

Privacy violations and discrimination in Myanmar

Submission to the UN OHCHR on unequal enjoyment of the right to privacy – May 2025

Introduction

Since the 2021 coup, the military has swiftly turned digital technologies into instruments of repression, systematically collecting and processing personal data to carry out mass surveillance, identify dissent, and crush opposition movements. The military's violations of the right to privacy also strengthen existing inequalities and enable discrimination against ethnic and religious minorities, women, LGBTIQ+ communities, persons with disabilities, older persons, and other marginalised groups.

Human Rights Myanmar submits this report on the situation in Myanmar to the UN High Commissioner's global review of discrimination and unequal enjoyment of the right to privacy, under Human Rights Council Resolution 54/21.

Privacy and data protection in Myanmar

Myanmar's military has demolished any semblance of legal or institutional safeguards for privacy since seizing power in 2021. Although the 2008 Constitution nominally guarantees privacy of "home, property, correspondence and other communications," no comprehensive data protection law exists, and authorities routinely override any residual protections.

Cyber Security "Law"

The centrepiece of this erosion is the [Cyber Security "Law."](#) enacted in 2025. Instead of safeguarding personal data, it mandates that all digital platforms retain users' information—names, phone numbers, IP addresses, browsing logs—for three years and hand it over on demand to military authorities. Earlier drafts included data protection clauses, but these were stripped out or shifted to the Electronic Transactions Act, leaving a fragmented and contradictory framework. Under this cyber law, security agencies intercept private communications and track locations without warrants. Appeals against surveillance or takedown orders go to military-controlled bodies, not independent courts, making every data request opaque and arbitrary.

Even before the 2025 law, the military laid the groundwork for mass surveillance. In late 2020, telecom operators and ISPs were compelled to install “lawful intercept” spyware, enabling eavesdropping on calls, texts, emails, and geolocation tracking. Though presented as a crime-fighting measure, the system was used to identify and silence political opponents. Since the coup, the military has imposed localised internet and mobile-data shutdowns—especially in conflict zones—cutting off entire communities from independent news and family networks, thus violating both privacy and information rights.

Great Firewall of Myanmar

By mid-2024, the military targeted nearly every privacy-protecting technology. A nationwide VPN block was enforced using Chinese Deep Packet Inspection (DPI) devices that detect and block encrypted traffic. As a result of the new “[Great Firewall of Myanmar](#)”, about four million social media interactions abruptly disappeared in the first few months, and over 300 major Facebook pages lost approximately 30 per cent of their engagement. Simultaneously, platforms like Facebook, WhatsApp, X, and Instagram have been repeatedly blocked or throttled. These measures force users onto state-sanctioned networks or unencrypted channels, stripping them of anonymity and exposing them to constant monitoring.

The military has also imposed broad licensing requirements on non-State actors. Any entity offering “cybersecurity services”—a term so vaguely defined it could include NGOs or individual consultants—must obtain a special license or face fines, imprisonment, or shutdown. Platforms with over 100,000 users must secure government approval, which remains undisclosed and is governed by military committees rather than courts. Through this regime, the junta can inspect, suspend, or ban virtually any website or app on vague “cybersecurity” grounds. Most telecom and internet companies, many of which are already directly or indirectly controlled by the military, comply to avoid being cut off entirely.

Military influence

Control over telecommunications infrastructure compounds these abuses. Major providers, including State-owned MPT, military-owned MyTel, and other notionally independent vendors, operate under military influence. Before Telenor’s forced sale in July 2022 to a military-linked buyer, executives had warned that there were no legal safeguards for customer privacy. Now, SIM re-registration requires linking every phone number to a National Registration Card (NRC) and a facial photograph.

In sum, Myanmar’s military regime has created a near-total surveillance state. Through draconian cyber laws, infrastructure control, and sophisticated monitoring technologies, the military has eliminated any practical distinction between private and public life online. With no independent oversight, every digital interaction—from phone calls to social media browsing—is subject to interception, censorship, and punishment. The right to privacy, once constitutionally guaranteed, has been reduced to a hollow promise, replaced by a pervasive apparatus of state surveillance and control.

Discriminatory data collection and processing

The military-controlled State and private actors in Myanmar harvest and utilise personal data in ways that can single out marginalised communities. These practices have deprived specific groups of their privacy, exacerbating existing social divisions.

SIM registration and metadata sharing

In March 2022, the military mandated that all mobile users re-register SIM cards with accurate National Registration Card (NRC) numbers, full legal names, residential addresses, and facial photographs. This directive applied to every telecom operator in the country—Telenor, MPT, Mytel, and others—and required in-person verification or digital uploads of identity documents.

People were told the measure aimed to curb fraud, but it was clear that the military intended to tie people to their digital identities so that the military could conduct mass surveillance of the population. The measure would also increase fear and lead to increased self-censorship and a chilling effect on people's free use of digital technologies.

Some of the data collected by telecoms operators is deeply personal, and collecting it is unnecessary to prevent fraud. Rather, it would enable the potential to discriminate. For example, people were required to provide operators with information about their protected characteristics.

In practice, the measure also disproportionately excluded people without NRC cards from buying SIM cards and accessing the digital space, including Rohingya Muslims and other stateless groups. As thousands of Rohingya discovered their SIM cards deactivated overnight in Rakhine State, they lost the ability to communicate with each other or access information such as on education and health, isolating them physically and digitally.

Compounding this exclusion, telecom operators are forced to hand over call logs, text metadata, and real-time geolocation data to military intelligence. Millions of people saw their personal communications harvested without judicial oversight, creating digital fingerprints that the regime could exploit to target critics and minority-group members.

Deep Packet Inspection and VPN blocks

The military directed telecoms operators to install Deep Packet Inspection (DPI) sourced from Chinese vendors. Once activated, DPI identifies and throttles unencrypted and encrypted traffic, making secure messaging apps (Signal, Telegram, WhatsApp) and virtual private networks (VPNs) effectively unusable for most users.

In May 2024, the military used DPI to turn on a VPN block, establishing the "[Great Firewall of Myanmar](#)". Within the first few months, the new system [blocked](#) roughly four million social-media interactions and causing more than 300 major Facebook pages to lose about 30 per cent of their engagement.

This technical blockade violated the right of every user to access the internet freely. But it also had a distinctly discriminatory impact. Ethnic-minority communities, such as in Chin, Kachin,

and Rakhine States—already isolated by geography—relied heavily on VPNs to communicate securely with relief agencies or human rights monitors. The VPN ban cut these channels, leaving minorities unable to coordinate medical evacuations or document atrocity crimes.

In Myanmar, there are concerns that DPI filters are configured to impede encrypted communications in specific areas dominated by ethnic minorities and communities that support the movement opposing the military, while leaving regime-approved content unobstructed.

In contrast, regime-aligned elites in major cities often use technology and digital knowledge to circumvent DPI. That digital isolation deepened existing inequalities, as rural and minority populations became uniquely vulnerable to surveillance and reprisal.

AI-enabled facial recognition

Under its “Safe City” initiative, the military has installed CCTV cameras in Yangon, Mandalay, and other urban centres. Chinese firms such as Huawei supplied video analytics technology capable of identifying individuals by matching live footage against mugshots in military police databases.

Within months of installation, there were allegations that individuals from ethnic minority groups were being flagged by these CCTV cameras based on their clothing, and subsequently detained without charge, held incommunicado for weeks.

There are also concerns that the AI systems being used by the military use training datasets consisting largely of ethnic Bamar men’s faces drawn from historical arrest records. As a result, these systems would exhibit higher false positives for women and ethnic minorities, leading to disproportionate stops and detentions. Such errors illustrate how advanced surveillance tools—ostensibly designed for “public safety”—are repurposed to target ethnic minorities, exacerbating historical patterns of discrimination.

Commercial spyware and targeted mobile surveillance

The military and military-controlled security services have used commercial spyware to compromise devices belonging to temporarily and permanently detained individuals, including journalists, human rights defenders, and minority rights activists. They have also used spyware to remotely infect devices, exfiltrating a person’s contacts, location history, and private chat logs, and sending them to a military-controlled server.

This data is later used by the military and military allies to identify a person’s home, detain them, and subject them to torture or cruel, inhuman and degrading treatment. There are concerns that the data is purposefully used to encourage discrimination, too. For example, the military uses intercepted data of an intimate nature to shame women in front of their community.

Predicting hidden practices

Given the military's complete opacity and history of weaponising ordinary administrative processes, it is highly probable that more invasive, AI-driven profiling and data sharing schemes are operating or are being developed in secret. For example, the military's longstanding practice of conducting door-to-door "voter" registration in ethnic villages—collecting fingerprints, iris scans, and family lineage data—likely feeds into centralised computer systems that assign "risk scores" based on ethnicity, inferred political affiliations, and biometric characteristics. The military will likely develop opaque algorithms to inform periodic sweeps of potential opposition supporters, leading to extra-legal "interviews" or arbitrary detentions.

Furthermore, data gathered by public service portals—such as welfare disbursement systems or electronic health records—may be discreetly shared with military intelligence to blacklist dissenting families from access to State support. Without transparency, freedom of information mechanisms, or independent auditors, these practices will remain unseen.

Conclusion

Since the 2021 coup, Myanmar's military has weaponised digital tools—enacting the 2025 Cyber Security Law to force data retention, deploying Deep Packet Inspection to block encryption, and installing AI-enabled surveillance—to dismantle any remaining privacy protections. These measures target everyone but have a particular discriminatory effect on ethnic and religious minorities, women, LGBTIQ+ persons, people with disabilities, and older individuals, transforming everyday technologies into instruments of repression. The absence of independent oversight means that every digital interaction is subject to arbitrary interception, censorship, and punishment. This constitutes a deliberate strategy of digital repression rather than inadvertent policy failure.

Recommendations

- **Expose intentional digital repression:** The High Commissioner should publicly characterise Myanmar's digital surveillance regime as a purposeful tool of repression and present these findings to the Human Rights Council.
- **Advocate targeted sanctions:** Urge Member States to sanction military officials and military-linked entities responsible for supporting and enforcing oppressive cyber legislation and procuring surveillance technologies.
- **Engage technology providers:** Call on the High Commissioner to advise companies supplying DPI, facial-recognition, or spyware to immediately suspend all activities supporting Myanmar's security apparatus.
- **Monitor and report:** Establish systematic UN-backed documentation of internet shutdowns, VPN bans, takedowns, and spyware incidents, incorporating input from civil society and technical experts.