SURVEILLANCE AND ITS IMPACT ON CIVIL LIBERTIES

Prachilekha Sahoo[1]

ABSTRACT

Surveillance, when pervasive and unregulated, poses a direct threat to civil liberties, which are essential for a free and dignified life. In a society where every action, word, or thought is subject to scrutiny, individuals may begin to self-censor, fearing that even innocent behaviour could be misconstrued and used against them. This erosion of freedom undermines the core principles of privacy, free speech, and autonomy, replacing openness with fear. What is marketed as protection may, in reality, be fostering an environment of mistrust and caution, where individuals live under constant observation, compromising their ability to truly live freely.

Keywords: Civil Liberties, Surveillance, Datafication, Autonomy, Privacy

Introduction

Surveillance is a deliberate and structured form of attention, typically aimed at achieving a particular goal, which inherently involves both care and control. This concept becomes especially significant when examining surveillance carried out by public authorities, as it often reflects a paternalistic approach.[2] In this context, the state's role extends to protecting and guiding citizens through legal frameworks and their enforcement. Surveillance, when defined in broader terms, can be categorized into two types: direct and indirect. Direct surveillance is targeted, focusing on specific individuals for specific reasons, whereas indirect surveillance does not have a clear or immediate target, often involving the collection of data without a specific purpose.

One of the complexities of surveillance in the modern age is the storage of data, which makes it accessible over extended periods. This extended availability allows for the redefinition of purpose, making the original intent of surveillance a fluid and evolving concept. Moreover, the

[1] The Author is a doctoral student in National Law University Odisha.
[2] Westin, Alan F., 'Privacy and Freedom' (1968) 25 Washington and Lee Law Review 166.

data collected may not always align with the initial purpose, as it can often be a byproduct of using a particular service.

The limitations of surveillance, particularly in relation to privacy, have sparked debate about its boundaries. Some scholars differentiate between passive and active observation. Passive observation occurs without the intent to influence or control the individual, whereas active observation involves the use of collected data to impose sanctions or modify behaviour. The true essence of surveillance, as proposed by some, lies in its ability to proactively intervene in an individual's actions by utilizing collected information.

In the era of datafication, the traditional notion of surveillance—requiring a clear, predefined purpose or target—has been increasingly challenged. Surveillance now often operates on a broader scale, driven by the collection and analysis of data. This shift highlights the central role that intentionality plays in modern surveillance systems, where data serves as the key justification for its existence and implementation.[3] As surveillance becomes more pervasive and data-driven, its impact on civil liberties, especially privacy and freedom, raises important concerns about the balance between security and individual rights.

1.1 Cultural Reflections of Surveillance in Literature & Media

From Franz Kafka's *The Trial*,[4] which hauntingly portrays an individual caught in the web of a faceless bureaucracy, to contemporary films like *Snowden*[5] and the TV series *Black Mirror*[6], our literature and popular media have long served as warnings about the creeping presence of state surveillance. These narratives capture public anxiety, yet often leave the core issues undefined. Beyond the popular fear of a dystopia unfolding around us, we seldom explore precisely *why* surveillance is dangerous or *what fundamental value* it threatens.

1.2 Digital Age and Nature of Privacy

Conversations about surveillance often revolve around the idea of "privacy," but that term itself

[3] H.S. Sætra, 'Freedom under the Gaze of Big Brother: Preparing the Grounds for a Liberal Defence of Privacy in the Era of Big Data' (2019) 58 Technol. Soc. 101160.
[4] Benjamin Winterhalter, Franz Kafka's *The Trial*: It's Funny Because It's True, JSTOR Daily (July 2, 2019), https://daily.jstor.org/franz-kafkas-the-trial-its-funny-because-its-true/.
[5] Edward Snowden, *XSurveillance: The Snowden Archive* (https://snowden.xsurveillance.site/ accessed 22 April 2025).
[6] Daniel Solove, 'Black Mirror: A Powerful Look at the Dark Side of Privacy, Security, and Technology' (TeachPrivacy, 21 November 2016) https://teachprivacy.com/black-mirror/ accessed 22 April 2025.

remains nebulous in the context of digital life. What does privacy mean when our smartphones track our movements, our conversations are stored in the cloud, and our online habits are continuously monitored? For many years, such scenarios felt like the realm of fiction or the relics of totalitarian regimes. But today, that illusion of safety is unravelling.

Technological advancement has not only revolutionized communication, commerce, and connectivity it has also made possible the mass recording of our actions, preferences, and associations. With the justification of national security, particularly since the events of 9/11, state authorities have shown an increased willingness to harvest data from the public often with little transparency and minimal oversight. Investigations have revealed how governments have been tapping into corporate data troves, and agencies like the NSA have invested in colossal infrastructure projects, such as the data facility in Utah,[7] reportedly designed to store and decode enormous volumes of digital communication from around the globe.

Despite the existence of legal frameworks meant to limit surveillance, their effectiveness is questionable. Many intelligence operations remain classified, shielded from public and judicial scrutiny. And when whistleblowers or journalists expose them, legal challenges often collapse not because the harms are not real, but because courts require a level of proof and personal injury that secret surveillance makes nearly impossible to show. In this environment, meaningful oversight is rare, and the legal system lags the capabilities and ambitions of modern surveillance programs.

1.3 Datafication and Surveillance

As our world becomes increasingly shaped by the logic of data, nearly every aspect of life can now be quantified, coded, and analysed. From the mundane routines of daily life to more complex interactions, individuals constantly generate data intentionally or not. Public authorities, in turn, have expanded their reach by tapping into this ever-growing stream of information. With the rise of artificial intelligence, especially AI-powered tools designed to assist with complex decisions, governments and institutions are finding new ways to manage public affairs more efficiently, often relying on insights drawn from big data.

AI systems are fundamentally dependent on data. They need vast amounts of it to identify

[7] Mél Hogan, 'Data Flows and Water Woes: The Utah Data Center' (2015) 2 *Big Data & Society* 1 https://doi.org/10.1177/2053951715592429 accessed 22 April 2025.

patterns, test assumptions, and deliver results. As machine learning algorithms process personal data to provide predictions and make decisions, the scope for large-scale monitoring—of both individuals and society has grown immensely. This shift naturally raises pressing questions about surveillance and its consequences. While AI presents new opportunities for streamlining services and improving governance, it also introduces serious ethical and social concerns.

Our cities, now dotted with sensors, smart devices, and connected infrastructure, have turned into data-generating ecosystems. Participating in modern life whether commuting, shopping, or simply using a smartphone inevitably leaves behind digital traces. This has made privacy a central issue, especially considering that most people prefer to keep their personal lives private and to choose when, how, and with whom to share sensitive information.

The misuse or overreach of data collection not only threatens individual privacy but can also affect entire communities. When public institutions or private corporations use data irresponsibly, they risk influencing behaviour or decisions in subtle, even coercive ways. In such environments, people may find their freedom to make independent choices slowly eroded, often without realizing it. The promise of AI and big data must, therefore, be weighed carefully against the rights and freedoms of those it aims to serve.

Civil liberties go far beyond legal guarantees; they are the essence of what it means to live freely and with dignity. In a society where surveillance is constant and pervasive, where every move, word, or idea can be monitored and dissected, these fundamental rights begin to lose their meaning. The freedom to think openly, to speak without fear, to challenge authority, or to simply have private moments without scrutiny; all gradually slip away. People begin to self-censor, to hold back their thoughts or words, not because they have done anything wrong, but because they fear how even the smallest thing might be twisted and used against them. The most innocent actions can start to feel dangerous. What we are allowing in the name of protection may actually be building a world where mistrust and caution replace openness and honesty. Ultimately, if civil liberties are compromised, we are not fully living we are merely existing under watch.

1.4 Objective and Significance of the paper

- The paper seeks to critically explore the various ways in which surveillance especially digital and biometric forms affect civil liberties within democratic frameworks. It

delves into how increasing deployment of surveillance tools by governments and private actors challenges fundamental rights.

- It pays particular attention to essential civil liberties such as the right to privacy, freedom of speech, expression, assembly, and the right to dissent. The paper questions how these rights are potentially compromised when surveillance is unregulated or lacks accountability.

- A key objective is to assess how indiscriminate or opaque surveillance may lead to a weakening of democratic institutions and a reduction in individual autonomy. The emergence of a surveillance-driven environment can cultivate fear and discourage free expression.

1.5 Methodology

- This study employs a doctrinal legal research approach, grounded in an extensive review of existing laws, judicial decisions, and statutory frameworks that govern surveillance and privacy rights. It draws upon constitutional provisions, landmark court rulings, legislative texts, and policy measures relevant to the subject. In addition, the paper engages with international human rights standards and norms to provide a comparative perspective. Supplementary analysis is carried out using secondary sources such as publications from civil society organizations, government reports, and the works of legal scholars and commentators, as well as credible media coverage. This methodology allows for a comprehensive understanding of the evolving relationship between surveillance mechanisms and the protection of civil liberties.

2.1 Understanding AI Surveillance

Artificial intelligence has brought a new level of sophistication to surveillance systems, going far beyond the basic capabilities of traditional motion detectors. Where older systems simply picked up on movement by registering pixel changes—often mistaking a rustling tree for a real threat AI-driven surveillance uses far more advanced methods to understand what's really happening in a scene.[8]

[8] Colin Quirk, 'How Artificial Intelligence Surveillance Redefines Security' (1 October 2024) https://resources.volt.ai/blog/artificial-intelligence-surveillance accessed 22 April 2025.

At the heart of this transformation are technologies like computer vision and machine learning. Computer vision allows surveillance systems to visually interpret their surroundings in a way that resembles human perception. These systems can recognize and categorize different objects—such as people, vehicles, or animals track how they move, and evaluate their behaviour. For example, in a high-security area, computer vision can help spot unauthorized individuals, monitor movement within restricted zones, and alert operators to anything that seems out of the ordinary.

Machine learning, on the other hand, gives these systems the ability to learn from experience. Instead of being manually programmed to recognize specific actions, they are trained on vast libraries of video and image data. Over time, they become adept at identifying patterns, spotting unusual activity, and even anticipating certain types of incidents. For instance, if a system has been trained on video footage of thefts, it can learn to detect behaviours that often precede such events—like someone loitering near high-value items—and raise alerts before anything happens.

In essence, AI-powered surveillance transforms standard security cameras into intelligent sentinels. They operate around the clock, analysing huge volumes of visual information in real-time. These systems can flag an abandoned bag, identify individuals from watchlists, or detect suspicious conduct much like a tireless digital guard with eyes everywhere.

The ongoing datafication of our world has made it possible to capture, encode, store, and process nearly every aspect of human activity. As a result, public authorities have expanded their influence by harnessing this vast pool of data. This is further amplified by advancements in artificial intelligence (AI), which assist in complex decision-making and help shape public policies to better manage societal functions. The widespread adoption of AI systems that leverage big data is therefore increasingly common.

AI systems are inherently reliant on data. These systems, particularly machine learning, use the data available to identify patterns, validate assumptions, and make decisions. Data, in this context, is fundamental to the operation and performance of AI, and its dependency on data is a core feature of its design. As data collection expands, the ability to monitor individual and societal behaviors grows, raising critical questions about the implications of

this surveillance.[9] The integration of big data and AI-driven automation offers significant potential, but it also brings about serious concerns.

Technologies that gather and transmit data are becoming ubiquitous in our urban environments, with many of these technologies now essential to daily life. This has raised significant privacy concerns, especially when individuals' ability to control what information is shared is diminished. People often prefer to keep their personal details private and share information selectively. The misuse or overreach of personal data can put individuals and entire communities at risk, as they may become vulnerable to the influence of external parties, be it government authorities or private corporations. In such a scenario, individuals may find their ability to make free, independent choices compromised.

Although regulatory frameworks such as the General Data Protection Regulation (GDPR) in the European Union[10] and the Personal Information Protection Law (PIPL)[11] in China are steps toward addressing these concerns, the principles behind these regulations are still evolving and remain subject to cultural and political influences. AI, as a field, is dynamic and continues to develop, which makes it crucial to remain vigilant in evaluating whether the trade-offs involved are acceptable.

2.2 Distinction between traditional and AI-based surveillance

With rapid technological progress, surveillance is no longer just about watching it's about responding. The role of surveillance is transforming from passive monitoring to proactive intervention. In today's world, where threats can emerge and escalate in seconds, timely action is often the key to avoiding disaster. Relying solely on traditional methods like reviewing camera footage after an incident is no longer enough. These outdated approaches struggle to keep up with the urgency and complexity of modern-day challenges.[12] Facial recognition technology erodes the right to privacy and the right to be forgotten by allowing for the ongoing

[9] Fontes, Catarina, Hohma, Ellen, Corrigan, Caitlin C., and Lütge, Christoph, 'AI-powered public surveillance systems: why we (might) need them and how we want them' (2022) 72 *Technological Forecasting and Social Change* 102137 https://doi.org/10.1016/j.techsoc.2022.102137 accessed 22 April 2025.

[10] Kao, Y.-H. and Sapp, S.G., 'The effect of cultural values and institutional trust on public perceptions of government use of network surveillance' (2022) 70 *Technological Forecasting and Social Change* 102047 https://doi.org/10.1016/j.techsoc.2022.102047 accessed 22 April 2025.

[11] Bartneck, C., Lütge, C., Wagner, A., and Welsh, S., *What is AI? An Introduction to Ethics in Robotics and AI* (Springer 2020) SpringerBriefs in Ethics.

[12] The Hans India, 'Balancing Safety and Privacy in the Era of AI Surveillance' (The Hans India, 2024) https://www.thehansindia.com/hans/education-careers/balancing-safety-and-privacy-in-the-era-of-ai-surveillance-964839 accessed 22 April 2025.

surveillance and identification of individuals without their consent. In a similar vein, emotion recognition systems invade personal privacy by assessing and interpreting an individual's emotional state, often without their knowledge or permission. The use of predictive analytics in surveillance can stifle free expression and ideological freedom, as individuals may feel compelled to self-censor for fear of their actions and thoughts being monitored for future risks. Furthermore, biometric tracking and the persistent recording of movements have become widespread forms of surveillance, collecting and storing detailed data about people's daily activities and whereabouts, frequently without explicit consent or proper oversight. Collectively, these technologies pose serious threats to individual autonomy and privacy.

2.3 Surveillance and Governance

The Aadhaar project, launched in 2009, marked a significant shift in how surveillance became intertwined with governance in India. Designed to streamline access to government services, Aadhaar assigned each resident a unique 12-digit identification number based on biometric and demographic data. Though it received legislative approval in 2016, the system sparked intense debate over privacy when authorities began insisting that Aadhaar be linked with essentials like mobile numbers, bank accounts, and pension schemes. This move allowed the government to compile vast amounts of personal information, effectively constructing a digital replica of each citizen.[13]

This digital dependency made it nearly impossible for people to navigate routine tasks without Aadhaar. A survey during the 2019 general elections by CSDS-Lokniti revealed a troubling consequence: several low-income individuals were denied access to food rations because of either a lack of Aadhaar or technical issues associated with it.[14] What was once a system based on voluntary participation gradually evolved into one of forced compliance, undermining the principle of informed consent. Concerns reached the Supreme Court in 2018, where a group of lawyers voiced alarm over the possible integration of Aadhaar with the National Register of Citizens (NRC), a database aimed at identifying legal citizens. They feared such a merger could be used to label individuals as "non-citizens," stripping them of social security benefits.[15] The government, meanwhile, continued to push digital identification further with the introduction

[13] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (No. 18 of 2016).
[14] Rajdeep Sardesai, *2019: How Modi Won India* (HarperCollins India 2021).
[15] Gautam Bhatia, 'The Aadhaar Verdict and the Right to Privacy' (The Wire 2018).

of a proposed National Digital Health ID. This initiative would store individuals' health information—an especially sensitive category of data.[16]

In the absence of robust data protection laws, linking such a health ID with Aadhaar could expose deeply private details, especially of marginalized groups such as sexual minorities. There are also concerns that anonymized data collected under the policy might be shared with third parties, blurring the lines between public welfare and commercial use. If this health ID becomes mandatory, those unwilling to participate could find themselves excluded from essential services.[17]

Moreover, beyond the risk of government overreach, there's the added threat of data leaks. In May 2017, the Centre for Internet and Society in India revealed that the personal details of 130 million Aadhaar holders were freely accessible online.[18] Digital surveillance has not only expanded state control but also brought powerful private entities into the fold—tech companies with the infrastructure and reach to collect, store, and exploit vast amounts of personal data. Social media platforms, in particular, have become hotspots for mass-scale data surveillance.[19]

3.1 Importance of Civil Liberties

One of the most significant challenges in the modern era is striking a delicate balance between surveillance activities conducted by governments and the protection of individual privacy. In an increasingly interconnected world, technological advancements have made it easier than ever for authorities to monitor and collect information on citizens. Civil liberties grant us the freedom to act independently. However, this freedom is not without its boundaries. It stops when our actions violate laws or encroach upon the rights of others. As such, it does not mean we can act without restriction—freedom doesn't justify lighting a cigarette in a non-smoking area or contaminating a dish to cause harm or discomfort to others.[20]

The true value of civil liberties lies in their ability to shield us from unwarranted government intervention. They safeguard us from arbitrary state control over our lives. These rights are integral to our fundamental freedoms and cannot be easily stripped away by the government.

[16] Rina Chandran, 'India's Digital Health ID Plan Raises Data Privacy Fears' (Reuters 2020).
[17] Ibid
[18] Centre for Internet and Society, 'Information Security Practices of Aadhaar (or Lack Thereof)' (May 2017).
[19] Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs 2019).
[20] Jascha Galaski, 'Why We Should Value Our Civil Liberties' (Democracy & Justice, 7 June 2022) https://www.liberties.eu/en/stories/civil-liberties/44284 accessed 23 April 2025.

It's important to note, however, that civil liberties are not exclusive to democratic nations. Even in authoritarian regimes like North Korea, citizens are officially granted civil liberties, such as the right to free speech. The real question, however, is whether these rights are genuinely respected or merely exist on paper.

3.2 Balancing Act

Ensuring national security while respecting privacy rights is a complex juggling act. On one hand, surveillance measures can help prevent and investigate criminal activities, safeguarding the public. On the other hand, unchecked surveillance can intrude upon individual privacy and lead to a chilling effect on freedom of expression and association. This delicate balance between security and privacy is essential for protecting political rights, as unwarranted surveillance can undermine citizens' rights to privacy, free speech, and peaceful assembly.

Striking the right balance requires robust legal frameworks, independent oversight, and transparency. Effective safeguards must be put in place to ensure that surveillance activities are targeted, proportionate, and subject to judicial review. Additionally, educating individuals about their rights and the implications of surveillance is crucial to fostering an informed public discourse on the topic.[21]

3.3 Technological Implications

Browsing the internet may seem like a routine activity, but the trail of digital footprints it leaves behind can expose far more about a person than one might expect. Every site visited, every search query entered, every link clicked, and every file downloaded adds to a detailed profile. Even seemingly minor details—such as how long you stay on a webpage or the type of device you're using—contribute to the broader picture.

When this browsing data is combined with other forms of surveillance—such as emails, texts, phone records, location history, media consumption habits, and more—it creates a highly detailed and revealing mosaic of an individual's personal life. These insights can reflect daily routines, preferences, belief systems, and even allow for fairly accurate predictions of a

[21] Gray Group International, 'Civil Liberties: Upholding the Cornerstones of Democracy' (1 October 2024) https://www.graygroupintl.com/blog/civil-liberties accessed 23 April 2025.

person's religion, sexual orientation, political ideology, and other intimate aspects of their identity.

Today, people turn to the internet for nearly everything: connecting with loved ones, searching for employment, managing finances, shopping, reading the news, booking holidays, learning new skills, and practicing their faith. The digital world has become so enmeshed in our everyday lives that it touches nearly every sphere of human activity.

3.4 Civil Liberties and Surveillance

What makes this especially concerning is the rise of sophisticated analytical tools. In industries like behavioural advertising, enormous investments are made to sharpen the ability to interpret browsing data. Tech giants such as Google and Meta rely on this profiling to sustain their business models. These systems don't just make assumptions about consumer habits—they develop predictive models based on correlations across massive data sets. These models can be used not only for targeted marketing, but also to categorize individuals based on sensitive factors like political views, religious affiliation, or ethnic background, posing serious privacy risks.

Such profiling practices have wide-reaching legal and ethical implications, especially concerning the rights guaranteed under Article 19(1)(a) of the Indian Constitution, which protects freedom of speech, belief, and religion. The ability of AI tools to infer deeply personal beliefs or values may lead to individuals being surveilled or discriminated against for their affiliations or ideologies. This could, in turn, undermine related rights such as freedom of association, assembly, or conscience.

While it might sound exaggerated to say that algorithms can read our thoughts, this is essentially the goal of many digital systems. Tools like Siri, Google Assistant, and Cortana are built to anticipate and fulfil user needs, learning from user behaviour in the process. Some experts even argue that platforms like Facebook or Google might understand our behaviours and preferences more accurately than we do ourselves. And for companies or state actors, absolute accuracy isn't necessary—likelihoods and patterns are often enough to trigger action. Yet, from the individual's point of view, whether the profiling is spot-on or mistaken, the consequences can be equally serious. A genuine political dissenter may be identified and silenced, while an innocent person wrongly profiled may face suspicion or punitive action.

Moreover, profiling can subtly fuel discrimination, reinforcing existing social biases across employment, education, law enforcement, and more.

It's also important to recognize how privacy and freedom of expression are intertwined. While these rights can occasionally appear to be in tension, privacy is actually a cornerstone of meaningful expression. For example, journalists depend on privacy to safeguard the identities of their sources. Without such protections, the ability to investigate and report would be severely compromised, affecting not only press freedom but the public's access to truth.

In India, key fundamental rights, including the right to privacy, freedom of speech, freedom of movement, and the right to protest, have faced increasing challenges due to surveillance practices. The right to privacy, reaffirmed in the historic *K.S. Puttaswamy v Union of India* (2017) case[22], underlines the individual's right to control personal information. However, the growing use of surveillance technologies, such as facial recognition and biometric systems, poses a threat to this right. These technologies allow for the tracking of individuals on a mass scale, often without their consent, which can result in unwarranted breaches of privacy. Data is collected in public spaces with minimal oversight, raising concerns about the misuse of such information for unintended purposes. The Aadhaar Act, which involves the collection of biometric data for identity verification, has sparked ongoing debates regarding its potential for state surveillance and the overreach it may invite.[23]

The freedom of speech and right to protest [24]in India have similarly been curtailed by surveillance practices, where the monitoring of dissent has become more prevalent. The Supreme Court's decision in *Shreya Singhal v Union of India* (2015)[25], which struck down Section 66A of the Information Technology Act, 2000, addressed attempts to stifle online free speech. However, surveillance continues to impact the way people express themselves, especially online, as individuals often self-censor due to concerns over being monitored. With technologies like GPS tracking and facial recognition, the freedom of movement has also become more constrained, as people can no longer move freely without the fear of being watched. The right to protest, essential to democratic expression, has been increasingly

[22] Justice K.S. Puttaswamy (Retd.) and Another v Union of India and Others (2017) 10 SCC 1.
[23] Sangeeta Mahapatra, *Digital Surveillance and the Threat to Civil Liberties in India* (2021) 3 GIGA Focus Asien 12, German Institute for Global and Area Studies (GIGA), Hamburg https://nbn-resolving.org/urn:nbn:de:0168-ssoar-73130-3 accessed 23 April 2025.
[24] Constitution of India 1950, Art 19(1)(a).
[25] *Shreya Singhal v Union of India* (2015) 5 SCC 1.

hindered by surveillance measures. The tracking of protestors, as seen during the farmer protests of 2020-21[26] and other student demonstrations, has raised alarm over the potential stifling of dissent. These developments highlight the ongoing tension between state security measures and individual freedoms, with surveillance technologies playing a significant role in reshaping this balance in India.

4.1 AI Surveillance and Privacy

State surveillance, in and of itself, is not inherently unlawful. Governments often have legitimate reasons to monitor certain activities, particularly in the interest of public safety and national security. Surveillance tools, for instance, play an essential role in counter-terrorism operations, helping authorities anticipate, prevent, and respond to threats. They serve to detect criminal activity and protect the public from harm. However, advancements in technology have drastically altered the landscape of state surveillance—both in scope and method. The digital age has given rise to an unprecedented volume of transactional data, commonly referred to as "metadata," which includes information like email logs, location history, web browsing patterns, and other forms of digital footprints.[27]

In his seminal 2013 report, former UN Special Rapporteur Frank La Rue [28]drew attention to the dangers posed by this development. He noted that communication data—now easily storable, retrievable, and searchable—was being accessed by state actors without adequate legal safeguards. When aggregated, this data reveals intimate aspects of an individual's life, posing serious concerns about the potential for misuse. States increasingly rely on such data in the name of law enforcement and national security, often mandating telecom providers to retain communication records for retrospective investigation. These practices significantly compromise the individual's right to privacy and may also encroach on freedoms of association and expression. The Office of the UN High Commissioner for Human Rights (OHCHR) has consistently highlighted the need to guard against "arbitrary or unlawful interference" with

[26] Sangeeta Mahapatra, *Digital Surveillance and the Threat to Civil Liberties in India* (2021) 3 GIGA Focus Asien 12, German Institute for Global and Area Studies (GIGA), Hamburg https://nbn-resolving.org/urn:nbn:de:0168-ssoar-73130-3 accessed 23 April 2025

[27] Office of the United Nations High Commissioner for Human Rights, 'The Right to Privacy in the Digital Age' (30 June 2014) UN Doc A/HRC/27/37 https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

[28] Frank La Rue, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (17 April 2013) UN Doc A/HRC/23/40

private life, home, or correspondence.

International human rights law provides a framework for assessing the legitimacy of surveillance. First, domestic legislation must authorize any such activity. As David Kaye, La Rue's successor, emphasized in a 2019 report[29], legal provisions should be clear, accessible to the public, and specific enough to allow individuals to understand and adjust their conduct accordingly. Vague or overly broad laws that grant sweeping powers to authorities without sufficient checks violate this standard. Second, surveillance must meet the principle of "necessity and proportionality."[30] This means it should only be employed when it is absolutely required to pursue a legitimate goal and must be the least intrusive means available. Third, the purpose justifying the surveillance must be legitimate. While states often cite national security or public order, the OHCHR warns against the misuse of such justifications, particularly when used to silence dissent or restrict civil liberties. A truly legitimate surveillance system, therefore, demands a strong, independent oversight mechanism—typically judicial in nature—that can ensure transparency, accountability, and access to remedies for those affected.

Yet even in democratic nations with well-established legal systems, surveillance programs often fall short of these high standards. In states with weak enforcement mechanisms or authoritarian tendencies, surveillance frequently occurs without accountability. The OHCHR's inaugural report on privacy in the digital age underscores this reality, pointing to a troubling global pattern of unchecked digital monitoring.

The emergence of artificial intelligence in surveillance has deepened these concerns. AI technologies enhance the capacity of states to conduct constant, widespread, and often opaque surveillance. As La Rue cautioned, advances in technology have removed previous constraints—such as cost, scale, and duration—that once limited the state's ability to monitor its citizens. AI-driven systems now automate what were once labour-intensive processes, reducing the reliance on human operatives and increasing the efficiency of data collection. This shift also introduces new risks: machine-led surveillance operates continuously, without

[29] David Kaye, 'Surveillance and Human Rights: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (28 May 2019) UN Doc A/HRC/41/35 https://undocs.org/A/HRC/41/35

[30] Necessary and Proportionate, 'International Principles on the Application of Human Rights to Communications Surveillance' (4 March 2016) https://necessaryandproportionate.org/principles

fatigue, and often without the nuance or discretion of human judgment.[31]

Furthermore, the pervasiveness of AI surveillance can exert a powerful chilling effect on society. When individuals are uncertain whether their messages are being read, their movements tracked, or their social media activity monitored, the natural consequence is self-censorship. The fear of constant observation—whether or not surveillance is actually occurring—can be enough to suppress free expression and political participation.[32] As surveillance capabilities grow ever more sophisticated, it becomes increasingly urgent to reinforce legal and institutional safeguards that protect fundamental rights in the digital era.

4.2 Surveillance in International and Regional Norms

Surveillance technologies operate within a legal and ethical landscape that remains fragmented at the international level. Despite increasing global reliance on digital monitoring systems, there is no comprehensive international framework that harmoniously balances national security concerns with the obligation to uphold fundamental human rights. The United Nations, through its Human Rights Council, has repeatedly emphasized the importance of protecting the right to privacy in the digital age, warning that unchecked surveillance poses significant threats to individual liberties. The UN Special Rapporteur on the right to privacy has advised states to ensure that surveillance mechanisms are aligned with established principles of international human rights law.

A robust legal foundation already exists in international law—chief among them being Article 17 of the International Covenant on Civil and Political Rights (ICCPR), along with General Comment No. 16, which collectively protect individuals against arbitrary or unlawful intrusions into their private lives. Nevertheless, the interpretation and enforcement of these norms vary across jurisdictions, often reflecting national and regional legal traditions.[33]

In the European Union, for instance, the General Data Protection Regulation (GDPR) sets stringent conditions for the processing and transfer of personal data, embodying a rights-based

[31] Steven Feldstein, 'Can a UN Report Help Rein in Expansive and Abusive Digital Surveillance?' *World Politics Review* (9 July 2019) https://www.worldpoliticsreview.com/articles/28016/can-a-u-n-report-help-rein-in-expansive-and-abusive-digital-surveillance

[32] Steven Feldstein, 'The Road to Digital Unfreedom: How Artificial Intelligence Is Reshaping Repression' (2019) 30(1) *Journal of Democracy* 39

[33] Global Coalition for Human Rights and Government Digitalization (GCHRAGD), *Surveillance and Human Rights: Background Paper* (June 2023) https://gchragd.org/wp-content/uploads/2023/06/GCHRAGD-SURVEILLANCE-AND-HUMAN-RIGHTS-background-paper.pdf accessed 23 April 2025.

approach to privacy protection. The Council of Europe, through Convention 108 on the Protection of Individuals with regard to Automatic Processing of Personal Data, has further reinforced this framework. Convention 108 has gained international relevance beyond Europe, with several non-European countries—including Argentina, Tunisia, and Uruguay—voluntarily adopting its standards. This widespread endorsement signals the convention's growing influence as a potential foundation for a global data protection treaty.

Beyond Europe, other institutions have also contributed to the evolving discourse. The Organisation for Economic Co-operation and Development (OECD) has developed significant guidelines on privacy safeguards, particularly in contexts involving national security and law enforcement access to data. Yet, the practical enforcement of these international norms often relies heavily on their incorporation into national legal systems, as noted by scholars in *The International Journal of Human Rights*.

To prevent the misuse of surveillance technologies, additional safeguards such as export control regimes have been introduced. The Wassenaar Arrangement, for example, limits the export of certain surveillance tools that could be exploited for oppressive purposes. Similarly, the European Union has undertaken efforts to regulate the export of cyber-surveillance products, aiming to curb their misuse in violating human rights.

In conclusion, while numerous international instruments and initiatives provide guidance on data protection and surveillance, the absence of a universally binding legal regime leaves a significant gap in the global governance of privacy rights. To bridge this divide, greater international cooperation is needed—one that aligns the imperatives of security with the enduring values of human dignity, autonomy, and freedom from arbitrary state intrusion.

Conclusion

The attempt to reconcile civil rights with the growing benefits of advanced surveillance technologies reflects an ongoing effort to resolve the inherent tension between individual freedoms and collective security. This delicate process requires a critical assessment of which civil liberties, if any, may need to be restricted in order to justify the deployment of particular surveillance tools. Recognizing that civil rights, while fundamental, may occasionally come into conflict with security objectives is central to this debate. Emerging technologies in

surveillance offer capabilities that, when used responsibly, can serve important societal interests—such as public safety and crime prevention.

Modern governance and technology present challenges to the unfettered exercise of civil liberties.

Nevertheless, the idea of "balance" should not automatically suggest that the expansion of surveillance must erode civil rights. Surveillance systems and civil liberties need not be positioned as oppositional forces. In fact, how society interprets the trade-offs between these two spheres is often shaped by cultural expectations, public trust in institutions, and historical experiences with overreach or misuse of surveillance.

To truly strike an equitable balance, a deeper appreciation of the complexities involved is necessary. This includes acknowledging the social and ethical costs of surveillance and committing to upholding civil rights even as technology evolves. Crafting responsible policies in this domain calls for inclusive dialogue, institutional transparency, and the formulation of legal safeguards that prioritize the protection of fundamental freedoms. Only through such comprehensive efforts can societies harness the benefits of surveillance while ensuring that the core principles of civil liberty remain intact.