

National Security Vs. Civil Liberties in the Digital Age: Where Lies the Balance?

Ravale Mohydin



(Faisal Khan - Anadolu Agency)

Technological advancements have transformed the political landscape in recent years, influencing how governments interact with their citizens and those from other nations. This policy outlook explores the intersection of technology, national security, and civil liberties. While technology has made it easier for individuals to access information, communicate with others, and participate in democratic processes, it has also raised concerns about threats to privacy, censorship, and surveillance. This paper delves into contemporary case studies to provide level-headed recommendations for policymakers to find the right balance in the digital age.

Introduction

Technological advancements have transformed the political landscape in recent years, influencing how governments interact with their citizens and those from other nations. From social media to mobile technology and cloud computing, technology has revolutionised how governments function and handle critical issues, including national security and human rights. While technology has made it easier for individuals to access information, communicate with others, and participate in democratic processes, it has also raised concerns about threats to privacy, censorship, and surveillance.

This policy outlook will examine the opportunities and challenges presented by technological advancements in governance by highlighting multiple examples from developing and developed countries. These opportunities and challenges afforded by technological advances also mirror the long-standing and complex debate between governments prioritising national security versus human rights. Two case studies of technology-enabled surveillance will highlight the need to balance these two vital functions of government: that conducted by the United States government post 9/11 attacks in the United States and the surveillance conducted by the Indian government in Indian Administered Kashmir after the revocation of Article 370 of the Indian Constitution in August 2019.

Drawing from the case studies, this paper will provide recommendations for policymakers to balance the need for national security with the protection of human rights in technological innovations. The overarching objective is to ensure that human rights remain at the forefront of technological innovations to promote just, effective, and sustainable governance.

The Utility of Technology in Governance

The use of technology in governance has been on the rise [since the early 2000s](#) when governments started to explore the possibilities of the internet and digital technologies for delivering public services, engaging with citizens, and promoting transparency and accountability. Integrating [modern technologies](#), including social media, mobile devices, and cloud computing, into daily life, business, and government operations promotes greater government transparency and new forms of public engagement beyond traditional boundaries. Governments have increasingly turned to technology to streamline their processes, improve their services, and enhance their communication with the public.

Governments have developed various technological solutions to address [various aspects of governance](#), including

e-government services, open data initiatives, social media engagement, online collaboration, and online participation. These tools have improved access to public services, provided greater transparency and accountability, and facilitated citizen participation in the democratic process. In this digital environment, there are opportunities for increased collaboration and participation, enabling stakeholders like citizens, businesses, and non-governmental organisations to shape political priorities, collaborate on public service design, and contribute to their implementation, resulting in more efficient and cohesive solutions to complex problems. This shift towards ["digitally-enabled participation"](#) and service production is causing a change in people's expectations of their interactions with their government, necessitating a new approach to public governance that emphasises citizen-driven solutions, where citizens and businesses play an active role in not just identifying and communicating their needs, but also working together with the government to address them.

With that said, governments around the world have [increasingly utilised technology as a tool to suppress dissent](#) and maintain their grip on power also. They have used digital surveillance technologies to track individuals, monitor their online activities, and intercept their communications, using this information to identify and target dissenting voices, leading to arrests, detention, and other forms of suppression. Governments have also deployed disinformation campaigns, using social media platforms to spread false information and propaganda to manipulate public opinion and undermine opposition movements in their countries and abroad. Furthermore, by controlling access to information, governments can limit the public's awareness of events in the name of national security. This approach can also prevent citizens from holding their leaders accountable.

Intersection of Technology, National Security and Human Rights in Governance

The intersection of technology, national security, and human rights in governance refers to how technology can take a binary route in the political and governance arenas. It can either advance or hinder human rights. Developed and developing countries use technology in governance, although [the level of adoption and implementation](#) varies widely across regions. For example, research findings show that the strongest predictor of the intention to use e-government services in developing countries is performance expectancy, or the expected competence of the government providing the services, followed by trust on the internet. Other significant predictors of usage behaviour include computer self-efficacy and the availabil-

ity of relevant resources. The varying levels of the use of technology in governance and unequal access to the internet itself may create a digital divide, i.e. the “gap [between demographics and regions](#) that have access to modern digital ICT and the backbone infrastructure and those that do not or have restricted or limited access”. There are two main manifestations of this divide: within a country and between countries, either due to the simple division between those who have material access and those who do not (which is narrowing as years go by as more people gain access to digital technology), or the lack of access to digital technology due to underlying social inequalities, and lack of support and help needed to effectively use technology.

This intersection of technology, national security and human rights in governance is important for several reasons:

1. Technology has become a critical tool for governments to deliver services, engage with citizens, and promote transparency and accountability. With the rise of the internet and digital technologies, governments can use technology to reach a wider audience, collect and analyse data, and respond to citizen needs more quickly and effectively.
2. National security plays a crucial role in shaping how technology is used in governance. Decisions relevant to national security can significantly impact the adoption and implementation of technology in government and influence how technology is used to promote or undermine human rights.
3. Human rights are a fundamental aspect of governance, and technology can act in a binary mode to either advance or impede these rights.

As mentioned above, technology can increase access to information, promote freedom of expression, and significantly enable greater citizen participation in the democratic process and political participation. In 2008, Barack Obama’s presidential campaign was the first ever major digital election campaign and [revolutionised the use of digital technology](#) in politics, using tactics such as YouTube videos, Facebook (now Meta), text messages, and targeted emails. They focused on small online donations, resulting in a record-breaking amount of almost 750 million USD by the end of the campaign. The use of digital tools allowed the campaign to speak directly to the public without mainstream media interference and encouraged community building. Obama’s digital efforts coincided with the emerging digitisation of politics and resonated with digital natives.

Technology has also played a significant role in increasing awareness of human rights abuses. Social media platforms, such as Meta, Twitter, and Instagram, have become important tools for citizen participation and engagement in the democratic process. These platforms have enabled

citizens to share information, organise protests and campaigns, and communicate with their elected representatives. Social media has also allowed individuals to draw attention to human rights abuses and share information about them with a global audience. For example, social media played a role in the Arab uprisings by helping to organise activists in Egypt and providing a platform for freedom of speech and civic engagement. Research suggests that social media’s primary importance resides in [communicating events to the rest of the world](#) rather than being a causal mechanism for the uprisings. Social media was found to act as a megaphone for spreading information outside the region rather than a “[rallying cry](#)” within it.

Mobile apps have made it easier for citizens to access information about their government and [participate in the democratic process](#). For example, some apps allow citizens to track government spending, report corruption, or submit complaints about public services. These apps have also enabled citizens to document human rights abuses, such as police brutality, and share them with a wider audience. An example of this is the [Citizens Portal Pakistan](#), an online platform launched by the government of Pakistan in 2018 to provide citizens with a convenient and efficient way to communicate with the government and report their grievances or complaints. The platform has a simple and user-friendly interface and allows citizens to submit complaints or feedback related to government services, track their progress, and rate the services provided by government departments. It has been widely praised for its effectiveness in [addressing citizens’ grievances](#), improving government services, increasing transparency and accountability, and enabling citizens to have a more proactive role in governance.

Crowdsourcing platforms have enabled citizens to report and map instances of human rights abuses in real-time. These platforms allow individuals to report incidents anonymously and aggregate them into a central database, creating a more comprehensive and accurate picture of human rights abuses. [Ushahidi](#) is an example of a non-profit software company that provides tools to help people collect, manage, and visualise data during crises. It was first created in Kenya in 2008 to map incidents of violence and election fraud during the presidential election. Ushahidi has since been used in various contexts, including tracking the spread of H1N1 in Mexico and monitoring the aftermath of the 2010 earthquake in Haiti. The platform aggregates information submitted via SMS, email, Twitter, or a web form and presents it on a map in real-time. Online petitions, such as those hosted on Change.org, have become popular tools for citizens to express their opinions and demand action from their governments. These petitions have been [used to advocate for policy changes](#), address human rights abuses, and hold governments accountable.

While technology has made it easier for individuals to access information, communicate with others, and partici-

pate in democratic processes, it has also raised concerns about privacy, censorship, and surveillance. The increasing troves of personal data collected and stored by governments and private companies have raised concerns about how that data is used, who has access to it, and whether it is being used to violate individuals' privacy rights. For example, the widespread use of facial recognition technology and other forms of biometric data collection has raised concerns about government surveillance and the potential for abuse. As the ability to capture faces from remote distances is becoming simpler and cheaper, it must be noted that [facial recognition data cannot be encrypted](#) like other types of data. As a result, there is an increased risk of unauthorised individuals accessing private information by exploiting the large volume of facial recognition data stored in government databases such as driver's licenses, mugshots, etcetera. This risk is further compounded by the fact that facial features, unlike passwords or credit card information, cannot be easily altered or changed. While some claim that the security risks associated with facial recognition technology (FRT) are minimised because each vendor's FRT algorithms are unique, this is not always the case, particularly when government databases use a single vendor (which many governments do). A security breach in such a case could potentially compromise all the systems.

Censorship is another issue, as mentioned above, that is closely tied to technology and human rights. While the internet has equipped individuals with unprecedented access to information, it has also made it easier for governments to control what information is available. Many countries, particularly those with authoritarian regimes, resort to internet censorship to restrict access to certain information or muzzle public discourse. The Indian government's [censorship measures](#) in Indian-administered Kashmir are a prime example and have been the subject of significant international scrutiny and criticism. The government's decision to impose an internet blackout for several months following the revocation of Article 370 severely impacted the region's economy and the daily lives of residents. In addition, the inability to access essential services such as healthcare and education significantly impacted the population's well-being, [particularly during the Covid-19 pandemic](#). The communication blackout also affected the ability of journalists and media professionals to report on events in the region. The government's restrictions on local news websites and media outlets prevented the dissemination of information and news from the region. This lack of information made it difficult for people outside the region to know what was happening, and it also made it challenging for people within the region to stay informed.

Human rights organisations have criticised the Indian government's censorship measures for violating the [fundamental right to freedom of expression](#) and limiting ac-

cess to information. The restrictions on the media and the arbitrary detention of individuals who express dissenting views or criticise the government have been condemned as a violation of human rights. The Indian government has also been criticised for using stringent laws such as the [Unlawful Activities Prevention Act](#) and the Public Safety Act to "[detain and arrest individuals](#) without proper due process". These laws give the government broad powers to detain individuals and restrict their freedom of speech and assembly. Despite the criticisms, the Indian government has defended its actions, stating that the restrictions on communication and the internet were necessary for security reasons. The government has also argued that the revocation of Article 370 and the subsequent changes in the region's status will lead to economic development and greater integration with the rest of India. However, many observers in the region remain sceptical of these claims and continue to voice their concerns towards the government's policies.

Finally, surveillance is another contentious issue closely linked to technology in governance and human rights. The widespread use of surveillance cameras, drones, and other surveillance technology has raised concerns about government intrusion into individuals' private lives. Many countries have also been accused of mass surveillance, using advanced technology to monitor citizens' online activities and collect vast amounts of personal data. For example, the United States (US) has increasingly been described as a "[surveillance state](#)" in recent years due to its extensive implementation of surveillance programs and practices.

Successive US governments have introduced various surveillance programs in the name of national security, such as the Patriot Act and the Foreign Intelligence Surveillance Act (FISA). The National Security Agency (NSA) is primarily responsible for the US government's surveillance activities, including the monitoring of internet and phone communications. The bulk collection of phone and internet data by the NSA has been the subject of public scrutiny in recent years following the [revelations](#) by former NSA contractor-turned-whistleblower Edward Snowden.

Snowden's disclosures also exposed the existence of PRISM, a program that enabled the NSA to access data from significant technology companies such as Google and Meta. Furthermore, there is widespread deployment of surveillance cameras in public spaces, including streets, airports, and government buildings, and the use of facial recognition technology has raised concerns about privacy and civil liberties. The reach of the US surveillance apparatus has also led to debates about the balance between human rights and national security, with some arguing that these measures violate individuals' right to privacy and freedom of speech, while others say that such steps are necessary for the protection against terrorism.

The National Security versus Human Rights Debate in the Age of Technology

This issue brings us to the long-standing and complex debate between [governments prioritising national security versus human rights](#). The tension between protecting national security and protecting human rights has generated significant discussion among policymakers, scholars, and the public. At its core, this debate centres around balancing the need to ensure public safety and security with the obligation to uphold all individuals' fundamental rights and freedoms, regardless of nationality or affiliation. On the one hand, advocates of prioritising national security argue that measures such as surveillance and censorship are necessary to prevent threats and ensure public safety. On the other hand, advocates of prioritising human rights contend that these rights are essential to a democratic society and should be protected at all costs. This approach includes protecting freedom of speech, assembly, and association, ensuring due process, fair trials, and the prohibition of torture and other forms of cruel and inhumane treatment. These rights are enshrined in international human rights conventions, such as the [Universal Declaration of Human Rights](#), and are widely considered to be fundamental principles of democratic governance.

Advancements in technology have added a further layer of complexity. While new technologies have provided governments with powerful tools to prevent threats and ensure public safety, they have also raised significant concerns about individual privacy and the potential for abuse. The impact of technological advancements on the debate between safeguarding national security and protecting human rights is further complicated by the fact that they are often driven by the private sector rather than the government. Private companies such as Google and Meta have access to [vast amounts of individuals' personal data](#), which can be used for commercial purposes or sold to third parties. Private companies' use of these data has raised concerns about the potential for abuses and the need for greater regulation to protect individual privacy rights. This debate is further complicated because these two goals are not always mutually exclusive. For example, measures designed to protect national security may also have the unintended consequence of violating individual rights and freedoms. Similarly, policies that prioritise human rights may be perceived as weakening national security and leaving the population vulnerable to external threats.

To provide a more nuanced view, the above two scenarios of using surveillance technology to suppress human rights to allegedly pursue national security objectives in the US

and the Indian Administered Kashmir can be compared and contrasted. To clarify, it is important to note that the Indian government's suppression of human rights in Indian-administered Kashmir involves both the use of force and technology-based surveillance. However, there are key differences between the US and the Indian government's use of technology-based surveillance in Indian-administered Kashmir that can potentially guide policymakers and other stakeholders when it comes to balancing national security with the protection of human rights.

The US surveillance apparatus operates with the stated purpose of ensuring national security, while the Indian government's use of technology-based surveillance in Indian-administered Kashmir is aimed at suppressing dissent and controlling the local population. This includes local administrators instructing shopkeepers in May 2022 to install surveillance camera systems inside their premises – at their own expense – to enhance the local and national police's ability to “[watch people's every move](#)”. In January 2023, Kashmiri locals must carry new digitised family IDs that rights campaigners fear “could lead to [increased surveillance](#) and data hacks”. As per Mehbooba Mufti, an opposition leader and former chief minister of Indian-administered Kashmir, “Kashmiris are viewed [by the Indian government] with deep suspicion, and this is another surveillance tactic to [tighten the iron grip on their lives](#)”. While surveillance cameras are everywhere across the US also, and the state can access personal data from social media companies thanks to programs such as PRISM, as noted above, the targeted nature of surveillance for Kashmiris as compared to people living in other parts of India is discriminatory. The US big brother system operates on a large scale, monitoring vast amounts of data and communications from all over the world, while the Indian government's use of technology-based surveillance in Indian-administered Kashmir is more localised, focusing on monitoring and controlling the activities of the local population. Mass surveillance curtails the possibilities of reporting abuses and leads to fewer activists (or even members of the public) and rights organisations within and outside the country to voice their concerns or advocate on the Kashmiris' behalf. This can also translate into potentially less media coverage of rights violations.

The US surveillance apparatus operates under a legal framework, with laws such as the Patriot Act and the Foreign Intelligence Surveillance Act providing a basis for government surveillance activities. In contrast, the Indian government's use of technology-based surveillance in Muslim-majority Indian-administered Kashmir has been criticised for lacking transparency and accountability, with no or little legal safeguards to protect against abuse of power. To be able to undertake the surveillance, the Hindu nationalist Bharatiya Janata Party (BJP) led-Indian government had to [revoke Article 370¹](#) from the Indian Constitution to be able to do so. Critics

¹ Article 370 granted Jammu and Kashmir a degree of self-rule, including the ability to have its own constitution, flag, and laws, but foreign affairs, defence, and communications remained under the control of the central government. Jammu and Kashmir had the power to create regulations about permanent residency, property ownership, and fundamental rights and could prohibit individuals from other parts of India from buying property or relocating there. However, some Kashmiris are concerned that the BJP seeks to alter the region's Muslim majority by permitting non-Kashmiris to purchase land.

of the move labelled it [unconstitutional and illegal](#) because the Indian government had suspended the Indian-administered Kashmir state assembly. So, there was no due process, and the bill was rushed through the Indian Parliament without the approval of the local assembly, which was necessary for the revocation to go forward (but would have most likely not been given).

On the other hand, the US Congress passed the Patriot Act with [broad, bipartisan support](#), equipping law enforcement with new methods to identify and stop acts of terrorism. The Senate approved the USA Patriot Act with only one opposing vote, and it received backing from 98% of the Senate, while the House of Representatives passed it with a vote of 357-66, gaining support from politicians across the political spectrum.

While the US monitoring programs have triggered controversies, with concerns raised about the significant [erosion of individual privacy and civil liberties](#) for Americans, the Indian government's use of technology-based surveillance in Indian-administered Kashmir has been widely condemned by human rights organisations for its abusive impact on the local Kashmiri population, including even leading to restrictions on freedom of movement, communication, and assembly, freedoms that have been enshrined in both Indian and international law. While both the US surveillance apparatus and the Indian government's use of technology-based surveillance in Indian-administered Kashmir involve monitoring communications and data, the purpose, scale, legal framework, and impact of these practices differ.

With that said, many rights campaigners have also called for a rolling back of the "[post 9/11 surveillance state](#)" as it "vastly expanded the US government's ability to conduct domestic surveillance" and that "over the same period, dramatic advances in technology further bolstered the government's spying powers and rendered decades-old [legal protections obsolete](#)". The Patriot Act was passed after the 9/11 attacks on US soil and allowed "easy governmental access to the private lives of law-abiding citizens", but that has "proven to have scant national security benefit while enabling the [monitoring](#) of racial and religious minorities, protesters, and political opponents", signalling that it was "time for a [course correction](#)".

Policy and Programmatic Recommendations for Effective Governance

It can be said that taking a nuanced approach to the debate between protecting national security and protecting civil rights may potentially bring benefits when it comes to governance. The benefits of technological advancements cannot and should not be ignored when it comes to governance, as technology can significantly reduce human rights

abuses and increase public trust in government by enabling greater transparency, accountability, and citizen participation. By leveraging technology responsibly and ethically, governments worldwide can increase transparency, accountability, and citizen participation, ultimately leading to a more just and equitable society.

What does a nuanced approach look like? Policymakers must carefully consider the potential impact of technology on human rights and take steps to mitigate any negative effects. While acknowledging the importance of protecting national security as a critical function of government, some measures such as surveillance and monitoring of communications can be considered necessary to prevent terrorist attacks and ensure public safety, another key function of a well-functioning government. However, policymakers must also recognise the importance of protecting individual rights and freedoms as excessive government surveillance and monitoring can infringe on not just individual privacy and civil liberties but also lead to the erosion of basic human freedoms and egregious violations such as restrictions on mobility, assembly, and expression.

Taking a pragmatic approach that balances national security and individual rights is likely the most effective approach to the debate between protecting national security and human rights. To achieve this balance, it is important to ensure that security-related policies, laws, and programs have popular consensus across the political spectrum and among the public. This means that policies should be transparent and participatory, with input from all stakeholders, including civil society, human rights groups, and legal experts. Importantly, security-oriented laws, policies and programs must have provisions for periodic evaluations for efficacy and current needs and then updated or revoked as required.

In addition, these policies must be implemented in a way that does not discriminate against any particular group. Policies that target specific ethnic or religious groups, for example, are likely to be ineffective and may even exacerbate the very security threats they are meant to address. Instead, policies should be designed to protect the entire population equally, regardless of race, religion, or other personal characteristics.

Finally, any policies related to national security must be developed within a legal framework that protects individual rights and freedoms. This means that policies must be consistent with international human rights standards, such as the Universal Declaration of Human Rights, and must be subject to oversight and review by an independent judiciary. By ensuring that security policies are developed and implemented transparently and inclusively, without discrimination and within a legal framework, it is possible to strike an effective balance between protecting national security and safeguarding civil liberties. This is especially important given the leaps and bounds by which technology is advancing every year with the likes of artificial intelligence, machine learning, extended reality and many others that have the potential to effectively reshape our world.