety and security; however, it's seen outside China as a means for more than state control. MSS is close to the old KGB holding responsibility for domestic and foreign security and espionage. The military technology of the United States and the high-tech industries are China's

main focus of overseas activities. Since 2007, the governments of Germany, Britain, and the USA have been making allegations against China for attempting to hack their respective department of defense databases. In China, the chances are incredibly high that everything you do is recorded and can be used against individuals. It focuses on the actions of individuals from a daily perspective by giving a score. If the government believes what you are doing is socially beneficial, the score will increase, and if not, the score will decrease. Low scores prohibit having access to travel, can affect families from doing certain things, and results in job loss. China is, therefore, constantly reviewing and analyzing citizens' use of the internet, perhaps having access to personal information that could be seen as breaking laws of privacy. China has major internet censorship and is constantly analyzing and reviewing citizens' use of the internet and having access to personal information, which can be seen as breaking laws on privacy.

## India

A few years ago in India, privacy was declared a fundamental right. However, in 2013, the government introduced electronic surveillance measures, which normalized the shift of only targeted surveillance and leaned more towards mass surveillance. The state of India uses various digital surveillance tools such as CCTVS and facial recognition cameras to track the actions of citizens as a mass.

India's notoriously secretive agency was founded in 1985 as an indispensable arm of the Indian government's strategy against Pakistan. The surveillance usage was more built upon threats from Pakistan. Since then, it has expanded into one of the most assertive intelligence agencies, with its activities expanding to Pakistan, Sri Lanka, Nepal, Bangladesh, and elsewhere. Its main objective remains the destabilization of Pakistan. To this end, it is particularly active in supporting independence movements in Bangladesh. In contrast, Pakistani authorities have also accused it of attacks in their country and infiltration by the U.S. and Chinese assets.

## Timeline of Events

| Date | Description of event |
|---|---|
| 1791 | In the United States, the Fourth Amendment was implemented, intended to protect people from unreasonable searches and seizures by the government. |
| 1952 | President Truan established the National Security Agency (NSA) with the mission to defeat terrorists as well as other organizations. |

| | |
|---|---|
| 2001 | In the wake of 9/11, Congress passed the Patriot Act, which changed the U.S government. |
| 2001 | NSA implemented the terrorist Surveillance program/an electronic surveillance program. |
| 2005 | Skynet, a mass surveillance system, was created by China (revealed in 2013). |
| 2007 | Launch of the US surveillance called PRISM. |
| April 2007 | China released an original version of Myspace, where any comments on political matters are banned. |
| 2013 | The Washington Post and the Guardian reveal a secret program named PRISM (launched in 2009) which allows NSA access to the personal data of millions of individuals through Facebook, Microsoft, Yahoo, and Google. |
| 2013 | Edward Snowden leaked classified information from the US NSA to the media. The government files surveillance charges against Edward Snowden, an NSA contractor, for the information leak. |

| | |
|---|---|
| December 2013 | For the first time, the UN files a report about privacy rights in the digital age. The report called for an end to electronic surveillance and expressed deep concern for the harm it caused by spying on foreign states and the mass collection of personal data and its negative impact on human rights. |

## UN involvement, Relevant Resolutions, Treaties and Events

The UN became active on this issue when most of the problems increased. OHCHR constantly takes action and looks over effective programs to protect human rights internationally. OHCHR has organized conferences and published reports to explore the challenges of dealing with the human right to privacy and other difficulties against human rights in the digital age. The latest report (Right to privacy in the digital age), released in 2021, focuses on the vast impacts of artificial intelligence (AI) usage. It specifies the urgent need for a temporary

prohibition of the use of AI systems until adequate safeguards are put in place as it can create a severe risk to human rights. The UN general embassy, through previous years, made other reports. In 2020 the report released discussed the issues of the violation of human rights due to various surveillance practices, which calls for a moratorium on the use of facial recognition technology. This report also calls for AI applications that cannot be used in compliance with international human rights laws to be banned.

The resolution made by Brazil and Germany in 2013 expressed deep concerns about the negative impact that interception of communications and surveillance may have on human rights. The general assembly believes that the rights held by people offline must be protected online and calls upon all states to protect and respect the privacy in digital communication. "calls on all States to review their procedures, practices, and legislation related to communications surveillance, interception, and collection of personal data and emphasizes the need for States to ensure the full and effective implementation of their obligations under international human rights law." Furthermore, previous panels have been made in the human rights committee on this issue.

**Relevant treaties, resolutions, and events that have occurred on this issue:**

- Universal Declaration of Human Rights, 10 December 1948
- Reform of the EU's 1995 data protection rules to strengthen online privacy rights, 25 January 2012

- The Right to privacy in the digital era resolution (initiated by Brazil & Germany, December 2013
- Developments in the field of information and telecommunications in the context of international security, 9 January 2014
- The impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests( 2020)
- The Right to Privacy in the Digital Age (2021) OHCHR

## Evaluation of Previous Attempts to Resolve the Issue

Outside the United Nations, there have been other attempts taking place. The Federal Bureau of Investigation (FBI) has also been taking the initiative by wanting to monitor emerging threats through social media so that they can quickly identify and track them. This can benefit citizens as it leads to their safety and well-being. Monitoring threats would include creating a new tab application to monitor Facebook, Twitter, and news reports. However, worries have come across that law enforcement will come into action, as a lack of freedom of speech is compromised. The Electronic Frontier Foundation (EFF) has long believed in the right to have a private conversation over a digital network. EFF is aware that protecting access to technology is essential to advancing

freedom for all and has tried its best to defend freedom of speech and fight illegal surveillance by fighting for years.

## Possible Solutions

- Reasonable suspicion: Governments could come to an agreement or implement privacy laws in which it is clearly stated that reasonable suspicion is required in order for private information to be used.
- Permission from the population—Government creates a treaty with people in which the population gives their full consent.
- Exceptions with serious events that threaten national security like terrorism
- Agreements with TNCs in order to limit surveillance—Work with companies like Instagram or Twitter in order to protect citizen private information to a reasonable extent.

This issue can make or break trust of populations to their governments. This relationship between politicians and citizens is crucial towards a transparent and satisfactory management of a nation. Issues like this have a possibility of getting easily ignored since armed conflicts and wars are future events; preemptive action is always harder to take place, as opposed to responsive action. This breach of privacy into the individual's personal life can affect them in many ways that can create discrimination by sharing and selling personal information that an individual might want to keep private.

## Sustainable Development Goal (SDG)

The sustainable development goal the issue relates to is goal number 10, Reduced Inequalities**.** The goal of this issue is to "*Reduce inequality within and among countries.*" In order for this sustainable goal to be achieved the unlawful electronic surveillance that is used against individuals to invade their privacy needs to be solved, or else the bigger picture that is this sustainable goal will never be achieved.

As said before, an example that is one of the roots of this discrimation that is created by electronic surveillance is the use of Facial recognition technology, which "strives to capture and detect an individual's facial characteristics, profiling individuals based on their characteristics such as ethnicity, national origin, race, gender, and others." These are often the basis for unlawful discrimination and therefore disrupts the equality that we as a society are trying to create. This invasion of privacy in the end damages our many forms of freedom, including freedom of assembly, freedom of expression, freedom of movement, as well as the principle of non-discrimination. So how can we really create true equality when these principles of freedom are put into harm? In the end, in order to create a society free of discrimation and inequality, the unlawful electric surveillance used to breach the private lives of individuals must be put to a stop.

## Bibliography

"Right to Privacy and Freedom from Surveillance." *Right to Privacy and Freedom from Surveillance | Liberty Victoria*, https://libertyvictoria.org.au/content/right-privacy-and-freedom-surveillance

AnnaFordyce, et al. "Privacy - Human Rights Case Summaries." *Human Rights Law Centre*, 16 Feb. 2021, https://www.hrlc.org.au/human-rights-case-summaries/tag/Privacy.

"Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis." *Health and Human Rights Journal*, 9 Dec. 2020, https://www.hhrjournal.org/2020/12/analyzing-the-human-rights-impact-of-increased-digital-public-health-surveillance-during-the-covid-19-crisis/.

field_visuel_grand_format. "A Constitutional View of Privacy Rights in China." *UIA*, 26 Nov. 2020, https://www.uianet.org/en/news/constitutional-view-privacy-rights-china.

## Appendix

I. Journalism under digital siege - video some impacts of digital surveillance on journalism and how it can censor and suppress voices.
II. *Legal constitutional analysis of China*- China's shakey privacy laws which are outweighed by the strength of the government.
III. USA electronic illegal surveillance- violation of privacy rights in mass surveillance by the US
IV. NSA acceptance monitoring by country- shows the percentage of

populations that would consent to being vigilated by governments.