

Forum: Legal Committee (GA6)

Issue: Establishing international legal frameworks regulating state surveillance and the protection of digital privacy

Student Officer: Vasilis Fragkos

Position:

Co-Chair

TOPIC INTRODUCTION

Due to the rapid technological advancements of the last few decades, surveillance has transformed. In the past, it referred mostly to targeted monitoring. In the modern era, however, it has shifted to a larger scale. Advancements in the technological sector have allowed governments to constantly collect and analyse mass amounts of personal information of everyday citizens; an action that is often challenged as unprecedented and a violation of law.

More specifically, governments, under the pretext of national security, crime prevention, counterterrorism, and cybercrime, increasingly employ digital surveillance tools. It is those acts that trigger concerns regarding multiple violations of fundamental human rights, with prime examples being those of freedom of speech and privacy.

This issue highlights multiple challenges that, even though they must, are yet to be resolved: The existing international laws are outdated, thus not limiting many modern technologies. The constantly emerging technologies create new challenges for regulation, which are yet to be resolved. Additionally, surveillance can become unlawful and disproportionate, as warned and (to a limited extent) has been proven by human rights organizations. That occurs when said acts are conducted without judicial warrants, clear statutory limits, and, of course, respect for constitutional rights; when the scale and intensity of data collection far exceed what is strictly necessary to address a specific threat.

It's common for states to have different views and opinions on state surveillance and its regulation, making it challenging for regulatory frameworks to be approved and adopted by member states. Moreover, due to the current absence of a common standard, tensions between security interests and individual freedoms can often arise.

It is of utmost importance that, as the Legal Committee, we attempt to battle this challenging issue. Collaborate and unite under the principles of the United Nations to set regulatory frameworks, bring international law up to a favourable standard, and overall ensure the protection of the digital privacy of all citizens in the world.

DEFINITION OF KEY-TERMS

State Surveillance

State surveillance refers to the systemic monitoring of individuals or populations by government agencies. It is most often conducted using tools such as camera equipment and communication intercepts, intending to manage security or control behaviour. ¹

Digital Privacy

“Digital privacy is the ability of an individual to control and protect the access and use of their personal information as and when they access the internet.” ²

Mass Surveillance

“Mass surveillance refers to the practice of collecting and monitoring vast amounts of data and information on individuals within a society, often without their knowledge or consent, with the aim of maintaining security and preventing threats.” ³

Metadata

Metadata refers to the data that provides information on other data. ⁴

Spyware

“Spyware is one type of malicious software (malware) that collects information from a computing system without your consent. Spyware can capture keystrokes, screenshots, authentication credentials, personal email addresses, web form data, internet usage habits, and other personal information.” ⁵

¹ House of Lords - Surveillance: Citizens and the State - Constitution Committee, publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1804.htm.

² “Digital Privacy Definition: What Is Digital Privacy & Digital Safety.” *Enzuzoprivacy*, 2026, <https://www.enzuzo.com/blog/digital-privacy-definition>.

³ Sumner, Stuart. “The Snowden Revelations.” *You: For Sale*, Elsevier, 2016, pp. 17–48, <https://doi.org/10.1016/b978-0-12-803405-7.00002-3>.

⁴ Cyberhaven, “What Is Metadata? Definition, Types, and Security Risks,” <https://www.cyberhaven.com/infosec-essentials/metadata>

⁵ Moeller, Robert. “Spyware.” *Afterimage: The Journal of Media Arts and Cultural Criticism*, vol. 38, no. 1, July 2010, pp. 34–34, <https://doi.org/10.1525/aft.2010.38.1.34>

Biometric Data

“Biometric data is a type of personal information that can be used to uniquely identify an individual, and is usually collected as a part of a digital identity verification process.” ⁶

Zero-Click Exploits

“Zero-click exploits are cyberattacks that compromise devices without user interaction, exploiting software or hardware vulnerabilities to gain unauthorized access.” ⁷

Predictive Policing

“Predictive policing is a method that employs advanced algorithms and artificial intelligence (AI) to forecast potential criminal activities, allowing law enforcement to allocate resources more efficiently and proactively address crime.” ⁸

Encryption Backdoors

“An encryption backdoor permits an invisible entry or a hidden pathway that lets illegitimate intruders bypass cryptography security protection. Essentially, they assist third parties like government agencies or law enforcement in gaining access to encrypted data without having to go through the normal decryption process.” ⁹

Digital Sovereignty

“Digital sovereignty is the capacity to control your digital destiny: your infrastructure, software, standards and data, including how they are governed and under which jurisdiction they operate.” ¹⁰

⁶ “Biometric Data - Definition, FAQs - Innovatrics.” *Innovatrics*, 5 Mar. 2021, <https://www.innovatrics.com/glossary/biometric-data/>.

⁷ Tasho Tashev. “What Is a Zero Click Exploit?” *Webopedia*, 27 Feb. 2025, <https://www.webopedia.com/technology/what-is-a-zero-click-exploit/>.

⁸ “Predictive Policing | Social Sciences and Humanities | Research Starters | EBSCO Research.” *Ebsco*, 2021, <https://www.ebsco.com/research-starters/social-sciences-and-humanities/predictive-policing>.

⁹ Austin. “What Is an Encryption Backdoor?” *Global Brands Magazine*, 19 Feb. 2025, <https://www.globalbrandsmagazine.com/what-is-an-encryption-backdoor/>.

¹⁰ Jimenez Egido, Irene. “What Is Digital Sovereignty and Why Does It Matter?” *Uncover IE*, 2 Jan. 2026, <https://www.ie.edu/uncover-ie/digital-sovereignty-master-in-public-policy/>.

Facial Recognition Technology (FRT)

“Facial recognition technology (FRT) in surveillance is a biometric identification system that matches facial features captured through digital cameras or CCTV with images stored in databases to identify individuals. This technology is increasingly utilized by law enforcement and security agencies to enhance public safety, particularly in high-risk areas such as airports and urban centers.” ¹¹

BACKGROUND INFORMATION

Historical Development of Surveillance

Traditional surveillance practices

Traditional surveillance practices usually consisted of basic interception and decoding of mail, as well as telephones (commonly known as wiretapping). Another known surveillance practice is that of covert monitoring. This consists of spies and agents usually conducting undercover operations. It was mostly conducted throughout the Cold War.

It's important to note that at the time, surveillance was generally targeted. It was also heavily limited by the technological capabilities of the time, as technological means supporting such operations were yet to be produced.

Expansion after the 9/11 attacks

On September 11th, 2001, a terrorist attack took place in the United States of America. The Twin Towers and the Pentagon building were hit and partially destroyed by an attack orchestrated by the terrorist organization “Al-Qaeda”. ¹²

Following those devastating events, counterterrorism became a primary security priority. That goes in contrast to times before, when it was often neglected and overlooked as unnecessary.

¹¹ “Facial Recognition Technology in Surveillance | Computer Science | Research Starters | EBSCO Research.” *Ebsco*, 2023, <https://www.ebsco.com/research-starters/computer-science/facial-recognition-technology-surveillance>.

¹² Britannica, "September 11 attacks," <https://www.britannica.com/event/September-11-attacks>

A primary example is the USA Patriot Act, which granted intelligence agencies far broader collection powers.¹³ expanded surveillance authorities. Intelligence agencies also acquired broader powers, allowing them to further conduct state surveillance with greater ease.

An additional aspect is that of international cooperation on information-sharing, which increased considerably. An act keen to evolve from state surveillance practices and become more transparent.

From that point on, Governments increasingly justified surveillance as a necessary act to maintain national security. A justification that would be challenged in the following years as a way for states to justify acts that would otherwise be deemed illegal.

The transition to the digital age

Observing the global transition to the digital age, it is evident that the widespread use of the Internet played a key role in the transformation of communications. Through smartphones and social media, enormous amounts of personal data were created, which could be intercepted and used in a malicious way.

Additionally, innovative cloud computing allowed for information to be stored across borders. This, of course, further empowered acts of state surveillance.

Ultimately, surveillance shifted as large-scale data collection became the norm for state surveillance, instead of more targeted monitoring practices, as was the case in the past.

Human Rights Dimensions

Privacy as a fundamental right

Privacy is not a conditional privilege or a temporary freedom granted by the state. As stated by the United Nations, it is an inherent human right. This standard is explicitly codified in Article 12¹⁴ of the Universal Declaration of Human Rights and Article 17¹⁵ of the International Covenant on Civil and Political Rights; they both prohibit arbitrary interference with personal lives, homes, and correspondence.

¹³ Britannica, "USA PATRIOT Act," <https://www.britannica.com/topic/USA-PATRIOT-Act>

¹⁴ United Nations. (1948, December 10). *Universal declaration of human rights*. United Nations. <https://www.un.org/en/about-us/universal-declaration-of-human-rights>

¹⁵ United Nations. (1966, December 16). *International Covenant on civil and political rights*. United Nations. Ohchr. <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>

Treating privacy strictly as an inalienable right rather than a policy preference sets a firm legal boundary: governments cannot routinely dismantle individual protections whenever security demands arise. That is a fundamental right set to protect the privacy of countless civilians; it must not be undermined.

Impact on freedom of expression

The impact of state surveillance on citizens' freedom of expression is very much present. Many times, individuals may engage in self-censorship: limiting their online searches, challenging their associations, and more.¹⁶ The fear is real, and it may dictate the actions of citizens that should've been protected by governments and resolutions whose aim is on preserving their rights.

Journalists face greater risks as they endanger themselves by uncovering and publicizing evidence of malicious acts.¹⁷ Through state surveillance, the perpetrators of the said malicious acts can become aware of the leak and break the law so as to preserve their public image and not face legal action.

Lastly, surveillance can discourage criticism of governments. When an individual wishes to publicly state their personal opinion/criticism, they shall be free to do so without the fear of repercussions. In a nation where the Government conducts state surveillance, the individual is afraid that such surveillance can be used against them; to suppress negative criticism. In such cases, the fundamental right of freedom of speech is suppressed.

Freedom of association and assembly

NGOs, human rights watchdogs, and legal advocacy groups are frequently subjected to targeted state surveillance.¹⁸ This hinders their ability to function without the fear of the state interfering, thus putting their life and freedom at risk. State surveillance also compromises their operational security; it exposes confidential informants or vulnerable victims.

It's not difficult to comprehend the suppression of political participation that also arises from state surveillance. When citizens suspect their political ties, event attendance, or campaign contributions are tracked, they are far more likely to withdraw from public life. People avoid joining

¹⁶ Penney, J. "Chilling Effects: Online Surveillance and Wikipedia Use," SSRN (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645

¹⁷ Committee to Protect Journalists, "Spyware and Press Freedom," <https://cpj.org/spyware/>

¹⁸ Amnesty International, "Demand an end to the targeted surveillance of Human Rights Defenders," <https://www.amnesty.org/en/petition/targeted-surveillance-human-rights-defenders/>

political parties, signing petitions, or endorsing policy reform out of concern that state records could be used against them later.¹⁹

The deployment of digital tracking tools, (eg. facial recognition at rallies, social media monitoring) dismantles most public demonstrations before they even begin. As a result, activists and ordinary citizens grow hesitant to organize or attend peaceable assemblies when participation carries direct risks of preemptive arrest or harassment.

In non-democratic regimes, these risks become acute. That's because legal frameworks offer no genuine checks and balances. Authoritarian governments leverage surveillance technologies to systematically dismantle opposition networks.²⁰ That is, of course, given that they operate unchecked by independent judiciaries or a free press, and so without fear of institutional accountability or public oversight.

Security Interests and State Justifications

Counterterrorism measures

A crucial security interest is the prevention of imminent terrorist attacks. Surveillance systems allow intelligence agencies to intercept communications. They also allow them to identify operational plots early, and to intervene before violence occurs. That single act, preemption, is consistently cited as the primary moral and practical justification in cases where the state monitors communications networks.

A counterterrorism measure worth taking into consideration is cross-border intelligence sharing. Modern counterterrorism relies on international information-sharing agreements between allied nations.²¹ Acts of state surveillance enable the governments to pool data on suspects. It also allows for travel patterns to be recognized, so emerging threats across borders do not go unnoticed.

The detection and apprehension of extremist networks is another keen counterterrorism measure conducted through state surveillance. Monitoring messaging platforms and financial transfers helps the authorities map out complex terror cells and track recruitment pipelines. Ultimately, that leads to the arrest of operatives before they execute attacks.

¹⁹ Freedom House, "Freedom on the Net," <https://freedomhouse.org/report/freedom-net>

²⁰ Freedom House, "Persistent Authoritarian Repression and Backsliding in Democracies Drive 15th Consecutive Year of Decline in Global Internet Freedom," <https://freedomhouse.org/article/new-report-persistent-authoritarian-repression-and-backsliding-democracies-drive-15th>

²¹ Britannica, "Five Eyes," <https://www.britannica.com/topic/Five-Eyes>

Lastly, the "saving lives" narrative. Public officials routinely frame surveillance as a necessary trade-off between individual privacy and collective security. They constantly argue that data collection directly saves lives and preserves state stability.

Combating serious crime

Dismantling organized criminal networks is keen in combating serious crime. Transnational crime rings rely on covert communication channels to coordinate operations. Surveillance tools allow law enforcement to identify the leadership structures and track the movements of syndicates and their personnel. All with the goal of criminal prosecutions and, of course, upholding security within the nations.

Disrupting human and drug trafficking is another front where state surveillance becomes almost essential. Cartels and trafficking syndicates move victims and illegal contraband through complex international routes.²² It is by intercepting location data, logistics calls, and financial records that the authorities locate victims and shut down supply lines.²³

Worthy of mention is investigating advanced cybercrime. In the last couple of years, illicit activities have shifted to dark web marketplaces and encrypted platforms; digital surveillance and network forensics are vital for unmasking anonymous operators and gathering electronic evidence.²⁴

Lastly, tracking money laundering activities. It's known that in the so-called "underworld", criminal enterprises obscure illicit funds through complex chains of international banking transfers. Automated financial monitoring and database integration allow agencies to flag suspicious transactions and freeze assets.²⁵

²² UNODC, "Using the Power of Technology to Help Victims of Human Trafficking," <https://www.unodc.org/unodc/frontpage/2022/July/using-the-power-of-technology-to-help-victims-of-human-trafficking.html>

²³ UNODC, "Behind the screen: how cyber investigations fight human trafficking," https://www.unodc.org/unodc/en/frontpage/2026/February/behind-the-screen_-how-cyber-investigations-fight-human-trafficking.html

²⁴ Europol, "Internet Organised Crime Threat Assessment (IOCTA)," <https://www.europol.europa.eu/publications-events/main-reports/iocta-report>

²⁵ U.S. Department of the Treasury, "Financial Action Task Force (FATF)," <https://home.treasury.gov/about/offices/terrorism-and-financial-intelligence/terrorist-financing-and-financial-crimes/financial-action-task-force-fatf>

Cybersecurity concerns

One of the most common cybersecurity concerns is the protection of critical national infrastructure. Power grids, water systems, transport hubs, healthcare networks, and much more critical infrastructure rely on connected digital systems.²⁶ Network traffic monitoring helps state actors detect unauthorized access attempts. That, of course, protects essential public services from paralysis; an event that, as seen in previous cases of such a nature, can even endanger the lives of citizens.

Defending against state-sponsored cyberattacks is another critical concern, where state surveillance is necessary. Foreign military and intelligence agencies deploy offensive cyber tools to disrupt defense systems or steal sensitive government data. Continuous network oversight allows defensive teams to detect intrusions. Thus, the state can counter state espionage and minimize the risk of (future) attacks.

Lastly, responding to systemic digital dependence. Over the last couple of years, the trend of government functions and national economies moving fully online continues to grow. Essentially, that means that national security becomes tied to data security. States argue that monitoring digital traffic is necessary to safeguard state servers and maintain social order.

Challenges Facing Existing Legal Frameworks

Diverging national approaches

A critical challenge is the variability in privacy definitions. We must comprehend that nations interpret privacy in fundamentally different ways. Some view it as an inalienable human right. Others treat it as a secondary consumer protection; and some treat state authority as paramount over individual liberties.

Conflicting national security priorities are yet another issue that challenges the existing frameworks. Local threat environments and geopolitical alliances cause states to weigh security concerns against civil liberties differently. Ultimately, that prevents any universal consensus on acceptable monitoring limits. The friction between legal systems must also be recognized as a challenge. Divergent legal traditions (eg. civil law vs. common law, democratic vs. authoritarian regimes) make cross-border legal requests, extradition, and joint oversight slow and chaotic.²⁷ Lastly, the prioritization of national sovereignty, which often interferes with measures taken to resolve issues of State Surveillance. More specifically, many governments explicitly reject

²⁶ CISA, "Secure Critical Infrastructure," <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/secure-critical-infrastructure>

²⁷ Congressional Research Service, "Cross-Border Data Sharing Under the CLOUD Act," <https://www.congress.gov/crs-product/R45173>

international human rights standards or treaties. They do so by claiming that domestic surveillance practices fall strictly under sovereign defense authority and are immune to outside interference.

MAJOR COUNTRIES AND ORGANIZATIONS INVOLVED

The United States of America (USA) ²⁸

The United States' National Security Agency (NSA) operates large-scale intelligence programmes that became globally known after the Edward Snowden disclosures in 2013.²⁹ Legal frameworks (national frameworks) such as the Foreign Intelligence Surveillance Act (FISA)³⁰ allow for structured but controversial state access to digital communications. Looking over the nation's broader stance, the country generally defends surveillance. It sees it as a necessary tool both for counterterrorism and cybersecurity. It does recognize associated risks regarding acts of State Surveillance (when conducted with malicious intent); however, it prioritizes the positive benefits of broader State Surveillance. Its intelligence practices have strongly influenced global debates. This, of course, highlights the nation's global influence and importance in this topic.

People's Republic of China ³¹

China operates one of the most extensive state surveillance systems in the world. It combines facial recognition, AI analytics, and digital monitoring. The surveillance carried out by the said surveillance systems is closely linked to state priorities. Prime examples of that are social stability and governance control.³² The system integrates public and private data sources. This, of course, creates a highly centralized monitoring infrastructure. It must be said, however, that

²⁸ *Mass Surveillance in America*. (2024). Stanford.Edu.
https://cddrl.fsi.stanford.edu/events/mass_surveillance_in_america

²⁹ Greenwald, G. "NSA collecting phone records of millions of Verizon customers daily," The Guardian, <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>

³⁰ United Nations. (1966, December 16). *International Covenant on civil and political rights*. United Nations. Ohchr. <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>

³¹ *Mass surveillance in China | human rights watch*. (n.d.). Wwww.Hrw.Org. Retrieved <https://www.hrw.org/tag/mass-surveillance-china>

³² Human Rights Watch, "Data Leviathan: China's Burgeoning Surveillance State," <https://www.hrw.org/news/2019/08/16/data-leviathan-chinas-burgeoning-surveillance-state>

such acts of state surveillance are often cited by human rights organizations as a model that raises major concerns about both privacy and civil liberties.

Russian Federation ³³

The government of Russia promotes the concept of “digital sovereignty”. It emphasizes state control over internet infrastructure and data flows. That concept, however, heavily limits citizens’ human right to privacy. That, of course, often raises concerns over adherence to international law.

The national legislation of the nation expands the government's access to communications data and strengthens the monitoring capabilities of security services. That equates to heavier control over the citizens. The nation often justifies the aforementioned surveillance practices through the pretext of national security and counter extremism narratives; though that is often challenged by NGOs and human rights watchdogs. Ultimately, Russia’s approach reflects a broader model. In the said model, state authority in cyberspace is prioritized, and individual privacy protections become undermined.

European Union (EU)

The General Data Protection Regulation (GDPR) sets strict legal standards for data protection and individual consent across all member states of one of the strongest alliances to exist, the European Union.³⁴ The Court of Justice of the European Union is the regulatory body reinforcing these rules. It has repeatedly restricted unlawful data transfers to continuously strengthen individual privacy protections. Under this framework, surveillance regulation remains tightly linked to fundamental human rights principles. Particularly, those of necessity and proportionality. Consequently, the EU model is widely recognized as the world's strongest regulatory framework for digital privacy. That is because it demonstrates that national security interests can successfully align with public transparency and, of course, the protection of civil liberties.

Amnesty International

Amnesty International has repeatedly documented the targeted misuse of commercial spyware against journalists and political figures worldwide. A keen example of the organization’s work in forensic investigations is the exposure of the Pegasus spyware scandal. The case brought to light the severe risks that unchecked surveillance technologies pose to civil society and public

³³Kerr, J. A. (2018, December 18). *The Russian model of internet control and its significance*. Wwww.Osti.Gov. <https://www.osti.gov/servlets/purl/149198>

³⁴ EUR-Lex, Regulation (EU) 2016/679 (GDPR), official text, <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>

figures.³⁵ Amnesty has significantly shaped global awareness surrounding spyware abuse and human rights violations through cases such as the Pegasus commercial spyware. The organization leverages these disclosures and continues to campaign for strict international regulations. It also campaigns to bring oversight mechanisms to prevent future state surveillance abuses.

TIMELINE OF EVENTS

DATE	DESCRIPTION OF EVENT
10 December 1948	Universal Declaration of Human Rights (UDHR) establishes the right to privacy under Article 12, forming one of the earliest international legal foundations for privacy protection.
23 March 1976	The International Covenant on Civil and Political Rights (ICCPR) entered into force, making the protection against arbitrary or unlawful interference in privacy legally binding for ratifying states.
26 October 2001	Following the September 11 attacks, many states significantly expanded surveillance powers, including the adoption of major counterterrorism legislation such as the USA Patriot Act in the United States.
5 June 2013	Edward Snowden's disclosures reveal large-scale global surveillance programmes conducted by intelligence agencies, significantly increasing international debate on digital privacy and state surveillance.
18 December 2013	The United Nations General Assembly adopts Resolution 68/167 on the "Right to Privacy in

³⁵ Amnesty International, "Demand an end to the targeted surveillance of Human Rights Defenders" (Pegasus Project, July 2021), <https://www.amnesty.org/en/petition/targeted-surveillance-human-rights-defenders/>

	the Digital Age,” marking the first major global recognition of digital privacy as a human rights issue.
24 March 2014	Office of the High Commissioner for Human Rights publishes report A/HRC/27/37, emphasizing legality, necessity, and proportionality as key principles for lawful surveillance.
27 April 2016	The European Union adopts the General Data Protection Regulation (GDPR), establishing one of the strictest global legal frameworks for data protection and digital privacy.
25 May 2018	GDPR enters into force across the European Union, significantly influencing global data protection standards and corporate data handling practices.
18 July 2021	Pegasus spyware revelations expose the alleged misuse of commercial spyware against journalists, activists, and political figures across multiple countries, intensifying calls for the regulation of surveillance technologies.
9 September 2021	Office of the High Commissioner for Human Rights calls for a moratorium on certain artificial intelligence systems that pose serious risks to human rights, particularly in surveillance contexts.
2024	Adoption of the Global Digital Compact reflects the increased international focus on digital governance, cooperation, and the protection of human rights in the digital age.

RELEVANT UN RESOLUTIONS, TREATIES AND EVENTS

UNGA Resolution 68/167 (2013) – “The Right to Privacy in the Digital Age” ³⁶

UNGA Resolution 68/167, titled “The Right to Privacy in the Digital Age,” was adopted on 18 December 2013. It was the first major United Nations resolution to explicitly address the right to privacy in the context of digital communications and mass surveillance. The resolution affirmed that the right to privacy applies both online and offline, establishing an important principle for the protection of individuals in an increasingly digital world. It called upon states to respect and protect the right to privacy in digital communications, particularly in relation to state surveillance and the collection of personal information. As a result, Resolution 68/167 became a major legal and political foundation for subsequent international discussions concerning digital surveillance, government monitoring, and the protection of privacy rights in the digital age.

UNGA Resolution 75/176 (2020) – “The Right to Privacy in the Digital Age” ³⁷

UNGA Resolution 75/176, also titled “The Right to Privacy in the Digital Age,” was adopted on 16 December 2020 and reaffirmed the international community’s commitment to protecting privacy in the digital environment. The resolution expressed concern regarding unlawful or arbitrary surveillance and emphasized the need for states to ensure that measures involving digital technologies remain consistent with international human rights obligations. It also encouraged states to review their surveillance laws, policies, and practices in order to ensure compliance with international human rights standards. Importantly, the resolution demonstrates the continued international concern surrounding digital surveillance while also highlighting the limitations of non-binding UN resolutions, as they do not themselves establish legally enforceable obligations. This is particularly relevant to GA6, as delegates can consider how stronger international legal mechanisms could build upon these existing commitments while respecting the committee’s non-binding nature.

³⁶ *International Conference of Data Protection and privacy commissioners*. (2014). <https://globalprivacyassembly.com/wp-content/uploads/2015/03/Letter-to-the-UN-High-Commissioner-for-Human-Rights-Right-to-Privacy-in-a-Digital-Age.pdf>

³⁷ *Seventy-fifth session agenda item 72 (b) promotion and protection of human rights: Human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms resolution adopted by the General Assembly on 16 december 2020*. (2020). https://digitallibrary.un.org/record/3896430/files/A_RES_75_176-EN.pdf

International Covenant on Civil and Political Rights (ICCPR) – Article 17 ³⁸

The International Covenant on Civil and Political Rights (ICCPR) entered into force on 23 March 1976 and established legally binding obligations for states that ratify it. Article 17 provides a fundamental protection against arbitrary or unlawful interference with an individual's privacy, family, home, or correspondence, as well as against unlawful attacks on their honour and reputation. Although the ICCPR predates modern digital technologies, its protection of privacy has become highly relevant to digital communications, online data, and electronic surveillance. Article 17 therefore serves as one of the primary binding international legal provisions through which states' surveillance practices can be assessed under international human rights law. For GA6, the ICCPR is particularly significant because it demonstrates how broad international legal principles can provide a binding foundation for protecting individual rights even as technology and methods of surveillance continue to evolve.

OHCHR Report A/HRC/27/37 (2014) – “The Right to Privacy in the Digital Age” ³⁹

The Office of the United Nations High Commissioner for Human Rights (OHCHR) report A/HRC/27/37, titled “The Right to Privacy in the Digital Age,” was published on 24 March 2014. The report examined how modern digital technologies and government surveillance practices affect the right to privacy and emphasized the importance of principles such as legality and proportionality when states conduct surveillance. It warned of the risks associated with mass surveillance, insufficient oversight, and the expanding use of digital intelligence-gathering technologies. The report also stressed the importance of effective safeguards and independent oversight to prevent surveillance powers from resulting in arbitrary or unlawful interference with individuals' rights. Consequently, A/HRC/27/37 became an influential interpretative framework for understanding how existing international human rights law should be applied to surveillance practices in the digital age, making it particularly relevant to discussions on strengthening international protections for privacy and human rights.

³⁸ United Nations. (1966b, December 16). *International Covenant on civil and political rights*. United Nations. Ohchr. <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>

³⁹ UN. Office of the High Commissioner for Human Rights. “The Right to Privacy in the Digital Age : Report of the Office of the United Nations High Commissioner for Human Rights.” *United Nations Digital Library System*, UN, 30 June 2014, <https://digitallibrary.un.org/record/777869?ln=en&v=pdf>.

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

National surveillance reform legislation

After facing controversies regarding malicious acts of state surveillance, countries such as Germany and the United States introduced reforms that aimed to reform the pre-existing legislation.⁴⁰ More specifically, the focus was clearly on oversight mechanisms and judicial authorization as ways to effectively manage the ongoing situation.

Despite these legislative updates, the practical impact of national surveillance reforms remains highly uneven across different jurisdictions. Judicial independence and statutory restrictions can genuinely curtail broad agency powers. They can also enforce strict warrant requirements. Conversely, where oversight bodies lack binding enforcement authority or where broad national security exceptions are routinely invoked, domestic reforms often remain superficial. That basically allows for intelligence agencies to continue intrusive monitoring. This is mainly conducted through regulatory loopholes that should stop being exploited, through measures taken by the collaboration of experts and the creation of structured mechanisms.

Regional regulatory frameworks (GDPR model)

The European Union established comprehensive data protection rules through the General Data Protection Regulation (GDPR). Those rules basically transformed individual privacy rights. That was achieved by mandating explicit user consent, strict transparency, and granular control over personal information. The GDPR set high compliance requirements for corporate entities and data processors. That slight shift in procedure fundamentally altered how digital information is collected, stored, and, of course, managed across member states.

This regulatory approach quickly created a ripple effect in international law and policy making. That, by establishing what is widely viewed as a global benchmark for digital privacy. Foreign governments and multinational corporations increasingly adapted their domestic legislation and operational standards. The reason lies in their wish to align with GDPR requirements. This pushed non-EU nations to modernize their own legal frameworks in order to maintain international trade and cross-border data flows.

However, the framework faces clear structural limitations when addressing state surveillance. That is, given that EU treaties treat national security as an exclusive competence of individual member states.⁴¹ The GDPR, on the other hand, primarily governs commercial data

⁴⁰ Courthouse News Service, "Court Curbs German Spies' Foreign Internet Surveillance," <https://www.courthousenews.com/court-curbs-german-spies-foreign-internet-surveillance/>

⁴¹ EUR-Lex, Consolidated Version of the Treaty on European Union, Article 4(2), <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12016M004>

handling. As a result, it lacks direct legal authority over state intelligence agencies or national security operations. Thus, government monitoring practices are left largely outside its regulatory reach.

UN Resolutions and Soft Law Frameworks

In response to growing concerns over global digital monitoring, the UN General Assembly adopted a series of resolutions on "The Right to Privacy in the Digital Age". Those resolutions essentially affirmed that human rights protected offline must be protected online as well. This effort was reinforced by the UN Human Rights Council through the creation of the Special Rapporteur on the Right to Privacy.⁴² That mandate was designed to evaluate state practices, document abuses, and offer guidelines. All to align national surveillance with international human rights treaties (essential to resolving cases of malicious State Surveillance).

Alongside official UN initiatives, international legal scholars and human rights organizations established civil society frameworks (most notably the "Necessary and Proportionate" principles of the International Principles on the Application of Human Rights to Communications Surveillance). These guidelines sought to set clear global benchmarks. They aimed to do so by mandating that any state interception of communications must prove explicit legal authorization, legitimate public goals, strict necessity, and prior judicial approval.

Despite establishing vital normative standards, these international frameworks operate almost entirely as "soft law." The reason lies in the execution of such resolutions. Because General Assembly resolutions and expert guidelines carry no legally binding enforcement mechanisms or punitive measures, member states face zero legal consequences for non-compliance. Ultimately, governments routinely prioritize domestic security interests, and overlook non-binding international principles. That leaves the aforementioned global standards frequently ignored in practice.

POSSIBLE SOLUTIONS

Establish international minimum standards for surveillance

The current regulatory vacuum is noticeably in need of reform. To do so, the international community must codify binding global standards that set clear legal boundaries for lawful interception. Crucially, any meaningful framework must explicitly prohibit indiscriminate mass surveillance. That basically establishes that bulk data collection inherently violates fundamental privacy rights. Instead, state monitoring must be governed by strict necessity and proportionality

⁴² OHCHR, "Special Rapporteur on the right to privacy," <https://www.ohchr.org/en/special-procedures/sr-privacy>

assessments. Essentially, governments would be required to prove that targeted surveillance is the least intrusive means available to address a specific, verified security threat.

(I believe that it's very clear how this can resolve cases where State Surveillance is challenged as malicious or not).

Strengthen independent oversight mechanisms

Effective regulation depends on robust, non-partisan oversight that is capable of holding intelligence operations accountable. States should institute mandatory prior judicial authorization for any intrusive monitoring. This would be conducted by maintaining records of proposals and judicial rulings, with the goal of guaranteeing legal compliance. Furthermore, establishing independent national supervisory bodies. These said bodies would be empowered to conduct regular, unannounced audits of intelligence agencies. Essentially, that would ensure that surveillance activities do not rule in unchecked executive power. Instead, they would be subject to statutory limits, which would increase both transparency and accountability.

Regulate commercial spyware and dual-use technologies

We must comprehend that reining in the proliferation of digital intrusion tools requires the strict international regulation of the private surveillance market. For that to occur, states must establish rigorous export control regimes and binding licensing systems for commercial tech vendors. That would prevent the transfer of dual-use technologies to regimes with documented human rights abuses. Additionally, international agreements should establish clear criminal penalties against both corporate entities and state actors involved in the unlawful deployment of spyware against any individual, as that would further deter misuse.

BIBLIOGRAPHY

General Bibliography

"What Is Data Retention? Best Practices & Policies." *BigID*, 2023, <https://bigid.com/blog/what-is-data-retention/>

"Predictive Policing Explained." *Brennan Center for Justice*, 1 Apr. 2020, www.brennancenter.org/our-work/research-reports/predictive-policing-explained

"What Is Pegasus Spyware?" *McAfee Blog*, McAfee, LLC, 2021, <https://www.mcafee.com/learn/what-is-pegasus-spyware/>

"What Is Zero-Click Malware?" *Kaspersky Resource Center*, Kaspersky Lab, <https://www.kaspersky.com/resource-center/definitions/what-is-zero-click-malware>

United Nations. "Universal Declaration of Human Rights." *United Nations*, www.un.org/en/about-us/universal-declaration-of-human-rights.

UN High Commissioner for Human Rights (OHCHR). "International Covenant on Civil and Political Rights." *OHCHR*, www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

"Pegasus Project Revelations (2021)." *Cyber Law Toolkit*, NATO CCDCOE, [cyberlaw.ccdcoe.org/wiki/Pegasus_Project_revelations_\(2021\)](https://cyberlaw.ccdcoe.org/wiki/Pegasus_Project_revelations_(2021)).

European Parliamentary Research Service (EPRS). "Regulating Facial Recognition in the EU." *European Parliament*, Sept. 2021, [www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA\(2021\)698021_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf).

"Mass Surveillance in America." *Center on Democracy, Development and the Rule of Law*, Stanford University, cddrl.fsi.stanford.edu/events/mass_surveillance_in_america.

"Edward Snowden and the NSA Mass Surveillance Controversy." *Teach Democracy*, teachdemocracy.org/wp-content/uploads/2025/01/snowden_nsa.pdf.

"Foreign Intelligence Surveillance Act (FISA)." *Bureau of Justice Assistance*, U.S. Department of Justice, bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286.

"Mass Surveillance in China." *Human Rights Watch*, www.hrw.org/tag/mass-surveillance-china.

Soldatov, Andrei, and Irina Borogan. "Russian Cyber Surveillance Under SORM." *Office of Scientific and Technical Information (OSTI)*, U.S. Department of Energy, 2018, www.osti.gov/servlets/purl/1491981.

"General Data Protection Regulation (GDPR)." *GDPR Info*, gdpr-info.eu/.

"International Principles on the Application of Human Rights to Communications Surveillance." *Electronic Frontier Foundation*, Mar. 2025, www.eff.org/files/2025/03/03/necessary_and_proportionate.pdf.

"Letter to the UN High Commissioner for Human Rights: Right to Privacy in a Digital Age." *Global Privacy Assembly*, <https://globalprivacyassembly.com/wp-content/uploads/2015/03/Letter-to-the-UN-High-Commissioner-for-Human-Rights-Right-to-Privacy-in-a-Digital-Age.pdf>

United Nations General Assembly. "Resolution 75/176: The Right to Privacy in the Digital Age." *United Nations Digital Library*, 16 Dec. 2020, digitallibrary.un.org/record/3896430/files/A_RES_75_176-EN.pdf.

UN High Commissioner for Human Rights (OHCHR). "International Covenant on Civil and Political Rights." *OHCHR*, www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

Office of the United Nations High Commissioner for Human Rights (OHCHR). "The Right to Privacy in the Digital Age: Report A/HRC/27/37." *United Nations*, 24 Mar. 2014, www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

Simmler, M. "Facial Recognition Technology in Law Enforcement." *Computer Law & Security Review*, vol. 56, 2025, article 106092. <https://alexandria.unisg.ch/server/api/core/bitstreams/fcc5235e-bab4-4e58-8b6e-0c39c329d290/content>

Tzanou, Maria, and Plixavra Vogiatzoglou. "National Security and New Forms of Surveillance: From the Data Retention Saga to a Data Subject Centred Approach." *SSRN Electronic Journal / European Papers*, 2024. <https://www.europeanpapers.eu/e-journal/national-security-forms-surveillance-data-retention-saga-data-subject-centred-approach>

Watt, Eliza. "The Role of International Human Rights Law in the Protection of Online Privacy in the Age of Surveillance." *2017 9th International Conference on Cyber Conflict (CyCon)*, IEEE, 2017, pp. 1-14. <https://ccdcoe.org/uploads/2018/10/Art-06-The-Role-of-International-Human-Rights-Law-in-the-Protection-of-Online-Privacy-in-the-Age-of-Surveillance.pdf>

United Nations. *Pact for the Future: Resolution Adopted by the General Assembly on 22 September 2024 (A/RES/79/1)*. United Nations, 2024, www.un.org/en/summit-of-the-future/pact-for-the-future.

Jiang, Q. "Interpreting the Global Digital Compact: Charting a New Vision Towards a Multi-Stakeholder Governance Model." *Journal of International Economic and Global Governance*, vol. 2, no. 1, 2025, pp. 45-66. <https://doi.org/10.12414/jiegg.250437>.

Office of the United Nations High Commissioner for Human Rights (OHCHR). *The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights (A/HRC/48/31)*. United Nations, 13 Sept. 2021, <https://www.ohchr.org/en/documents/thematic-reports/ahrc4831-right-privacy-digital-age-report-united-nations-high>

Endeley, Robert E. *End-to-end Encryption, Backdoors, and Privacy*. ProQuest Dissertations Publishing, 2024, <https://www.proquest.com/openview/fb35c693e604da5fd6e90dff37d1f1c8/1?pq-origsite=gscholar&cbl=18750&diss=y>

Qandeel, Mais. "Facial Recognition Technology: Regulations, Rights and the Rule of Law." *Frontiers in Big Data*, vol. 7, 2024, article 1354659. <https://doi.org/10.3389/fdata.2024.1354659>.

House of Lords - Surveillance: Citizens and the State - Constitution Committee, publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1804.htm.

"Digital Privacy Definition: What Is Digital Privacy & Digital Safety." *Enzuzoprivacy*, 2026, <https://www.enzuzo.com/blog/digital-privacy-definition>.

Sumner, Stuart. "The Snowden Revelations." *You: For Sale*, Elsevier, 2016, pp. 17–48, <https://doi.org/10.1016/b978-0-12-803405-7.00002-3>.

Moeller, Robert. "Spyware." *Afterimage: The Journal of Media Arts and Cultural Criticism*, vol. 38, no. 1, July 2010, pp. 34–34, <https://doi.org/10.1525/aft.2010.38.1.34>

"Biometric Data - Definition, FAQs - Innovatrics." *Innovatrics*, 5 Mar. 2021, <https://www.innovatrics.com/glossary/biometric-data/>.

Tasho Tashev. "What Is a Zero Click Exploit?" *Webopedia*, 27 Feb. 2025, <https://www.webopedia.com/technology/what-is-a-zero-click-exploit/>.

"Predictive Policing | Social Sciences and Humanities | Research Starters | EBSCO Research." *Ebsco*, 2021, <https://www.ebsco.com/research-starters/social-sciences-and-humanities/predictive-policing>.

Austin. "What Is an Encryption Backdoor?" *Global Brands Magazine*, 19 Feb. 2025, <https://www.globalbrandsmagazine.com/what-is-an-encryption-backdoor/>.

Jiménez Egido, Irene. "What Is Digital Sovereignty and Why Does It Matter?" *Uncover IE*, 2 Jan. 2026, <https://www.ie.edu/uncover-ie/digital-sovereignty-master-in-public-policy/>.

"Facial Recognition Technology in Surveillance | Computer Science | Research Starters | EBSCO Research." *Ebsco*, 2023, <https://www.ebsco.com/research-starters/computer-science/facial-recognition-technology-surveillance>.

United Nations. (1948, December 10). *Universal declaration of human rights*. United Nations. <https://www.un.org/en/about-us/universal-declaration-of-human-rights>

United Nations. (1966, December 16). *International Covenant on civil and political rights*. United Nations. Ohchr. <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>

- Kerr, J. A. (2018, December 18). *The Russian model of internet control and its significance*. Www.Osti.Gov. <https://www.osti.gov/servlets/purl/1491981>
- United Nations. (1966, December 16). *International Covenant on civil and political rights*. United Nations. Ohchr. <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>
- Mass surveillance in China | human rights watch. (n.d.). Www.Hrw.Org. Retrieved <https://www.hrw.org/tag/mass-surveillance-china>
- Kerr, J. A. (2018, December 18). *The Russian model of internet control and its significance*. Www.Osti.Gov. <https://www.osti.gov/servlets/purl/149198>
- International Conference of Data Protection and privacy commissioners. (2014). <https://globalprivacyassembly.com/wp-content/uploads/2015/03/Letter-to-the-UN-High-Commissioner-for-Human-Rights-Right-to-Privacy-in-a-Digital-Age.pdf>
- Seventy-fifth session agenda item 72 (b) promotion and protection of human rights: Human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms resolution adopted by the General Assembly on 16 december 2020. (2020). https://digitallibrary.un.org/record/3896430/files/A_RES_75_176-EN.pdf
- United Nations. (1966b, December 16). *International Covenant on civil and political rights*. United Nations. Ohchr. <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>
- UN. Office of the High Commissioner for Human Rights. "The Right to Privacy in the Digital Age : Report of the Office of the United Nations High Commissioner for Human Rights." *United Nations Digital Library System*, UN, 30 June 2014, <https://digitallibrary.un.org/record/777869?ln=en&v=pdf>.
- Cyberhaven, "What Is Metadata? Definition, Types, and Security Risks," <https://www.cyberhaven.com/infosec-essentials/metadata>
- Britannica, "September 11 attacks," <https://www.britannica.com/event/September-11-attacks>
- Britannica, "USA PATRIOT Act," <https://www.britannica.com/topic/USA-PATRIOT-Act>
- Penney, J. "Chilling Effects: Online Surveillance and Wikipedia Use," SSRN (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645
- Committee to Protect Journalists, "Spyware and Press Freedom," <https://cpj.org/spyware/>
- Amnesty International, "Demand an end to the targeted surveillance of Human Rights Defenders," <https://www.amnesty.org/en/petition/targeted-surveillance-human-rights-defenders/>
- Freedom House, "Freedom on the Net," <https://freedomhouse.org/report/freedom-net>
- Freedom House, "Persistent Authoritarian Repression and Backsliding in Democracies Drive 15th Consecutive Year of Decline in Global Internet Freedom," <https://freedomhouse.org/article/new-report-persistent-authoritarian-repression-and-backsliding-democracies-drive-15th>
- Britannica, "Five Eyes," <https://www.britannica.com/topic/Five-Eyes>

UNODC, "Behind the screen: how cyber investigations fight human trafficking," https://www.unodc.org/unodc/en/frontpage/2026/February/behind-the-screen_-how-cyber-investigations-fight-human-trafficking.html

UNODC, "Using the Power of Technology to Help Victims of Human Trafficking," <https://www.unodc.org/unodc/frontpage/2022/July/using-the-power-of-technology-to-help-victims-of-human-trafficking.html>

Europol, "Internet Organised Crime Threat Assessment (IOCTA)," <https://www.europol.europa.eu/publications-events/main-reports/iocta-report>

U.S. Department of the Treasury, "Financial Action Task Force (FATF)," <https://home.treasury.gov/about/offices/terrorism-and-financial-intelligence/terrorist-financing-and-financial-crimes/financial-action-task-force-fatf>

CISA, "Secure Critical Infrastructure," <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/secure-critical-infrastructure>

Congressional Research Service, "Cross-Border Data Sharing Under the CLOUD Act," <https://www.congress.gov/crs-product/R45173>

Greenwald, G. "NSA collecting phone records of millions of Verizon customers daily," The Guardian, <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>

Human Rights Watch, "Data Leviathan: China's Burgeoning Surveillance State," <https://www.hrw.org/news/2019/08/16/data-leviathan-chinas-burgeoning-surveillance-state>

EUR-Lex, Regulation (EU) 2016/679 (GDPR), official text, <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>

Amnesty International, "Demand an end to the targeted surveillance of Human Rights Defenders" (Pegasus Project, July 2021), <https://www.amnesty.org/en/petition/targeted-surveillance-human-rights-defenders/>

Courthouse News Service, "Court Curbs German Spies' Foreign Internet Surveillance," <https://www.courthousenews.com/court-curbs-german-spies-foreign-internet-surveillance/>

EUR-Lex, Consolidated Version of the Treaty on European Union, Article 4(2), <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12016M004>

OHCHR, "Special Rapporteur on the right to privacy," <https://www.ohchr.org/en/special-procedures/sr-privacy>