GNI Policy Brief on Government Interventions in AI:

ONE PAGER (GOVERNMENTS)

The Global Network Initiative (GNI) is a multistakeholder initiative focused on safeguarding freedom of expression and privacy in tech. In October 2025, GNI and its multistakeholder AI Working Group (AIWG) launched a Policy Brief to aid understanding of the human rights implications of government interventions in artificial intelligence AI ("Brief"). The Brief presents a taxonomy of five types of government interventions—hard and soft governance, investment, procurement, and informal influence—across the AI value chain of infrastructure, development, and deployment, with illustrative examples from diverse regions.

The Brief highlights how government interventions in AI can both advance and undermine the rights to freedom of expression, privacy, and non-discrimination. Positive measures—such as mandatory human rights assessments, risk-based regulation, privacy laws, inclusive investments, and rights-focused procurement—can strengthen protections, while overbroad censorship, discriminatory surveillance, restrictive export controls, and weak legal safeguards risk violating rights and deepening inequality.

The Brief concludes with recommendations for governments, companies, and civil society, encouraging all sectors to use international human rights law as a basis for developing and analyzing interventions that impact human rights. The recommendations made to **governments** include:

Adopting Rights-Based AI Governance: Governments should adopt a rights-based AI governance framework, ensuring that human rights principles are embedded throughout the development and use of AI systems by all parties through laws, regulations, institutions, mandatory risk-based assessments for AI developers and deployers, accessible remedies, and engagement in multilateral / multistakeholder AI governance initiatives.

Rights-Protecting Restriction of Information: Restrictions should be legal and legitimate in line with the three-part test, as well as being narrowed tailored to focus on illegal content. Governments should be cautious about shifting legal liability for AI-generated content to intermediaries, as this may incentivize over-removal and over-censorship, and should permit independent adjudication for illegal content in conformity with due process norms.

Rights-Protecting Surveillance: AI-enabled data collection and analysis must be legal, with appropriate transparency, independent oversight, and remedy/accountability mechanisms to guard against misuse. Data collection should be minimised, user anonymity permitted, strong data protection laws enacted, and safeguards adopted for any user data requests.

Tailored Export Controls: Export restrictions should consider human rights impacts, informed through meaningful engagement with and adopting recommendations from civil society. Such controls should additionally restrict dual-use AI to states with documented human rights violations, be narrowly targeted, and permit international collaboration for rights-respecting uses.

Rights-Protecting Sovereign AI: Sovereign AI initiatives should be grounded in rights-based governance frameworks, be inclusive, ensure equitable access through open tools and literacy programs, and promote economic inclusion, especially in underserved regions.

Rights-Protecting Public Sector Use Cases: Public sector bodies should avoid AI in high-risk applications, mitigate lower-risk impacts, maintain a public inventory of AI use cases, implement remedies, and engage meaningfully with civil society and affected communities.