



Human Rights Commission

Question of: Addressing the Impact of AI Surveillance Expansion
on Privacy and Freedom of Speech in China

President

Introduction

The rapid expansion of artificial intelligence (AI) surveillance technologies has raised concerns regarding individual privacy and freedom of speech, particularly in many authoritarian states such as the People's Republic of China. The Chinese government has increased its ability to monitor and control its population through the integration of AI facial



recognition, data tracking, and predictive policing systems into everyday life. This trend has sparked intense global debate about the balance between national security, technological innovation, and fundamental human rights.

AI surveillance is broadly defined as the use of artificial intelligence to analyze data collected from digital and physical environments to monitor individuals or groups. In China, this includes CCTV (Closed-Circuit Television) networks, biometric data collection, and AI algorithms that track online speech and behavior. The historical roots of this issue trace back to the rise of mass surveillance under the Chinese Communist Party, that mainly followed the 2009 Urumqi riots and the 2013 "Sharp Eyes" project. These initiatives marked the beginning of a more centralized, enhanced AI surveillance infrastructure. The main concerns behind expansion of AI surveillance in China is not just a technological development, it also represents a deeper social and political shift. Surveillance tools are used to suppress dissent, limit free speech, and maintain strict governmental control over citizens. Citizens are monitored in real-time through facial recognition in public spaces, online activity is tracked, and social media platforms are heavily censored. The issue extends beyond China's borders as these surveillance technologies are increasingly exported to other nations, raising concerns about the global spread of digital authoritarianism and its affect on freedom of speech and digital privacy. Addressing this issue is essential to ensure that technological advancements aren't abused for some sort of authority but to empower people and not to silence or monitor them.

This topic closely aligns with the theme "*Deliberate to Liberate*" since it calls on the international community to thoughtfully and collectively address the ethical sides of AI

surveillance and deliberate on effective solutions to safeguard civil rights. The global community can work toward liberating individuals from excessive state control and protecting the fundamental rights to privacy and free expression by promoting transparency and legal accountability.

Definition of Key Terms

Separatist:

Separatist: A person, group, or movement that seeks to break away from a larger political entity to form an independent state or gain autonomy. This refers to groups in regions like Xinjiang, and Hong Kong advocating for independence or self-rule.

Sentiment:

Sentiments: Refers to feelings, attitudes, or opinions held by people. In this context, separatist sentiments describe the public feelings or support for separation, autonomy, or resistance against the central government's control.

Cyber Sovereignty Doctrine:

The **Cyber Sovereignty Doctrine** is a principle promoted by China, asserting that each country has the right to govern and control its own internet infrastructure, data, and online activities without external interference. Under this doctrine, the Chinese government argues that state sovereignty extends to cyberspace, which allows China to censor information, control tech companies, and regulate digital platforms according to its national interests and values.

Artificial Intelligence (AI)

Artificial Intelligence (AI) refers to computer systems or machines that can perform tasks normally requiring human intelligence, such as recognizing patterns, learning from data, and making decisions.

Facial Recognition Technology

Facial Recognition Technology is a type of biometric system that uses AI to identify or verify a person by analyzing their facial features from images or videos.

Biometric Tracking

Biometric Tracking involves collecting and using unique biological data (such as fingerprints, facial features, or DNA) to identify and monitor individuals.

In China, biometric data like facial scans and fingerprints are collected, which enables the government to monitor ethnic minorities continuously.

Golden Shield Project

The Golden Shield Project, also known as the “Great Firewall of China,” is a government initiative started in 1998 to build a nationwide internet censorship and surveillance system. It laid the foundation for today’s AI-driven surveillance by blocking access to certain foreign websites and monitoring online content, helping control information flow within China.

International Sanctions

Penalties or restrictions imposed by one or more countries against entities or nations to influence behavior, often in response to human rights abuses or security concerns. The U.S. and others have sanctioned Chinese surveillance companies like Hikvision over alleged abuses in Xinjiang, which limited their access to international markets.

General Overview

Currently In the 21st century, rapid advancements in Artificial Intelligence (AI) have revolutionized surveillance capabilities which empowered governments with new tools of monitoring their populations. In China, the state has built one of the most advanced AI surveillance infrastructures globally. By 2020, China accounted for approximately 54% of the world’s surveillance cameras, with over 415 million cameras installed nationwide, according to Comparitech. These include facial recognition, video analytics, and biometric tracking. Chinese authorities claim that these technologies enhance public safety and social harmony, yet human rights advocates argue that they are systematically taking away civilian's privacy and suppressing freedom of speech. Particularly concerning the use of AI surveillance to monitor and suppress ethnic minorities in regions like Xinjiang, silence pro-democracy activists in Hong Kong, and regulate online speech across the country.

History

China's surveillance infrastructure has evolved significantly over the past two decades. Its roots can be traced back to the **Golden Shield Project**, launched in 1998, which aimed to build a nationwide surveillance and censorship system. By the early 2010s, the rise of AI technologies allowed the government to expand these efforts rapidly. The introduction of **facial recognition** in 2015, developed by companies such as Hikvision and Sense Time, transformed the country's public surveillance capabilities. Surveillance cameras were installed across streets after the year 2015 including in public spaces and transportation hubs, which allowed for vast monitoring and improved tracking of individuals in everyday environments.

The development of the **Social Credit System**, piloted in 2014 and implemented across several provinces by 2018, also further integrated AI surveillance with personal data collection, assigning citizens scores based on their behavior online and offline.

Some notable examples include the monitoring of **pro-democracy activists in Hong Kong (2019–2020)** and the surveillance of **Uyghur Muslims**, where advanced AI systems are used to track religious and ethnic minorities, which shows how these technologies are used beyond crime prevention.

Causes of the problem

There are many major factors that have driven China's expansion of AI surveillance. The primary motivator is state control **and political stability**. The Chinese Communist Party (CCP) views surveillance as vital for maintaining political authority and preventing social unrest. In regions like Xinjiang and Tibet, where separatist sentiments exist, AI strictly tracks behavior, monitors religious practices, and suppresses dissent under the guise of counter-terrorism.

Another major cause is technological ambition. China's drive to become a global AI superpower is another key cause. Under the New Generation Artificial Intelligence Development Plan (2017), China has committed significant resources to AI research and development. Surveillance technology is one of the most advanced and commercially successful applications of this AI drive, which positions China as both a technological leader and exporter.

Domestically, the success of AI-powered surveillance showcases China's

technological progress and demonstrates the government's ability to translate research into practical, and real-world governance tools. Surveillance systems powered by AI also contribute to China's ambitions in fields such as smart cities, national security, and industrial automation, which reinforce its status as an innovation hub.

However, this technological ambition is not purely economic or scientific it also serves strategic geopolitical interests. China is enhancing its internal security while setting standards in emerging global markets and often challenging Western dominance in technology governance through mastering surveillance technologies.

China's "**Cyber Sovereignty**" doctrine promotes strict state control over cyberspaces. Authorities justify monitoring online speech and communications as a way to safeguard national security and "social harmony". This ideology drives censorship, data collection, and surveillance algorithms that control online access and speech.

This doctrine enables internet censorship through mechanisms like the Great Firewall, which blocks access to foreign websites and filters domestic content that challenges state narratives. Even social media platforms, search engines, and messaging apps operating in China are required to comply with strict government regulations, facilitating real time content filtering and the takedown of politically sensitive material.

Moreover, the Cyber Sovereignty works on mass collection of user data from online interactions, creating large databases that feed surveillance algorithms. These algorithms monitor trends in public sentiment, track the spread of ideas, and identify individuals or groups deemed threats to political stability.

As well as social governance efficiency .Surveillance is deemed as a critical tool to enhance social governance and efficiently manage China's vast and densely populated urban areas. The Chinese government integrates artificial intelligence (AI)-powered surveillance systems into law enforcement, urban management, and public services. These systems are used to monitor traffic, crime, and social behaviors, creating what authorities present as a safer society. However, this comes at a cost to personal privacy and individual freedoms. Advanced surveillance normalizes monitoring, limits civil liberties, and violates rights like freedom of speech

Impacts of the Problem

The expansion of AI surveillance in China has had many effects on individual freedoms. For instance, Privacy Erosion. Citizens in China face constant monitoring of

their movements and online activities. Studies estimate that Chinese urban residents are filmed **hundreds of times daily**, leading to a significant loss of personal privacy.

The government uses AI algorithms to filter and censor online content while mainly targeting politically sensitive discussions. Social media platforms like WeChat are heavily monitored, with users facing account detentions or legal action for expressing dissent. This surveillance extends to private chats and group discussions, creating an environment of self-censorship among citizens. Even humor, satire, or vague references to political issues can trigger censorship algorithms and lead to punishing measures.

In Xinjiang, over **1 million Uyghurs** have reportedly been subjected to constant biometric surveillance and data profiling, further marginalizing these communities. These measures are justified by authorities as counter-terrorism efforts, although human rights organizations describe them as systemic repression. The resulting environment severely limits religious practices, cultural expression, and personal freedoms within these minority groups.

The Social Credit System penalizes citizens for behaviors that are considered undesirable, such as criticizing the government online or associating with activists, restricting their ability to travel, find employment, or access public services in their own country. This system assigns numerical scores to individuals based on their compliance with social and legal norms, with low scores resulting in penalties. Surveillance data from public spaces, online activity, and financial behavior feed into these scores, which promotes the constant monitoring of personal behaviors.

International Response

The global response to China's AI surveillance expansion has been mixed, which reflected geopolitical tensions and concerns about human rights.

Some western democracies, including the United States, United Kingdom, and the European Union, have criticized China's surveillance practices, particularly in Xinjiang as they labeled them as violations of human rights. The U.S. has imposed sanctions on Chinese companies in response, such as Hikvision and SenseTime, and restricted their access to American technology.

International human rights organizations like Amnesty International and Human Rights Watch have condemned the repression enabled by surveillance, urging the UN and international bodies to investigate.

However, some countries have adopted or purchased Chinese surveillance technologies, particularly in Africa, the Middle East, and Southeast Asia, due to their cost effectiveness and efficiency. This growing export of AI surveillance tools has raised concerns about the global spread of authoritarian tech governance.

At the United Nations, efforts to address AI surveillance have included discussions in the Human Rights Council and the Third Committee yet international agreements on regulating AI surveillance remain limited.

Major Parties Involved

The People's Republic of China (PRC)

The People's Republic of China (PRC) is the primary driver of AI surveillance expansion within its borders. The Chinese government has implemented extensive surveillance technologies such as facial recognition, voice recognition, and online data monitoring, which is justified as measures to maintain national security and social stability. The PRC has passed laws like the Cybersecurity Law (2017) and Data Security Law (2021) that allow the government's authority to access personal data.

Chinese Communist Party (CCP):

The Chinese Communist Party (CCP) is the founding and ruling political party of the People's Republic of China (PRC). It holds absolute power over the Chinese government and military. The CCP establishes national policies, controls the state apparatus, and oversees all levels of government, including surveillance and censorship programs. It plays a role in shaping China's stance on privacy, security, and political expression.

United Nations Human Rights Council (UNHRC)

The United Nations Human Rights Council (UNHRC) has showed concern over China's surveillance practices, particularly regarding their impact on privacy and freedom of expression. Many UN Rapporteurs have called on China to respect the right to privacy, especially in regions like Xinjiang, where surveillance is used to monitor ethnic minorities. The UNHRC has raised the issue of digital rights violations and emphasized that surveillance must comply with international human rights law.

Amnesty International

Amnesty International has actively documented and reported on China’s AI-driven surveillance systems and their negative impact on human rights. The organization published detailed investigations exposing how these technologies are used for mass surveillance. They regularly establish public campaigns and call for international action against the misuse of AI surveillance technologies. It also urges governments and international bodies to impose sanctions on companies providing surveillance technology used in human rights violations.

United States of America (USA)

The USA has imposed export restrictions and sanctions on Chinese technology companies such as Hikvision and Dahua, which supply surveillance systems. The US used platforms like the UN and the G7 to advocate for global standards in protecting digital rights and privacy. Moreover, the USA promotes initiatives like the Clean Network Program to block Chinese surveillance technologies from being adopted by other countries.

Human Rights Watch (HRW)

Human Rights Watch (HRW) is a non-governmental organization (NGO) that has published numerous reports regarding the abuse of AI surveillance in China. HRW has raised concerns about the Chinese government's use of surveillance to suppress dissent, control information flow, and monitor social behavior. The organization has called on tech companies to cease providing technology that enables human rights abuses in China. It also works with international bodies like the UN (United Nations) and the EU (European union) to advocate for stronger policies protecting privacy and free speech globally.

Timeline of Events

Date	Event
2004 / Month / Day	China pilots the national Grid-style social management project in Beijing’s Dongcheng District, rolling out neighborhood "grid watchers" and integrating them with CCTV networks. The

project allowed for micro level reporting of citizen activities. The use of surveillance into daily life was normalized during this period.

2006

China Launches **Project Skynet**, deploying CCTV surveillance nationwide later rebuilt with facial recognition. It improved neighborhood monitoring but raised concerns about personal privacy. This became one of the largest public surveillance systems in the world. It significantly expanded state surveillance capacity beyond just local projects. The skynet's infrastructure became the backbone for later AI surveillance.

2012/ April / 3

Artist Ai Weiwei initiated **WeiweiCam**, live streaming for webcams at his Beijing studio to highlight government surveillance, then, authorities shut it down after two days. The event sparked international debates on privacy and censorship. Making it a cultural symbol of resistance to state surveillance. It highlighted artistic activism against AI surveillance.

2014/ January

Mandatory legal name registration for any online video that is uploaded is enforced by the State Administration of Press, Publication, Radio, Film and Television. This intensified censorship on social media platforms. It linked digital identities directly to individuals. Content moderation systems were automated and scaled up. The move decreased anonymous speech online.

2016/ November / 7

The expansion of Xinjiang "Strike Hard" surveillance

campaign began, and authorities deployed facial recognition smart glasses and

targeting tools like the "Uyghur alarm." This marked one of the most intense AI-driven surveillance campaigns globally. Facial recognition specifically targeted ethnic minorities. Smart glasses allowed for portable surveillance. The campaign became a symbol of racialized surveillance practices.

2017/ June/ 1 The **Cybersecurity Law** is passed and applied, which allowed for state powers to collect personal data. It legally mandated compliance for foreign and domestic tech firms. The law enforced stricter censorship methods. Many citizens called it a step toward an authoritarian internet.

2018/ November Xinhua introduced the world's first AI news anchor at the Wuzhen World Internet Conference. Supporters said it made news delivery faster and more efficient. But critics said it could make news less trustworthy.

Moreover, police in Beijing and Zhengzhou started using smart glasses with facial recognition during public events. This expanded the government's surveillance abilities. The officers could quickly identify people in crowds using the glasses.

2021/ June/ 10 The Data Security Law brought stricter rules for how data is classified and monitored. It was created to stop data misuse and protect China's control over its own data. The law made handling sensitive information much more controlled. Big international companies struggled to follow these new rules. At the same time, privacy groups

asked for better protection of people's personal data.

2021/ November/ 1

The Personal Information Protection Law (PIPL) was introduced, which made it necessary to get consent

before collecting biometric data. This was China's first major privacy law. It was

partly based on the EU's GDPR (The General Data Protection Regulation) rules, but

some people questioned how well it would be enforced. Civil society groups agreed

with the law's goals but worried that the Chinese government might not fully apply

it.

2023/ August

The Cyberspace Administration of China (CAC) launched a public consultation on new facial recognition rules. The draft explained how the technology could be used legally. It required companies to get user consent and be more transparent. While the rules tried to stop businesses from misusing facial recognition, they still allowed the government powers to use it.

2024/ September/ 30

The Cyberspace Administration of China (CAC) officially approved new rules for facial recognition technology. These rules required companies to get users' permission, be clear about how they use the data, and keep it safe. This was the first detailed set of laws to manage facial recognition. The goal was to protect people's privacy while still allowing businesses to use the technology. The new rules came after more people started

worrying about how facial recognition is being used.

Attempts to solve the issue

[United Nations General Assembly Resolution 68/167 – The Right to Privacy in the Digital Age, 18 December 2013 \(A/RES/68/167\)](#)

This resolution reaffirms that the right to privacy is a fundamental human right in the digital era. It calls on states to review their surveillance laws, ensure legality, necessity, and proportionality.

[UNGA Resolution 78/213 – Promotion and Protection of Human Rights in the Context of Digital Technologies 22 December 2023 \(A/RES/78/213\)](#)

This resolution emphasizes that human rights apply equally offline and online, urging member states to strengthen protections for privacy and freedom of expression. It encourages national policy reviews and the adoption of governance frameworks consistent with human rights obligations.

[UNGA Resolution A/78/L.49 – Seizing the Opportunities of Safe, Secure and Trustworthy AI Systems 21 March 2024 \(A/RES/78/L.49\)](#)

This was the UN's first resolution on AI, calling for human rights based regulation of AI systems, data privacy safeguards and international cooperation on AI governance. Gaining unanimous support from 121 states including China and the U.S, it created global political momentum around ethical AI, informing national AI strategies.

Possible Solutions

Encourage governments and relevant UN bodies to implement strict data privacy laws limiting the misuse of AI surveillance data. Implementing strict data privacy laws would help protect citizen's personal data from being misused by AI surveillance system. These laws would ensure that collected data is only used for lawful purposes, such as national security or crime prevention, and not for suppressing free speech. Additionally, clear penalties for violations would discourage government agencies and private companies from exploiting surveillance data. This promotes a safer and more transparent digital environment where people's rights are protected.

Promote the creation of independent oversight bodies to monitor AI surveillance

practices and protect citizens' rights.

Independent oversight bodies would regularly review how AI surveillance technologies are used and ensure they follow privacy laws. These organizations would be separate from the government to prevent bias and corruption. They could handle complaints from citizens and investigate potential abuses of surveillance systems. These oversight bodies would help build public trust in the use of surveillance technology by creating accountability.

Urge international organizations and NGOs to raise awareness about the risks of AI surveillance on freedom of speech through educational campaigns.

Raising awareness about the risks of AI surveillance can help citizens understand how their freedom of speech is impacted. Educational campaigns led by NGOs and international organizations could inform the public about how surveillance technology works and its possible misuse. These campaigns could also highlight the importance of protecting privacy rights in the digital age. Through this, people are empowered to advocate for their own rights and call for better privacy protections.

Encourage governments and technology providers to enforce limitation and data minimization in AI surveillance systems.

Enforcing purpose limitation ensures that AI surveillance tools only collect and process personal data for lawful objectives, such as national security or crime prevention. This prevents the use of surveillance technology for political monitoring, suppression of dissent, or tracking personal beliefs and opinions. Data minimization policies would require surveillance systems to collect only the smallest amount of information necessary to achieve their lawful purpose, reducing the risk of privacy violations. Together, these measures create clear legal and technical limits on what surveillance systems can do which protects citizens' privacy and freedom of speech from unnecessary invasion of privacy.

Guiding Questions

1. What AI surveillance technologies are currently being used in China?
2. How has AI surveillance in China impacted individual privacy rights and freedom of speech?
3. What laws or government policies in China support or restrict AI surveillance

practices?

4. How do Chinese citizens and international human rights organizations view the use of AI surveillance in China?
5. What are some recent examples of surveillance-related crackdowns on free speech or political dissent in China?
6. How does China's AI surveillance compare to surveillance practices in other countries (e.g., the US, Russia, EU nations)?
7. What international laws, treaties, or declarations (e.g., Universal Declaration of Human Rights) address privacy and freedom of speech in the context of surveillance?
8. What are the ethical concerns raised by the global community regarding the expansion of China's AI surveillance?
9. How has AI surveillance in China influenced or limited digital activism and online dissent?
10. What is the role of censorship algorithms and content moderation AI in restricting free speech on Chinese social media platforms?

Appendix

- <https://www.ohchr.org/en/statements/2021/06/china-must-respect-human-rights-says-un-rights-chief>
- <https://www.amnesty.org/en/documents/asa17/4137/2021/en/>
- <https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance>
- <https://freedomhouse.org/country/china/freedom-net/2023>
- <https://www.accessnow.org/issue/artificial-intelligence/>
- <https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list>
- <https://www.technologyreview.com/2019/10/08/132829/china-ai-surveillance-export-privacy-human-rights/>
- <https://rsf.org/en/country/china>
- <https://thediplomat.com/2020/03/the-global-spread-of-chinas-surveillance-technology/>

Bibliography

Apuzzo, Matt, and David Pierson. "All Eyes on Surveillance: How China Harnesses Data-Fusion to Make Sense of Surveillance Data." *Brookings*, Brookings Institution, <https://www.brookings.edu/articles/how-china-harnesses-data-fusion-to-make-sense-of-surveillance-data/>. Accessed 28 June 2025.

Chen, Adrian. "Surviving the Crackdown in Xinjiang." *The New Yorker*, 12 Apr. 2021, <https://www.newyorker.com/magazine/2021/04/12/surviving-the-crackdown-in-xinjiang>. Accessed 28 June 2025.

Digital Policy Alert. "China Publishes Draft Measures for the Safe Application of Facial Recognition Technology." *Digital Policy Alert*, 21 Mar. 2025, <https://digitalpolicyalert.org/event/29402-cyberspace-administration-issued-guidelines-clarifying-regulations-on-the-safe-application-of-facial-recognition-technology>. Accessed 28 June 2025.

HsFkramer. "China Releases Laws to Regulate the Use of Facial Recognition Technology." *HsFkramer.com*, 2021, <https://www.hsfkramer.com/notes/data/2025-posts/china-releases-laws-to-regulate-the-use-of-facial-recognition-technology>. Accessed 28 June 2025.

Metz, Cade. "How China Created an AI-Infused Surveillance Operation." *Wired*, Condé Nast, <https://www.wired.com/story/inside-chinas-massive-surveillance-operation/>. Accessed 28 June 2025.

"China Quietly Building a National Voiceprint Database to Allow Automated Speaker Recognition." *Private Internet Access Blog*, <https://www.privateinternetaccess.com/blog/china-quietly-building-national-voiceprint-database-allow-automated-speaker-recognition/>. Accessed 28 June 2025.

Reuters. "China Says Facial Recognition Should Not Be Forced on Individuals." *Reuters*, 21 Mar. 2025, <https://www.reuters.com/technology/china-says-facial-recognition-should-not-be-forced-individuals-2025-03-21/>. Accessed 28 June 2025.

South China Morning Post. "Skynet: China's Massive Video Surveillance Network Explained." *South China Morning Post*, <https://www.scmp.com/abacus/who-what/what/article/3028246/skynet-chinas-massive-video-surveillance-network>. Accessed 28 June 2025.

Time Staff. "China Is Building a National Voice Database to Strengthen Its Surveillance Powers." *Time*, 22 Oct. 2017, <https://time.com/4992849/china-voice-database-surveillance/>. Accessed 28 June 2025.

Contact Information

President: Ward Abualghanam

Phone number: +962 790977360

Email: ward_abualghanam@abs.edu.jo