



## INCLO input for UN report: Global surveillance tech expanding faster than its legal, ethical and human rights safeguards

In response to the request by the UN Special Rapporteur on the rights to freedom of peaceful assembly and association (FOAA) for inputs for her upcoming thematic report, INCLO prepared a submission that represents the collective expertise of 16 national human rights organizations, with contributions from 10 different countries.

Our document illustrates how global surveillance technologies, including AI-assisted facial recognition, body-worn cameras, drones, CCTV, spyware, and social media monitoring, are expanding faster than the legal, ethical, and human rights safeguards that govern them. These tools disproportionately target marginalized groups, chill free expression and protest, and entrench state power while undermining democratic participation.

We collectively call on States to mandate human-rights impact assessments, ensure transparency, independent oversight, bias mitigation, and remedies for affected individuals, and limit intrusive technologies to protect privacy, assembly, and civic engagement. Urgent, coordinated action is needed to align technological expansion with democratic accountability and safeguard inclusive public life.

## Digital and AI-powered surveillance

Governments often invoke national security, public order, or emergency response to justify the expansion of digital and AI-powered surveillance, deployed without transparent legal frameworks, meaningful oversight, or effective human-rights safeguards. As a result, tools such as facial recognition, biometric databases, predictive analytics, drones, and social-media monitoring are producing significant chilling effects that deter people from protesting, organizing, or participating in civic life.

Across all countries, common patterns emerge. Digital surveillance disproportionately targets marginalized communities and social movements, compounding inequality and undermining inclusive civic participation. Oversight bodies often lack independence or resources. Procurement and deployment remain opaque, enabling authorities to expand surveillance powers without public debate. Most significantly, fear of being monitored, profiled, or misidentified discourages individuals from exercising core democratic rights. The cumulative effect is a contracting civic space in which protest, association, and free expression become increasingly fraught.

## Facial Recognition Technology (FRT)

Governments now deploy facial recognition technology (FRT), behavioural analytics, high-definition camera networks, and algorithmic processing to monitor public spaces. Although framed as tools for safety and crime reduction, these technologies increasingly enable authorities to track protesters, suppress civic participation, and facilitate targeted repression. Across all contexts, AI-assisted surveillance transforms public life by eliminating anonymity, facilitating mass monitoring, and embedding discrimination into automated decision-making.

Existing laws rarely regulate FRT adequately, leaving major gaps that enable deployment without transparency or accountability. Oversight bodies warn that, without coherent policy, core principles of fairness, proportionality, and non-discrimination remain unprotected. International jurisprudence, including the *Glukhin v. Russia* recognizes that such intrusive monitoring can violate rights to privacy, expression, and peaceful assembly. Without strict legal safeguards and independent oversight, FRT threatens fundamental democratic freedoms.

## Body-Worn Cameras, Drones, and CCTV

Body-worn cameras (BWCs), drones, and CCTV have become core components of modern policing. Their expansion is often justified in the name of transparency, efficiency, or public safety, yet the legal frameworks governing their use lag far behind.

The result is pervasive, mobile, networked surveillance with uneven safeguards and significant risks for civil liberties.

Police agencies typically retain broad discretion over when devices are activated, how long data is stored, and who can access recordings. This discretionary framework, combined with opaque procurement and frequent partnerships with private companies, creates apparent risks of selective recording, discriminatory enforcement, manipulation of footage, and lack of accountability. Increasingly, public and private camera systems are integrated into unified monitoring platforms, often equipped with AI analytics or facial recognition. Although some deployments, such as São Paulo's BWC program, demonstrate that strict safeguards can reduce police violence, most global deployments lack the transparency and oversight necessary to safeguard rights.

## Cyber-Patrolling & Social-Media Monitoring

Social media, central to contemporary organizing and political expression, has become a primary domain for state surveillance. Governments increasingly use AI-enabled systems to extract, analyze, and store data from public and private online spaces. These systems frequently operate without judicial authorization, legal clarity, or oversight, and are routinely used to profile political opponents, Indigenous communities, journalists, students, and activists. These practices normalize state monitoring of civic life and undermine democratic participation by creating widespread fear of retaliation.

## Spyware

Spyware represents one of the most covert and intrusive forms of state surveillance. Tools such as Pegasus and Circles enable remote access to phones, messages, and location data without a user's knowledge. Although marketed for national security, spyware is routinely used to monitor domestic critics. Spyware undermines the confidentiality necessary for civic organizing and disproportionately violates the rights of those challenging state power.

## Encryption

End-to-end encryption is essential for digital security and a fundamental safeguard for protest organizers, journalists, and the general public. Yet governments increasingly seek to weaken encryption by mandating exceptional-access systems or "backdoors."

Ireland's proposed legislation granting police access to encrypted communications reflects a wider global trend that would expose entire populations to increased surveillance and cybersecurity vulnerabilities. International human-rights bodies

consistently warn that undermining encryption threatens privacy, expression, and the ability to organize safely.

## Conclusion

Without strong legal limits, independent oversight, and mandatory transparency, the expansion of surveillance technologies risks entrenching a new era of ubiquitous surveillance that threatens the freedoms necessary for democratic participation.