General Assmebly 6 (GA6)

Developing legal frameworks for the ethical use of surveillance technology

Nimar Grover

Forum: General Assembly 6

Issue: Developing legal frameworks for the ethical use of surveillance technology

Name: Nimar Grover

Position: Main Chair

Introduction:

The ethical use of surveillance technology has been a growing matter of contention, particularly as advances in digital innovations allow for invasive monitoring, tracking, and data collection. While the technologies yield valuable benefits such as enhancing public safety, preventing crime, and supporting law enforcement officers, they also pose difficult ethical and legal challenges. Key concerns include the infringement on privacy rights, absence of transparency in how data is handled, and the ways in which mass surveillance may restrict freedom of movement and expression. Surveillance across most of the globe occurs with minimal oversight, and, as such, it is difficult to hold authorities accountable for abuse of power. Additionally, the use of artificial intelligence and facial recognition within surveillance adds new layers of complexity and brings with it the risk of discrimination and inaccurate profiling, especially of marginalized groups. As surveillance becomes more prevalent in public and private spaces, the need for concise and enforceable legal boundaries grows increasingly to prevent unethical use and ensure that fundamental human rights are not infringed upon. In this report, the development of legal frameworks for the ethical use of surveillance technology will be analysed and explained in the context of Sixth (Legal) Committee of the General Assembly.

Definition of key terms:

Digital authoritarianism

Digital authoritarianism refers to the government use of information technology for purposes of social control, oppression, surveillance or to otherwise reinforce their rule over their citizens or foreign populations.

Panopticism

Panopticism is a social theory that describes a mode of social control in which individuals begin to police themselves due to constant surveillance, thus shaping disciplined, docile and productive bodies.

Data protection

Data protection is the process of safeguarding sensitive data from corruption, misuse, exploitation or data loss.

Online Privacy

The definition of online privacy is the level of privacy protection an individual has while connected to the Internet. Risks to online privacy range from phishing scams to malware to problems with website security that may result in identity theft.

Private Surveillance

Private surveillance is the act of monitoring or observing individuals, groups or environments to gather information. Private security surveillance plays a crucial role in the protection and security of specific groups or individuals. However, there have also been studies on how private surveillance services may have serious human rights impacts.

Government Surveillance

A government's collection of information by ongoing observation of individuals or group, often justified by national security concerns. In the context of cybersecurity, the surveillance is generally conducted by observations of networks, information processing and communication systems.

Privacy Breach

A privacy breach, also referred to as a data leakage, refers to the unlawful and unauthorized exposure or disclosure of personal information. Surveillance technologies can often be seen as a breach of privacy if used unethically and the privacy of a customer not respected.

Mass surveillance

Mass surveillance is defined as the monitoring of or collection of information about an entire or a substantial fraction of a population, particularly by electronic means. It can be argued that by systematically monitoring people’s lives, mass surveillance enables the potential for unchecked state power and control over individuals.

Surveillance capitalism

Surveillance capitalism is a concept in political economics which denotes the widespread collection and commodification of personal data by corporations. It is the monetization of data

captured through monitoring people's movements and behaviours online and in the physical world.

General Overview:

This section aims to highlight the key concepts and features to fully understand the issue of developing legal frameworks the ethical use of surveillance technology.

The History and Initial Stages of Surveillance Technology

Although they exist in a more archaic form, the roots of surveillance technology predate many of the technologies we use today. In the past, surveillance was handled by humans. It was much simpler to track when one person could keep an eye on others from a distance. For example, the numerous spies that allowed states to monitor everything during times of conflict or the secret police of ancient empires. On the other hand, the origins of contemporary surveillance technology can be traced back to the first half of the 20th century, particularly during the world wars, when military intelligence was greatly aided by radio interception, aerial reconnaissance, and code breaking.

Surveillance technologies advanced drastically during the Cold War era, particularly with the emergence of satellite imaging, wiretapping, and secret electronic monitoring. National intelligence services primarily used these tools to monitor internal dissension and foreign powers. These technologies, however, were costly, only available to state actors, and received little public scrutiny. There was little international discussion of the ethical issues surrounding these tools, which were mostly limited to scholarly and legal circles.

The development of digital infrastructure in the latter half of the 20th century marked the beginning of the transition to mass surveillance. Large volumes of personal data could be gathered, stored, and examined at previously unheard-of scales due to the development of personal computers, internet connectivity, and mobile communications. Governments were no longer the only ones conducting surveillance; businesses, service providers, and private organizations started gathering user data for profit, creating difficult moral and ethical dilemmas.

Expansion and Globalization of Surveillance Practices

The reach of surveillance technologies grew along with the globalization of digital networks. The capacity to collect data has now grown exponentially in the twenty-first century. For example, State-led surveillance increased dramatically after the 9/11 terrorist attacks in the United States. Governments all over the world have increased their power to monitor digital activity, intercept

communications, and gather biometric information under the guise of national security. Legal frameworks for these operations were established by laws like the UK's Investigatory Powers Act and the USA PATRIOT Act, frequently with insufficient checks and balances.

At the same time, the technological sophistication of the surveillance tools advanced quickly. Surveillance has transformed into predictive monitoring due to significant developments in artificial intelligence, facial recognition, geolocation tracking, and algorithmic profiling. These technologies are now integrated into public areas, immigration control, law enforcement, and even the healthcare and education systems in many nations.

Additionally, a sophisticated worldwide market for surveillance equipment was created during this time. Powerful surveillance hardware and software are now designed, manufactured, and sold by private companies to both authoritarian and democratic governments. Such technologies' international sale has sparked worries about potential abuse, particularly when they are sent to countries with a track record of violating human rights. Businesses can also now function with little accountability due to the absence of international regulation, frequently avoiding ethical review procedures.

The distinction between corporate and state surveillance has also become blurrier in this digital age. User data is regularly gathered, stored, and made profitable by social media platforms, search engines, or e-commerce websites. While these practices are often justified under terms of service or user consent, many argue that such data collection constitutes a form of indirect surveillance that remains insufficiently regulated.

Ethical Dilemmas and Human Rights Implications

The development of increasingly complex surveillance systems has sparked intense ethical discussion. The conflict between privacy and security is at the heart of these issues. Governments frequently defend surveillance as a way to uphold law and order, prevent terrorism, and safeguard national security. These arguments, according to critics, can easily result in overreach, which would violate people's rights and undermine democratic values.

Consent is one of the most important ethical dilemmas. People are frequently unaware that they are being watched, especially when it comes to passive online data collection or public areas. The rights to privacy, freedom of speech, and immunity from arbitrary interference which are all guaranteed by international human rights frameworks such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights are called into question by this.

Bias and discrimination are also serious issues. It has been demonstrated that surveillance technologies, especially those that use AI algorithms and facial recognition, generate biased results based on age, gender, and race. As a result, marginalized communities may be disproportionately targeted, which would exacerbate already existing social injustices and contribute to systemic change.

The use and storage of gathered data raises additional ethical concerns. There is a chance of abuse, hacking, or unapproved sharing if there are unclear restrictions on data access and retention. Ensuring transparency and accountability is made more difficult by the opaque nature of many surveillance programs, particularly those run by private contractors or intelligence agencies.

Key Events Timeline

June 19, 1948	An early basis for upcoming ethical discussions regarding surveillance is laid when the United Nations General Assembly adopts the Universal Declaration of Human Rights (UDHR), establishing Article 12 that upholds the right to privacy.
October 24, 1949	Modern intelligence surveillance infrastructure in the West began with the full establishment of the Central Intelligence Agency (CIA) during the Cold War.
May 20, 1960	Closed-circuit television (CCTV) systems are used for the first time in recorded history, increasing the scope of physical surveillance in urban settings.
October 26, 2001	Following the 9/11 attacks, the USA PATRIOT Act was passed in the US, greatly extending both domestic and foreign surveillance capabilities under the pretext of counterterrorism.
March 11, 2004	Following the Madrid train bombings, Europe enacts a flurry of anti-terrorism and surveillance laws that increase regulation of public areas and digital communications.
June 5, 2013	Edward Snowden releases classified NSA documents revealing extensive

	worldwide monitoring activities and igniting a global dialogue on ethics, privacy, and supervision.
April 14, 2016	One of the most extensive digital privacy frameworks in the world, the General Data Protection Regulation (GDPR) is formally adopted by the European Union.
December 18, 2018	Resolution 73/179, adopted by the UN General Assembly, calls for the responsible use of digital surveillance tools while reaffirming the right to privacy in the digital age.
March 2020	In response to the COVID-19 pandemic, governments worldwide start utilizing digital surveillance tools like biometric scanning and contact tracing applications.
July 18, 2021	According to the Pegasus Project investigation, Israeli NSO Group spyware was used to surveil politicians, journalists, and activists around the world without their consent.
September 22, 2021	A report outlining the risks of AI-based surveillance systems and the necessity of international regulatory frameworks is released by the UN Human Rights Council.
October 31, 2022	Resolution 77/211, passed by the UN General Assembly, highlights the pressing need to uphold the right to privacy in light of modern surveillance technologies.
February 15, 2023	The Digital Rights Policy Framework, which provides moral standards for surveillance methods throughout the continent, is introduced by the African Union.
June 2023	Citing threats to civil liberties and discrimination, France and Italy introduce national restrictions on the use of facial recognition technology.
August 2024	Unauthorized use of cross-border AI surveillance networks is revealed by

new whistleblower leaks, which have sparked international outrage and a renewed regulatory discussion.

Principal Stakeholders

Nigeria:

Nigeria is Africa's most populous country and a regional leader in digital policy and security. However, it has a lack of strong data protection laws, potential for political misuse, surveillance of journalists and activists. Nigeria has been revealed as Africa's largest customer of surveillance technology contracts, spending hundreds of millions of dollars annually, and at least US$2.7bn on known contracts between 2013–2022. The surveillance technology has been used to spy on peaceful activists, opposition politicians, and journalists, singling them out for harassment, arrest and torture, in violation of international human rights law and supplier companies' own self-policing measures.

United States of America (USA):

USA is one of the global leaders in developing surveillance software and hardware. The practice of mass surveillance in the United States dates back to wartime monitoring and censorship of international communications from, to, or which passed through the United States. Following the September 11th attacks in 2001, local and international mass surveillance capabilities grew immensely. Mass surveillance tactics are also cited as responsible for profiling Hispanic Americans and contributing to the so-called "self-deportation". The FBI has also developed numerous software for the purpose of wiretapping telephone calls, internet communications, usage of smartphones, etc.

Singapore:

Over the past decade, the Singaporean government has geared up its surveillance capabilities by using cutting-edge technology to monitor civilians. There are more than 90,000 police cameras (PolCams) island wide, and the Singapore Police Force (SPF) plans to install more than 200,000 by the mid-2030s, including upgrading current ones with better features. It is important to note that the Constitution of the Republic of Singapore does not include a right to privacy of its citizens. In addition, because of various pieces of legislation including the Criminal Procedure Code (amended in 2012) and the Computer Misuse and Cybersecurity Act (amended in 1997), the Government does not need prior judicial authorisation to conduct any surveillance interception (Goh, 2015).

Russia:

Russian-backed companies have been rumoured to have provided sophisticated surveillance technologies to several Latin American countries. There are over 1 million video surveillance cameras in Russia. One in three is connected to a facial recognition system, according to data from Russian Minister for Digital Development Maksut Shadayev. The Grand Chamber of the European Court of Human Rights has unanimously held that the Russian system of secret interception of mobile telephone communications was a violation of article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms. Over the last decade, Russia's approach has grown to include more restrictive laws, advanced surveillance capabilities, and new regulatory mechanisms.

China:

China leads the world with over 200 million CCTV cameras. Its extensive surveillance network covers cities, streets, and public spaces. These cameras act as a deterrent, discouraging potential criminal activities. Mass surveillance in the People's Republic of China (PRC) is the network of monitoring systems used by the Chinese central government to monitor Chinese citizens. It is primarily conducted through the government, although corporate surveillance in connection with the Chinese government has been reported to occur. The Chinese government has also been reported to have increasingly employed advanced technology to amplify its repression of religious and faith communities.

Iran:

Iran is becoming more and more reliant on surveillance technology to support hijab enforcement in society. New repressive policies in Iran involve the increased use of technology and surveillance, including through State-sponsored vigilantism, that further infringe upon women and girls' fundamental rights. Among the efforts include Iranian officials deploying "aerial drone surveillance" to monitor women in public places. Surveillance cameras on Iran's major roadways also are believed to be involved in searching for uncovered women. UN investigators said they obtained the "Nazer" mobile phone app offered by Iranian police, which allows the public to report on uncovered women in vehicles, including ambulances, buses, metro cars and taxis. (Keaton J. et Gambrell J., 2025)

Potential Avenues for Resolution

The most effective way to address the ethical concerns raised by surveillance technology is to establish global legal frameworks that clearly define where it can be employed. Such guidelines could give world standards on issues such as the proportionality and necessity for surveillance,

consent-based data collection, facial recognition limits, and the safeguarding of vulnerable groups.

Member states can also work on the establishment of autonomous monitoring institutions or regulatory authorities governing the use of surveillance technology. These could be present both at state and international levels, ensuring observance of ethical standards and scrutiny of potential abuses.

It is also important to consider developing nations without direct access to advancing technologies. The implementation of UN-led programs could allow these developing nations to understand how to use surveillance technologies in their country effectively and ethically. These would also ensure developing nations are not behind schedule or forced to adopt technologies without legal safeguards in place to protect human rights.

Periodic multilateral forums could be suggested by delegates for governments, technology companies, academic researchers, and civil society organizations to discuss and refresh ethical guidelines as technology evolves. These can also encourage responsible innovation and trade in surveillance technologies and ensure that private companies are answerable to international standards.

Therefore, all solutions must balance between promoting safety and safeguarding civil rights. All solutions need to be rooted in current human rights mechanisms and be respectful of the United Nations' responsibility to protect freedom, dignity, and privacy everywhere.

References

Bermudez, Krystal. “Iran Utilizing Surveillance Technology to Support Hijab Enforcement.” FDD, 14 Mar. 2025, www.fdd.org/analysis/2025/03/14/iran-utilizing-surveillance-technology-to-support-hijab-enforcement/.

“Cybersecurity Terms | CyberWire.” N2K CyberWire, 2024, https://thecyberwire.com/glossary/government-surveillance

Goh, Gabey. “Singapore Is Using Spyware, and Its Citizens Can’t Complain.” Digital News Asia, 2 Aug. 2015, www.digitalnewsasia.com/digital-economy/singapore-is-using-spyware-and-its-citizens-cant-complain.

https://www.uscirf.gov/user/41. “Religious Freedom in China’s High-Tech Surveillance State.” USCIRF, 2023, www.uscirf.gov/countries/china/religious-freedom-chinas-high-tech-surveillance-state

“Iran: Government Continues Systematic Repression and Escalates Surveillance to Crush Dissent in the Aftermath of Protests, UN Fact-Finding Mission Says.” OHCHR, 2025, www.ohchr.org/en/press-releases/2025/03/iran-government-continues-systematic-repression-and-escalates-surveillance.

Mantellassi, Federico. “GCSP Publication | Digital Authoritarianism: How Digital Technologies Can Empower Authoritarianism and Weaken Democracy.” Www.gcsp.ch, 16 Feb. 2023, www.gcsp.ch/publications/digital-authoritarianism-how-digital-technologies-can-empower-authoritarianism-and.

“Obama Quietly Extends Post-9/11 State of National Emergency.” MSNBC.com, www.msnbc.com/all/obama-quietly-extends-post-911-state-msna156916.

“Russia: How the Kremlin Is Using AI to Enhance Video Surveillance.” Eurasianet, 2024, https://eurasianet.org/russia-how-the-kremlin-is-using-ai-to-enhance-video-surveillance

Terzyan, Aram. “Russia’s Cyber Crackdown: Sovereignty, Surveillance, and Wartime Control.” Modern Diplomacy, 20 Sept. 2024, https://moderndiplomacy.eu/2024/09/20/russias-cyber-crackdown-sovereignty-surveillance-and-wartime-control/

“UN Report Says Iran Stepping up Electronic Surveillance of Women to Enforce Hijab Laws.” Timesofisrael.com, 2025, www.timesofisrael.com/un-report-says-iran-stepping-up-electronic-surveillance-of-women-to-enforce-hijab-laws/

Universal Periodic Review Stakeholder Report: 24th Session, Singapore the Right to Privacy in Singapore Submitted by Privacy International. https://privacyinternational.org/sites/default/files/2017-12/Singapore_UPR_PI_submission_FINAL.pdf

“What Is the Definition of Online Privacy? | Winston & Strawn Legal Glossary.” Winston & Strawn - What Is the Definition of Online Privacy? | Winston & Strawn Legal Glossary, www.winston.com/en/legal-glossary/online-privacy