December 2025

Vic Takavarasha, HRC Head Chair

Haganum Model United Nations XVI

Combating Digital Authoritarianism and Over surveillance

Human Rights Council (HRC)

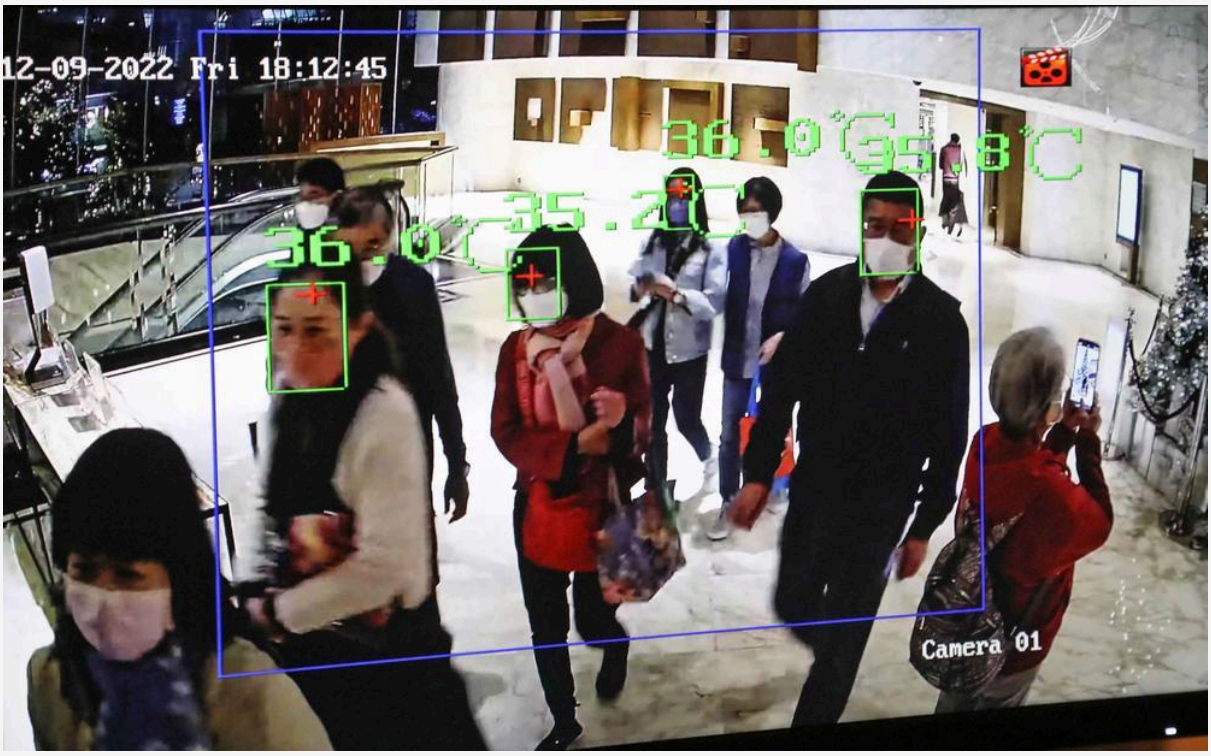

Table of Contents

Introduction

Technology has surely yet discretely reshaped our everyday lives. Through the means of technology we have been able to communicate faster, organise and manage large amounts of information, and keep people connected across nations in ways that were only dreams decades ago. Technological developments have brought numerous benefits globally, from economic growth and improved public safety to being able to watch videos or call a friend to fill time. However through all these amazing advances, a worrying issue has been slowly emerging.

As digital tools become more powerful and reliable, some countries have begun to use them to not just help citizens, but to monitor, control, and influence them. This issue is what we call digital authoritarianism. Digital authoritarianism relies on technologies such as centralized data systems, facial recognition, and internet censorship to control behaviour both in person and digitally and also limit disagreement on certain national opinions, ideologies, or systems. Over-surveillance has become increasingly common in both democratic and non-democratic countries, making the issue a very pressing and rather scary matter. Governments and institutions can now unfortunately collect, store, and analyse enormous amounts of personal data, and often with limited or no transparency.

These developments have raised serious concerns. When surveillance becomes excessive, it threatens the fundamental rights we have placed such as privacy, freedom of expression, access to information, and political participation. As surveillance technologies spread and improve globally and data analytics become more sophisticated, the challenge has gone way beyond national borders, increasing international attention.

At the centre of this issue lies a difficult question, how can we protect national security and order in the public without limiting individual's rights and freedom? This question alone makes digital authoritarianism and over-surveillance one of the most complex and pressing modern challenges today, and a critical topic for international debate and cooperation

Definition of key terms

Data privacy-

The protection of personal information and an individual's right to control who can obtain said information.

Data Integration-

The combining of data from multiple sources to create a more unified dataset

Authoritarian States-

A form of government in which power is concentrated in the hands of a single ruler or a small group. Citizens of authoritarian states usually have strict submission to authority, limited political freedom, and repression of individual rights.

Centralized Data Systems-

A system where all the information of an organisation is collected then managed and stored in a specific location or platform

Digital authoritarianism-

The use of digital information technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations.

Facial recognition technology-

Biometric technology that uses Ai to verify a person's identity by analyzing unique facial features. Commonly used for unlocking personal devices such as computers and phones, airport security, or law enforcement purposes.

Internet censorship-

The controlling and/or suppression of online information, content, or access by the government, organisations, or people. Usually used to restrict certain speech or ideologies, control narratives, or restrict inappropriate media

Mass surveillance-

The surveillance of an entire or large fraction of a population in order to monitor a group of citizens.

Metadata-

The descriptive information about data, such as time, location, source, file size, and etc.

Spyware-

Malware that is secretly installed onto a device to spy on activity for collection of personal data, such as passwords, bank and personal information,and browsing habits, to send it to attackers without the knowledge or consent of the device's owner.

General Overview

In recent years, the rapid expansion of digital technologies has changed the relationship between states and their citizens. Technology that once seemed so futuristic has become part of everyday governance systems, giving governments new ways to improve security, increase their efficiency, and manage public services. At the same time, these developments have introduced new issues in privacy, freedom of expression, and the balance between power the state and the individual.

Around the world, governments are starting to rely more on technologies such as facial recognition, biometric data bases, and artificial intelligence to monitor populations on a scale that would have been difficult to visualise a decade ago. In authoritarian states these tools often come along with strict internet regulation and online monitoring. This allows for authorities to exert significant influence over public information, and political discourse. For example using systems to monitor communications, or shutting down internet access during times of protest in order to manage unrest and limit the flow of information.

Private technology companies play quite a role in this modern issue, as they design, develop, and supply the digital infrastructure that makes modern surveillance possible. Luckily, investigative journalists, and academic researchers have taken the role of overseers. Questioning and assuring these companies do not violate the rights of individuals. Through their reports, advocacy, and public campaigns, they document abuses, and push for greater transparency and accountability.

In response to these pushes, the international community has attempted to establish norms and protections through legal and institutional frameworks such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and resolutions adopted by the United Nations Human Rights Council. Despite these efforts, significant challenges still remain. Rapid technological advancement continues to surpass regulations, and nations must go through the hard task of maintaining public order and national security without undermining the rights of their people.

As a result, the issue of digital surveillance is not one that comes with a clear answer, but instead with finding the balance between innovation , security, global cooperation, and national sovereignty.

Major Parties Involved

China-

Due to their extensive development and use of state-led digital surveillance and governance systems, China is widely known for being the center of discussion when it comes to digital authoritarianism. Since the early 2000s, following the rapid technological expansion in the 2010s, China has been investing heavily in surveillance infrastructure and technology, including facial recognition, large-scale data integration, online censorship, and regulation of which online platforms can be used by their citizens. The Chinese government says these measures are to maintain social stability, public security, and efficient governance. However, internationally, China's approach has drawn some negative attention in UN forums such as HRC and OHCHR due to the fact that China's digital surveillance has been seen as excessive and a violation of privacy and freedom of speech. This discussion over China's digital governance has had a great influence on global debates over the balance between state sovereignty, technological development, and an individual's privacy. China's interest in this issue remains in protecting its right to regulate digital spaces without external interference.

Russia-

Russia is another major party involved in the issue, particularly due to its increasing regulation of digital spaces and its developments on its capabilities in online surveillance. Since the early 2010s, Russia has set laws strengthening its control over internet framework, data storage, and online content, often stating the reason for these laws is due to better national security and political stability. With Russia's periods of political unrest and geopolitical tensions, digital surveillance has become a key component of national security policy. However, there are concerns over targeted suppression on freedom of expression, activists, journalists, and privacy that have been expressed by HRC and western states. Russia's position prioritises state sovereignty over information and resistance to what it views as "external influence" through digital spaces.

Iran-

Iran has frequently been involved in discussions on over-surveillance due to its monitoring of digital communications and its internet shutdowns. Since the late 2000s, following the protest movements, Iran has focused on strengthening online surveillance and censorship to limit political disagreement and maintain internal stability. These actions are often justified as a way to protect national security and cultural protection. But Iran has faced international backlash for their surveillance practices being rather extensive and a breach on human rights. However Iran's interest in the issue remains on keeping governmental control over digital communication while opposing any foreign comment that it is seen as a threat upon its national sovereignty.

Private Technology and Surveillance Companies-

Private technology companies are major non-state parties involved in this issue due to their control and ownership over digital platforms, data storage, and surveillance technologies. Since the rapid growth of the digital economy in the early 21st century, technology firms have gathered huge amounts of personal data and developed advanced tools to better analyze this data. Surveillance technology companies provide governments with spyware and facial recognition software. While these firms often do operate within the legal frameworks, their products have been linked to misuse by state authorities or individuals, raising concerns over who is accountable in situations like these and how we can better regulate such technology. Private technology and surveillance company's interests lie in maintaining their access and strength in global markets while working with and satisfying the increasing calls for transparency and ethical responsibility.

Technologically Developed Countries-

Technologically developed countries such as Canada, the United States, United Kingdom, EU member states, Israel, Japan, South Korea, and Australia constitute a major deal in the issue of digital authoritarianism and over-surveillance. These states are all well developed in terms of digital infrastructure, intelligence capabilities, and unlimited access to large-scale data collection technologies. Due to the increased global security concerns, since the early 2000's many of these states have expanded their surveillance programs involving metadata, online monitoring, and cooperation between governments and private technology companies. Similar to China, Russia and Iran, these developments and measures are justified by the need for national security, counter-terrorism, and crime prevention. However concerns have been raised regarding these states privacy, transparency, and proportionality.

Timeline of Events

2009 June 12 Iranian authorities monitor and restrict internet access during presidential elections, marking one of the earliest widely known uses of digital surveillance to control political unrest.

2013 June 5 Edward Snowden, a former American National Security Agency intelligence contractor, exposes the US National Security Agency's mass data collection programs, exposing their global surveillance practices and beginning an international debate on privacy.

2014 March 1 China expands its social credit system, meaning citizen's online and offline behavior can now affect their state-assessed scores. To be able to achieve this large-scale digital monitoring had to be conducted.

2016 July 1 Russia enacts the Yarovaya Law, which strengthened state control over internet communications and required data storage to be on domestic servers.

2017 July 3 The UN Human Rights Council (HRC) adopted the Resolution A/HRC/34/L.7 on the right to privacy in the digital age,which urged states to balance their surveillance with human rights protections.

2020 March 11 The COVID-19 pandemic speeds up the use of digital tracking tools globally.

2021 October 1 Reports show China's nationwide use of facial recognition in public transport and urban areas, showing their expansion of mass surveillance technologies.

Relevant UN Treaties and Events

International Covenant on Civil and Political Rights (ICCPR): Establishes legal protections for privacy and freedom from arbitrary interference. This created the basis for what international standards on surveillance should be, 16 December 1966

Universal Declaration of Human Rights (UDHR): Recognizes the right to privacy and protection against arbitrary interference. This provided the foundation ideas for human rights in the new digital age, 10 December 1948

UN Human Rights Council Resolution A/HRC/34/L.7: Emphasizes the right to privacy in the digital age and calls on states to ensure surveillance is lawful, necessary, and proportionate. This ensures that states can still maintain surveillance whilst still keeping individual's rights, 3 July 2017

Reports by the UN Special Rapporteur on the Right to Privacy: Regular reports highlight risks of mass surveillance, spyware, and internet monitoring. This provides guidance for states on respecting privacy while maintaining security, Since 2013

International Telecommunication Union (ITU) Conferences on Cybersecurity: Promote discussion on internet governance, cybersecurity, and responsible state use of technology, encouraging privacy-protecting measures, Recurring with multiple years

Previous Attempts to Solve the Issue

General Data Protection Regulation (GDPR), European Union:

The EU has implemented strict data protection laws to limit how nations and private companies collect, use, and store personal data.

UN Special Rapporteur on the Right to Privacy Reports, United Nations:

The UN monitors global surveillance practices and provides insight to nations to make sure surveillance is proportionate, necessary, whilst respecting human rights.

Snowden Revelations and Subsequent Oversight Reforms, United States:

After the 2013 leaks exposed NSA for mass data collection, the US government enacted reforms such as the USA FREEDOM Act to monitor and limit large data collection.

Civil Society and Tech Company Initiatives, Global:

Organizations like Access Now, Privacy International, and technology firms have created privacy-enhancing tools, end-to-end encryption, and campaigns to reduce the further misuse of surveillance technologies.

Possible Solutions

Solution #1- Putting Focus on Companies

A huge yet underlooked issue in this issue are companies we use everyday such as social media platforms or websites. It may be useful to investigate these companies and see if they are collecting data illegally, whether their data is used in an ethical manner, and if their data bases are well secured. This helps ensure incidents such as the Pandabuy data breach does not occur and individuals passwords and personal data is kept safely.

Solution #2- Sanctions Approach

In HRC we focus mainly on maintaining the rights of people and do not take lightly to countries violating human rights. That is why imposing sanctions to states that violate human rights with their usage of digital authoritarianism.

Solution #3- Balancing Freedom of Speech and Limiting Hate Online

Though freedom of speech is important to combat digital authoritarianism, it's equally important to not harm others with our words and posts online. As a delegate attempt to create a solution that maintains as much freedom of speech and expression without hurting or affecting others, such as banning forms of nudity, hate speech, online hate platforms (websites, reddit feeds, large group chats), online harmful cults, and the spread of harmful trends. This ensures that individuals are still able to express themselves fully online while preventing the spread of hate and dangerous ideas online.