Committee: Special Conference on Free will in the age of Artificial Intelligence (SPECON)

Topic: Examining the moral implications of mass surveillance

Student Officer: Sevastiana Kattideniou

Position: Deputy President

Personal Introduction

Hello delegates! My name is Sevastiana Kattideniou, I'm 17 years old, and I'm an IB2 student at Campion. It is my utmost pleasure to welcome you to this conference and committee!

My MUN journey began in 2019, as a nervous Year 7 delegate at SPECON, right here at CSMUN. That experience sparked my love and interest in debate and diplomacy, and since then, I've had the opportunity to represent countries in various committees such as GA2, GA3, and WHO. Through all this, I've come to appreciate how MUN is not just about speaking - it's about listening, collaborating, and building an inclusive space for all voices to be heard. Chairing this year feels like a full-circle moment: from sitting where you will now be to helping guide the very kinds of debates that first inspired me. I want this committee to be a space for everyone, regardless of your experience level. This year, our committee will tackle a complex and deeply relevant topic, examining the moral implications of mass surveillance. In an age defined by data, governments and corporations possess unprecedented access to information. The line between national security and personal privacy and freedom is growing increasingly thin. As delegates, your task will be to dissect these ethical dilemmas: How much surveillance is too much? When does protection become oppression? And whose rights are we willing to compromise when facing collective safety?

Through this study guide, I aim to introduce you to this topic, offer important information that will aid in drafting your resolutions, and, most importantly, encourage you to conduct research beyond this guide.

For any further questions, feel free to contact me via my email address at skattideniou@campion.edu.gr. I hope to meet all of you in October!

Remember someone's always watching…

Sevastiana

Topic Introduction

In the context of this year's theme, "Free Will in the Age of Artificial Intelligence", mass surveillance refers to the large-scale monitoring of individuals by governments and corporations and is one of the greatest threats to individual autonomy, as AI systems are increasingly shaping, controlling, and predicting human behaviour[1]. It gained momentum after the events of 9/11 and during COVID-19 for security and public health reasons, using advanced technologies such as facial recognition, location tracking, social media monitoring, and data mining.[2] Governments have claimed that mass surveillance is necessary for national security, but most often lack strong oversight and transparency. For example, the 2016 UK Investigatory Powers Act enabled the collection of web and phone data but was later ruled as partially illegal for violating privacy and freedom of expression[3].

Authoritarian regimes use surveillance as a way to control information flows and censor dissent, while private companies collect and monetise data, often in cooperation with state agencies. This has raised serious moral concerns about privacy and freedom of expression. Legal frameworks are unable to keep pace with technological advancements, and governments benefiting from these tools have little to regulate.[4]

Without a secure and effective international legal framework, mass surveillance risks are becoming normalised and permanent. Once entrenched, surveillance systems are difficult to dismantle, embedding themselves into everyday functions of state and corporate power. Mass surveillance threatens the core of free will and privacy in our modern society. Different groups are harmed in varying ways - activists and journalists may face suppression and harassment, minorities may be unfairly targeted or profiled, and ordinary citizens may self-censor out of fear of constant monitoring. Society, as a whole, begins to shift towards a state of control and compliance, where democratic values erode and trust in institutions and government declines.

[1] "The Power and Limits of AI in Predicting Human Actions." DataScience next Conference, 18 Mar. 2025
[2] Barriga, Antónia do Carmo, et al. "The COVID-19 Pandemic: Yet Another Catalyst for Governmental Mass Surveillance?" Social Sciences & Humanities Open, vol. 2, no. 1, 2020, p. 100096,
[3] Wikipedia Contributors. "Investigatory Powers Act 2016." Wikipedia, Wikimedia Foundation, 11 July 2019
[4] Akpobome, Omena. (2024). The Impact of Emerging Technologies on Legal Frameworks: A Model for Adaptive Regulation. International Journal of Research Publication and Reviews. 5. 5046-5060. 10.55248/gengpi.5.1024.3012.

Thus, making this topic essential to be discussed, and as delegates, you need to consider how to create frameworks that address legitimate security concerns while safeguarding individual rights in the age of artificial intelligence.

Definition of key concepts

Surveillance

"The careful watching of a person or place, especially by the police or army, because of a crime that has happened or is expected."[5]

Privacy

"Someone's right to keep their personal matters and relationships secret."[6]

Metadata

"Data that provides information about other data"[7], often collected without direct content, yet still intrusive, as it can reveal patterns of behaviour and social networks

Intelligence-gathering

"Intelligence gathering refers to the essential task of collecting information from diverse sources to preserve life and property." [8], governments and security agencies often defend mass surveillance by portraying it as a vital component of this process

Data Mining

"Data mining is the process of sorting through large data sets to identify patterns and relationships that can help solve business problems through data analysis. Data mining techniques and tools help enterprises to predict future trends."[9]

Sunset Clauses

"Part of a law or contract that states when it will end, or the conditions under which it will end"[10]

[5] "MASS SURVEILLANCE Collocation | Meaning and Examples of Use." CambridgeWords, 25 Sept. 2024
[6] Cambridge Dictionary. "PRIVACY | Meaning in the Cambridge English Dictionary." Cambridge.org, 2019
[7] Merriam-Webster. "Definition of METADATA." Merriam-Webster.com, 2019,
[8] "Intelligence Gathering - an Overview | ScienceDirect Topics
[9] Stedman, Craig. "What Is Data Mining?" TechTarget, Sept. 2021
[10] Cambridge Dictionary. "Sunset Clause." @CambridgeWords, 9 July 2025

Closed Circuit Television (CCTV)

"A system that uses video cameras to send television signals to a specific, limited viewership"[11], isn't typically shared with the public, but directly to the camera's owner.

Facial recognition

"A contemporary security solution that automatically identifies and verifies the identity of an individual from a digital image or video frame"[12]

Data scraping

"The activity of taking information from a website or computer screen and putting it into an ordered document on a computer", [13], used to predict patterns and trends

Background Information

Mass surveillance has evolved from a tool for specific investigations to a widespread monitoring system embedded into our everyday life, shaping how we exercise our rights - such as freedom of expression, assembly, and access to information - and altering how societies function by normalising constant oversight. For example, activists may avoid organising protests due to fear of being tracked, journalists might hesitate to contact sensitive sources, and citizens could refrain from researching controversial topics online. Surveillance measures can undermine civil liberties and democratic accountability by fostering fear and self-censorship. Individuals may hesitate to express opinions, protest, or seek information if they believe their actions are being recorded, constraining the exercise of free will and participation. Metadata collection, which is seen as less intrusive, in reality enables the reconstruction of personal networks and movements without individuals' awareness. By mapping a person's life (where they go, whom they meet, what times they are active, etc.), authorities and corporations can infer details about someone's political views, health conditions, and private relationships. This raises risks of discrimination and exploitation, challenging privacy and autonomy in subtle but influential ways.

[11] Martin, Roland. "Closed-Circuit Television | Meaning, Camera, System, History, & Facts | Britannica."
[12] "Facial Recognition Technology | Homeland Security."
[13] Cambridge Dictionary. "Data Scraping." @CambridgeWords, 17 May 2023

Consequences

Mass surveillance can have a positive effect by aiding in crime prevention, public safety, and efficient crisis response.[14] An example of this is that the UK's widespread use of CCTV has been linked to a 16% reduction in crime in monitored areas, according to a 2022 study by the College of Policing.[15] These technologies have enabled more efficient crisis response and enhanced public safety. However, when left unchecked, mass surveillance becomes a dangerous tool, reinforcing systemic discrimination and consolidating authoritarian power, without transparency or accountability. Efforts to create a moral and legal framework around surveillance will deeply affect various stakeholders: governments may have to recalibrate national security strategies, corporations could face revenue losses from the restriction of data monetisation, and individuals may finally reclaim their right to privacy and freedom of expression.[16] But differences in implementation will emerge. More economically developed countries, MEDCs, like Germany and Japan, have invested in strict legal safeguards and advanced oversight mechanisms. Meanwhile, LEDCs, such as Ethiopia and Myanmar, have used surveillance tools to suppress dissent and monitor minority communities - deepening existing inequalities in digital rights.[17] Taking the case of Myanmar, Chinese surveillance technology was deployed in Yangon to monitor citizens during protests in 2021. Facial recognition cameras targeted demonstrators, often resulting in arbitrary arrests.[18]

Challenges

Establishing ethical surveillance frameworks will face significant challenges. One key obstacle is the rapid pace of technological advancement, which consistently outpaces the development of legal and ethical frameworks. As surveillance technologies become more sophisticated, laws struggle to keep up, leaving gaps where practices can become established before appropriate safeguarding is introduced.

[14] YANG, Sihan, et al. "The Impact of Surveillance Cameras and Community Safety Activities on Crime Prevention: Evidence from Kakogawa City, Japan." Sustainable Cities and Society, vol. 115, Elsevier BV, Sept. 2024, pp. 105858–58.
[15] College of Policing. "Closed-Circuit Television (CCTV)." College of Policing, 19 Feb. 2021
[16] "Surveillance and Privatizing National Security – GIS Reports." GIS Reports, 20 June 2025
[17] "Ethiopia: New Spate of Abusive Surveillance." Human Rights Watch, 6 Dec. 2017
[18] Human Rights Watch. "Myanmar: Facial Recognition System Threatens Rights." Human Rights Watch, 12 Mar. 2021

Another challenge is the lack of global consensus on what separates and constitutes necessary versus excessive surveillance.[19] Different states interpret security needs through varying lenses, influenced by their histories, governance systems, and perceived threats. For some, extensive surveillance is framed as essential to prevent terrorism or organised crime, while others see these practices as a violation of individual freedoms. This divergence complicates efforts to establish a unified international standard.

Resistance from governments that prioritise control further complicates the situation. Authoritarian regimes often view surveillance as a key mechanism for maintaining political stability, while even democratic governments may hesitate to scale back surveillance powers once they are in place, citing public safety concerns.

Additionally, the interests of large technology corporations cannot be overlooked. Many companies profit from the collection and analysis of user data and may resist regulatory measures that threaten these revenue streams. Their power can slow or weaken efforts to implement ethical standards and transparency requirements.

There are also practical barriers to implementation. Ethical surveillance frameworks require oversight, technical infrastructure, and continuous monitoring to ensure compliance, all of which demand resources, expertise, and political will. Moreover, disparities in resources between countries risk deepening global inequalities, with wealthier nations able to enforce ethical practices while LEDCs may lack the capacity to protect citizens from abuses. Balancing the need for security with the protection of privacy and autonomy is therefore a complex task.

Surveillance Technologies

Surveillance technologies are used by both democratic and authoritarian governments to monitor populations, enforce laws, and maintain public order. However, their deployment raises significant ethical, legal, and social concerns. Among the most widely used tools are CCTV and facial recognition, mobile tracking and geolocation services, social media data scraping, and artificial intelligence (AI).

CCTV and facial recognition systems are prevalent across the globe. They are used in public spaces to deter crime, identify suspects, and enhance security. In cities like London, CCTV networks are

[19] Feldstein, Steven. "The Global Expansion of AI Surveillance." *Carnegie Endowment for International Peace*, 17 Sept. 2019

extensive and are often integrated with facial recognition software to quickly match individuals against criminal databases.[20] While these tools can help in solving crimes or locating missing persons, they are also heavily criticised. One major concern is the potential for racial profiling, as facial recognition systems have been shown to perform less accurately on people of colour.[21] Additionally, the presence of these technologies at protests or political gatherings raises fears of unwarranted surveillance.

Mobile tracking and geolocation services rely on data collected from smartphones, either through apps or directly from telecom providers. This information can reveal an individual's real-time location, movements, and patterns of behaviour. Governments may use this data for public health purposes or for law enforcement. However, this practice poses serious privacy concerns. Often, users are unaware that their data is being shared or sold to third parties, including government agencies. The lack of transparency and consent in these practices can undermine trust in both private companies and public institutions.[22]

Social media and data scraping are also increasingly used by public and private entities to monitor user behaviour. Platforms like Twitter, Facebook, and Instagram are analysed to detect trends, assess public sentiment, or identify potential threats. For example, law enforcement agencies may use social media scraping tools to identify individuals planning protests or engaging in illegal activities online. While this can enhance predictive capabilities and improve public safety, it also opens the door to mass surveillance and the infringement of free expression. Users may be monitored even when they believe their accounts are private or their data is secure.[23]

Artificial intelligence (AI) plays a growing role in automating surveillance systems. AI algorithms can process vast amounts of data from video feeds, mobile devices, and online activity to detect patterns and flag "suspicious" behaviour. For instance, AI might be used in airports to monitor body language and alert security personnel to possible threats.[24] While AI can improve efficiency and reduce human

[20] Boffey, Daniel, and Mark Wilding. "Live Facial Recognition Cameras May Become 'Commonplace' as Police Use Soars." The Guardian, The Guardian, 24 May 2025

[21] Hardesty, Larry. "Study Finds Gender and Skin-Type Bias in Commercial Artificial-Intelligence Systems." MIT News | Massachusetts Institute of Technology, Feb. 2018

[22] Oluwatoni Olujinmi. "Geolocation Tracking, All the Risks Connected to It." World Excellence International, 27 Apr. 2023

[23] Muhammad Tuhin. "The Dark Side of AI: Bias, Surveillance, and Control." Science News Today, 24 Apr. 2025

[24] Abbasi, Omar. "Artificial Intelligence at Airports - Revolutionizing Airport Management." Embross | Passenger Self Service, 2 Feb. 2024

error, it also raises concerns about accountability and bias. Decisions made by algorithms without human oversight can lead to false positives, discrimination, and violations of individual rights.

Case Studies

2013 Snowden Revelations

Edward Snowden, a former National Security Agency (NSA) contractor, leaked thousands of classified documents, and the world came face-to-face with the reality of mass digital surveillance. Programs like PRISM 9 revealed that not only were American citizens being monitored, but so were foreign governments, journalists, and millions of private individuals.[25]

The outrage was global. For many, it confirmed what had long been suspected - that surveillance wasn't just about protection; it was about power. This moment ignited global debate on ethics, transparency, and the need for legal oversight. It was made clear that unchecked surveillance undermined democratic accountability.

2016 UK Investigatory Powers Act

Often referred to as the "Snooper's Charter," the United Kingdom passed legislation in 2016 allowing the collection of internet browsing histories and even hacking into devices (without the user's knowledge). While presented as a tool to combat terrorism, privacy advocates criticised it as one of the most extreme surveillance laws in democratic history.[26]

In 2018, the European Court of Human Rights ruled that the law violated fundamental rights to privacy and freedom of expression. This case highlighted how democratic states are not immune to overreach and how legal systems struggle to keep pace with surveillance technologies.

[25] BBC News. "Edward Snowden: Leaks That Exposed US Spy Programme." BBC News, 17 Jan. 2014
[26] Liberty. "SNOOPERS' CHARTER." Liberty

Key Events/Timeline

Date	Description of Event
September 11th, 2001	The 9/11 attacks marked a major shift in global security policy. Led by the U.S., governments expanded surveillance systems to combat terrorism. The USA PATRIOT Act granted sweeping powers to monitor communications and collect data like phone records, emails, and financial transactions.[27] This reframed privacy as secondary to collective protection, normalising mass data collection with minimal oversight. Legal boundaries blurred, transparency declined, and civil liberties steadily eroded - sparking growing public concern over government overreach.
May 11th, 2006	USA Today exposes the NSA's collection of billions of domestic phone call records from AT&T, Verizon, and BellSouth. First major domestic surveillance scandal post-9/11.
June 5th, 2013	National Security Agency (NSA) contractor Edward Snowden leaked classified documents exposing global mass surveillance programs like PRISM. Surveillance of citizens, foreign leaders, journalists, and more is revealed.
June 2nd, 2015	A legal response to Snowden's leaks. Ended

[27] Department of Justice. "The USA Patriot Act: Preserving Life and Liberty." Justice.gov, Department of Justice, 2001, www.justice.gov/archive/ll/highlights.htm.

	bulk phone metadata collection by the NSA, but left loopholes. Introduced court oversight for some programs.
November 29th, 2016	The United Kingdom allows the collection of browsing history, phone records, and hacking of devices. Claimed to be for national security.
May 25th, 2018	The General Data Protection Regulation comes into force, setting a global benchmark for data protection and privacy.[28]
January 2020- May 2023	Several governments, particularly in Asia and the Middle East, deploy digital tracing apps, thermal scanning, and facial recognition for public health. Often adopted with no clear oversight or sunset clauses.[29]
December 2021	Myanmar deploys Chinese facial recognition tech in Yangon to identify and arrest protesters.
February - December 2023	Integration of AI, facial recognition, and predictive policing in public surveillance systems. Raises new concerns around accountability, bias, and machine-led policing.
February 2nd 2025	The European Union's Artificial Intelligence Act came into force - banning the use of AI-powered predictive policing, facial recognition (including mass scraping of images

[28] European Commission. "Legal Framework of EU Data Protection." European Commission, 2018, commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en.
[29] Burgess, Matt. "How Singapore Beat Covid-19." WIRED, 16 Dec. 2020, www.wired.com/story/singapore-covid-news-tracetogether/.

	to build databases), and other manipulative AI systems such as emotion recognition. These bans aimed to mitigate risks to human rights and accountability.[30]

Major countries, organisations and alliances

United States of America (USA)

The United States stands as a pioneer in the debate over mass surveillance. Following the events of 9/11, the U.S. enacted the USA PATRIOT Act, granting extensive powers to intelligence agencies like the National Security Agency to collect and analyse vast amounts of data, including on foreign nationals. Programs such as PRISM, revealed by Edward Snowden in 2013, exposed the global scale of American surveillance, including the monitoring of citizens, diplomats, journalists, and even allied governments.[31] While the U.S. maintains that surveillance is critical to national security, many argue that its policies often lack sufficient transparency and oversight. Despite extensive powers, the U.S. still faces repeated data leaks and scandals, showing its system prioritises security over trust. As the world's leading tech hub and a founding member of the Five Eyes, American surveillance practices set global norms and influence others' approaches.

United Kingdom

The UK operates a highly developed surveillance infrastructure, with some of the densest CCTV coverage in the world, increasingly supported by facial recognition and AI analytics. The Investigatory Powers Act 2016 grants intelligence agencies access to a wide range of digital data, including browsing history and communications metadata, often without users' knowledge. While these powers are justified as tools to combat terrorism and organised crime, they have raised serious civil

[30] "Article 5: Prohibited Artificial Intelligence Practices | EU Artificial Intelligence Act." *EU Artificial Intelligence Act*, 2 Feb. 2025, artificialintelligenceact.eu/article/5/.
[31] "Enemies of the Internet 2014 - USA: NSA Symbolises Intelligence Services' Abuses | Refworld." *Refworld*, 2023, www.refworld.org/reference/annualreport/rsf/2014/en/98666.

liberty concerns. Parliamentary oversight exists but has been criticised as insufficient.[32] As a democracy, the UK's choices are often cited to legitimise surveillance powers elsewhere, making its approach globally significant.

China

China operates one of the most technologically advanced surveillance systems in the world. The government heavily relies on facial recognition, biometric data, AI-powered analytics, and real-time tracking to monitor its population. Surveillance is deeply embedded in daily life, from public transport and workplaces to schools and residential areas. The Chinese Communist Party frames this as essential for maintaining public order and national security, but in practice, it serves as a powerful tool for political control. One of the most controversial aspects is the surveillance of ethnic minorities, particularly in Xinjiang, where technologies are used to monitor, profile, and detain members of the Uyghur Muslim community. China's model raises urgent ethical concerns, especially as its surveillance technologies are increasingly exported to other countries - influencing how governments around the world approach surveillance and control.

Russia

Russia has built a surveillance infrastructure that blends legal authority with advanced technology to monitor its population, particularly political opponents and dissenting voices. Under laws like the Yarovaya Law, telecom and internet companies are required to store user data and provide unrestricted access to security services, notably the Federal Security Service (FSB). Surveillance tools such as the System for Operative Investigative Activities (SORM) allow state agencies to intercept communications without meaningful oversight. During protests and elections, facial recognition and social media monitoring are used to identify and track participants. The Russian government justifies these measures of national security and anti-terrorism efforts, but critics argue that the true intent is to suppress freedom of expression and maintain tight control over civil society. The lack of judicial transparency and the broad powers granted to law enforcement raise serious ethical concerns, particularly where the legal system offers limited protection against state overreach. Russia's

[32] "Investigatory Powers Act 2016." Legislation.gov.uk, 2016, www.legislation.gov.uk/ukpga/2016/25/contents.

surveillance practices highlight how authoritarian-leaning regimes use legal mechanisms to legitimise invasive state control.

Nigeria

Nigeria represents a key example of how surveillance practices are developing in the Global South amidst political instability and limited regulatory frameworks. In recent years, the Nigerian government has expanded its capacity to monitor online activity, including requiring telecom companies to retain user metadata and internet browsing histories. Surveillance tools have also been used to track protests, particularly during movements like #EndSARS.[33] Civil society organisations warn that without proper legislation and oversight, surveillance will continue to be used against marginalised communities. Limited digital literacy and infrastructural gaps also make the population more vulnerable to covert data extraction.

India

India is actively expanding its surveillance capabilities, particularly through its Central Monitoring System (CMS), which allows the government to intercept calls, messages, and online activity without prior judicial approval. The government defends these measures as necessary for national security and counter-terrorism, but civil liberties groups have raised concerns over the lack of transparency and the absence of meaningful oversight. India's approach reflects a broader global trend where rapidly advancing digital infrastructure in emerging economies outpaces the development of ethical and legal safeguards. As surveillance becomes more integrated with AI (such as the Aadhaar system), questions around consent, data security, and misuse become more and more urgent. The scale of data collection is impressive, but without legal checks, the risks of misuse are high. As the world's largest democracy, India represents how emerging economies balance technological ambition with weak institutional protections.

[33] "Tracking Protest Surveillance | Privacy International." *Privacyinternational.org*, 2024, privacyinternational.org/examples/tracking-protest-surveillance.

Brazil

Brazil presents a complex case where surveillance intersects with political instability, weak oversight, and human rights concerns. While digital tools are used for public safety and health monitoring - such as location tracking during the COVID-19 pandemic - there is growing concern over how these tools are applied. Intelligence agencies have been accused of surveilling journalists, Indigenous leaders, and Non-governmental Organisations (NGOs) without clear legal justification. These groups often face heightened scrutiny, especially when advocating for environmental protection or Indigenous rights. Brazil's legal framework for data privacy is still developing, and enforcement remains inconsistent. The lack of transparency and oversight allows surveillance to be weaponised against civil society, raising alarms about the erosion of democratic accountability. Brazil shows how fragile democracies risk sliding into surveillance misuse when institutions are weak.

Somalia

Somalia represents the challenges of countries with little to no digital surveillance infrastructure. Weak state capacity, poor connectivity, and ongoing conflict mean the government cannot systematically monitor communications or public spaces. While this lack of surveillance avoids mass privacy intrusions, it leaves the population vulnerable to terrorism, cybercrime, and disinformation campaigns with no protective oversight. Somalia illustrates the other side of the debate - that weak surveillance capacity in fragile states can create security gaps and instability, raising the question of how global standards should address both "too much" and "too little" surveillance.

European Union (EU)

The European Union has positioned itself as a leader in data protection and privacy rights. Regulations such as the General Data Protection Regulation (GDPR) set global standards for the ethical handling of personal data. However, EU member states have varying surveillance practices, and balancing national security with civil liberties remains a contentious issue. The European Court of Human Rights and the Court of Justice of the European Union have struck down multiple surveillance laws that violate privacy rights, reinforcing legal boundaries. Still, cooperation with international intelligence alliances, including sharing data with the U.S., complicates the EU's moral stance.

Five Eyes Alliance

Comprising the United States, the United Kingdom, Canada, Australia, and New Zealand, the Five Eyes is one of the most comprehensive intelligence-sharing alliances in the world. Originally formed for military communications, it has evolved into a powerful mechanism for global digital surveillance. Leaked documents have shown that the alliance operates beyond national boundaries, often bypassing domestic legal restrictions by sharing data with partners. The Five Eyes have faced criticism for enabling mass surveillance while undermining transparency and public accountability. The alliance exemplifies how cooperative security frameworks can amplify surveillance power, raising.

Previous attempts to solve the issue

USA Freedom Act (2015)

After the Snowden Leaks (2013) revealed global surveillance by the NSA and its partners, public debates were catalysed and led to various legal reforms in the U.S, one of them being the USA Freedom Act of 2015,[34] which ended metadata collection. However, many loopholes remain. The USA Freedom Act addressed bulk collection of phone metadata by the NSA and introduced a system where companies retained the data, and government access required a court order. It raised unprecedented public awareness globally and sparked similar debates in Europe and other democracies. It is considered partially effective, as some surveillance practices were limited while many others continued under different legal systems and frameworks.

The General Data Protection Regulation (GDPR, 2018)

The GDPR in the EU is one of the most robust data protection laws. It mandates informed consent, limits data storage, and ensures user rights. Yet, its enforcement is inconsistent across member states. As a final result, it introduced strong data rights for EU citizens, including the "right to be forgotten" and data breach notifications. It was highly effective as a legal framework - but implementation varies widely. Wealthier EU nations enforce it better than others, and large tech companies often find ways to delay compliance.[35]

[34] Billings, Arielle. "International Association of Privacy Professionals." Iapp.org, 16 June 2015, iapp.org/news/a/the-usa-freedom-act-explained.

[35] European Council. "The General Data Protection Regulation." *Consilium*, 13 June 2024, www.consilium.europa.eu/en/policies/data-protection-regulation/

The United Nations Human Rights Council

The UNHRC has repeatedly raised concerns about surveillance, calling for international frameworks to prevent abuse, though without binding resolutions. Several resolutions were adopted, including the 2013 and 2016 resolutions on "The Right to Privacy in the Digital Age." [36] These efforts brought digital privacy into formal human rights discourse and pressured some states to review their surveillance laws. On the other hand, the resolutions are non-binding, lack enforcement, and are often ignored by powerful surveillance-heavy nations.

Possible solutions

Global Framework for Ethical and Accountable AI Surveillance

A strong and balanced solution would be to create an international framework for ethical AI surveillance, bringing together clear global standards and legal safeguards. This framework would require that AI technologies used in surveillance - like facial recognition, data scraping, or emotion detection - be independently audited to check for bias, unfair targeting, and lack of transparency. Governments would need to publicly explain how these systems work, what data they rely on, and what steps have been taken to avoid harm. A dedicated body within the United Nations Educational, Scientific and Cultural Organisation (UNESCO) could be set up to oversee and certify that systems meet ethical standards. Building on models like the European Union's General Data Protection Regulation (GDPR), the framework would also set out legal conditions for surveillance: it must be clearly defined by law, used only when necessary for public safety or national security, approved by independent bodies, and limited in time. This approach would help ensure that surveillance is carried out responsibly and doesn't come at the cost of human rights, while also giving countries a shared foundation for how to use powerful technologies in a fair and accountable way.

Annual Global Surveillance Review

Establish a UN-mandated annual reporting mechanism in which member states are required to submit detailed disclosures of their surveillance activities. These reports would include information

[36] *RIGHTS in the DIGITAL AGE CHALLENGES and WAYS FORWARD OECD DIGITAL ECONOMY PAPERS*. www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/rights-in-the-digital-age_d3a850de/deb707a8-en.pdf.

on what data is being collected, the technologies being used (including AI-based systems), the purpose of data collection, and any partnerships with private companies or foreign governments. The process would be overseen by an independent panel under the UN Office of the High Commissioner for Human Rights (OHCHR), to promote transparency and discourage abuse. While compliance would initially be voluntary, the mechanism could be strengthened through diplomatic pressure or made a condition for receiving international aid or digital infrastructure funding.

Surveillance Transparency Laws

Encourage national governments to enact legislation that compels law enforcement and intelligence agencies to publish regular transparency reports. These laws would mandate disclosure of the number of surveillance requests made, the legal justifications used, the types of data collected, and any known data breaches or misuse. Reports would also indicate whether surveillance targets were domestic or foreign, and whether oversight mechanisms (such as parliamentary review) were followed. Transparency laws aim to foster trust between the public and state institutions and are especially relevant in democratic states, and can be adopted progressively by other countries as international norms evolve.

UNESCO-led Global Digital Education Programme

Launch an international public education campaign - led by UNESCO and supported by NGOs such as Privacy International - to raise awareness about digital privacy and mass surveillance. By being led by UNESCO, the programme can be internationally recognised and UNESCO-led efforts often involve global networks - such as the UNESCO Associated Schools Network or World Heritage community, which would make for a more effective educational programme. This initiative would involve creating school curricula, interactive online workshops, and community outreach programs that educate people about their digital rights, how their data is collected, and tools they can use to protect their privacy (e.g., Virtual Private Networks (VPNs), privacy browsers). The program would focus especially on youth, marginalised communities, and those living under repressive regimes where digital surveillance is most harmful. Education is vital to empowering citizens to demand accountability and make informed decisions in the digital age.

Bibliography

Abbasi, Omar. "Artificial Intelligence at Airports - Revolutionising Airport Management." Embross | Passenger Self Service, 2 Feb. 2024 https://www.embross.com/blog/artificial-intelligence-at-airports-revolutionizing-airport-management/

Akpobome, Omena. (2024). *The Impact of Emerging Technologies on Legal Frameworks: A Model for Adaptive Regulation.* International Journal of Research Publication and Reviews. https://ijrpr.com/uploads/V5ISSUE7/IJRPR31902.pdf

Barriga, Antónia do Carmo, et al. "The COVID-19 Pandemic: Yet Another Catalyst for Governmental Mass Surveillance?" *Social Sciences & Humanities Open*, vol. 2, no. 1, 2020. https://www.sciencedirect.com/science/article/pii/S2590291120300851

BBC News. "Edward Snowden: Leaks That Exposed US Spy Programme." BBC News, 17 Jan. 2014. https://www.bbc.com/news/world-us-canada-23123964

Billings, Arielle. "International Association of Privacy Professionals." *Iapp.org*, 16 June 2015

"Big Data in the Fight against Terrorism: Is Mass Surveillance Ethically Justifiable?" *Uni-Wh.de*, 2024 https://www.uni-wh.de/en/big-data-in-the-fight-against-terrorism-is-mass-surveillance-ethically-justifiable

Boffey, Daniel, and Mark Wilding. "Live Facial Recognition Cameras May Become 'Commonplace' as Police Use Soars." *The Guardian*, 24 May 2025 https://www.theguardian.com/technology/2025/may/24/police-live-facial-recognition-cameras-england-and-wales

Cambridge Dictionary. "Data Scraping." *CambridgeWords*, 17 May 2023

Cambridge Dictionary. "PRIVACY | Meaning in the Cambridge English Dictionary." *Cambridge.org*, 2019

Cambridge Dictionary. "Sunset Clause." *CambridgeWords*, 9 July 2025

College of Policing. "Closed-Circuit Television (CCTV)." *College of Policing*, 19 Feb. 2021 https://www.college.police.uk/research/crime-reduction-toolkit/cctv

Deighton Pierce Glynn. "European Court of Human Rights Declares UK's Mass Surveillance Regime Unlawful." *DPG Law*, 13 Sept. 2018

https://dpglaw.co.uk/european-court-of-human-rights-declares-uks-mass-surveillance-regime-unlawful/

"Ethiopia: New Spate of Abusive Surveillance." *Human Rights Watch*, 6 Dec. 2017 https://www.hrw.org/news/2017/12/06/ethiopia-new-spate-abusive-surveillance

European Commission. "Data Protection." *Commission. Europa.EU*, 2024 https://commission.europa.eu/law/law-topic/data-protection_en

European Council. "The General Data Protection Regulation." *Consilium*, 13 June 2024 https://www.consilium.europa.eu/en/policies/data-protection-regulation/

"Facial Recognition Technology | Homeland Security."

Feldstein, Steven. "The Global Expansion of AI Surveillance." *Carnegie Endowment for International Peace*, 17 Sept. 2019 https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance?lang=en

Hardesty, Larry. "Study Finds Gender and Skin-Type Bias in Commercial Artificial-Intelligence Systems." *MIT News*, Feb. 2018 https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212

"How Mass Surveillance Works in Xinjiang | The Xinjiang Data Project." *Aspi.org.au*, 2018https://xjdp.aspi.org.au/explainers/how-mass-surveillance-works-in-xinjiang/

Human Rights Watch. "Myanmar: Facial Recognition System Threatens Rights." *Human Rights Watch*, 12 Mar. 2021 https://www.hrw.org/news/2021/03/12/myanmar-facial-recognition-system-threatens-rights

"Intelligence Gathering - an Overview | ScienceDirect Topics" https://www.sciencedirect.com/topics/computer-science/intelligence-gathering

Liberty. "SNOOPERS' CHARTER." *Liberty https://www.libertyhumanrights.org.uk/fundamental/mass-surveillance-snoopers-charter/*

Martin, Roland. "Closed-Circuit Television | Meaning, Camera, System, History, & Facts | Britannica." https://www.britannica.com/technology/closed-circuit-television

"Mass Surveillance." *European Parliament*, www.europarl.europa.eu/...

"MASS SURVEILLANCE Collocation | Meaning and Examples of Use." *CambridgeWords*, 25 Sept. 2024 https://dictionary.cambridge.org/example/english/mass-surveillance

Merriam-Webster. "Definition of METADATA." *Merriam-Webster.com*, 2019

Muhammad Tuhin. "The Dark Side of AI: Bias, Surveillance, and Control." *Science News Today*, 24 Apr. 2025 https://www.sciencenewstoday.org/the-dark-side-of-ai-bias-surveillance-and-control

Oluwatoni Olujinmi. "Geolocation Tracking, All the Risks Connected to It." *World Excellence International*, 27 Apr. 2023 https://www.worldexcellence.com/geolocation-tracking-risk/

RIGHTS in the DIGITAL AGE: CHALLENGES and WAYS FORWARD. *OECD Digital Economy Papers*, 2022 https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/rights-in-the-digital-age_d3a850de/deb707a8-en.pdf

"Six Years after the Snowden Revelations, the Fight against Bulk Surveillance Continues – Digital Freedom Fund." *Digital Freedom Fund*, 2023 https://digitalfreedomfund.org/six-years-after-the-snowden-revelations-the-fight-against-bulk-surveillance-continues/3/

Stedman, Craig. "What Is Data Mining?" *TechTarget*, Sept. 2021

Stedman, Craig. "What Is Data Mining?" *TechTarget*, Sept. 2021 *(duplicate)*

"Surveillance andPrivatisingg National Security – GIS Reports." *GIS Reports*, 20 June 2025

"The Power and Limits of AI in Predicting Human Actions." *DataScience next Conference*, 18 Mar. 2025

UNESCO. "Ethics of Artificial Intelligence." *UNESCO* *https://www.unesco.org/en/artificial-intelligence/recommendation-ethics*

University of Michigan. "History of Surveillance Timeline / Safecomputing.umich.edu." *University of Michigan*, 2024

Wikipedia Contributors. "Investigatory Powers Act 2016." *Wikipedia*, Wikimedia Foundation, 11 July 2019

Wu, Tony, et al. "The Ethics (or Not) of Massive Government Surveillance." *Stanford.edu*

YANG, Sihan, et al. “The Impact of Surveillance Cameras and Community Safety Activities on Crime Prevention: Evidence from Kakogawa City, Japan.” *Sustainable Cities and Society*, Sept. 2024