GLOBAL NETWORK INITIATIVE

GNI Submission to the UK Joint Committee on Human Rights' Inquiry on Human Rights and the Regulation of AI

About the Global Network Initiative (GNI)

The Global Network Initiative (GNI) is a multistakeholder organisation comprising leading technology companies, civil society organisations, academics, and investors. Our mission is to protect and advance freedom of expression and privacy rights in the technology sector worldwide. We develop and promote rights-based expectations for responsible business conduct, facilitate collective learning across key stakeholder groups, and advocate for regulatory and policy frameworks grounded in international human rights law.

GNI members operate and engage across diverse jurisdictions and sectors, giving us unique insight into both the opportunities and risks presented by AI systems. Our approach combines legal expertise, technical understanding, and practical experience in implementing human rights safeguards.

Over the last several years, GNI has reviewed, commented on, and helped shape a range of "online safety" bills across several jurisdictions. Our human rights analysis and recommendations for policymakers considering how best to address digital harms can be found in our Content Regulation & Human Rights Policy Brief, which uses international human rights principles to analyze a wide range of legislative efforts and provides proactive guidance on how to address online safety in a rights-protective manner. Furthermore, through its multistakeholder AI Working Group, GNI is currently developing a Policy Brief on Government Interventions in AI, which analyses a taxonomy of such interventions through an international human rights law lens.

Human Rights as a Core Framework for AI Governance

GNI applauds and welcomes the Committee's explicit framing of this inquiry around human rights, which we believe is the correct and essential lens for understanding and governing AI. By grounding AI regulation in human rights, the UK can uphold its obligations under international human rights law, including the right to privacy, equality, due process, non-discrimination, freedom of opinion and expression, and access to remedy. This approach also reinforces public legitimacy: people are more likely to trust AI systems when they see that their fundamental rights are respected, protected, and enforceable.

The Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the European Convention on Human Rights (ECHR), the UN Guiding Principles on Business and Human Rights (UNGPs), and the OECD Guidelines for Multinational Enterprises on Responsible Business Conduct (OECD Guidelines) provide a well-established, globally recognised foundation for aligning technological innovation with societal values. In addition, the guidance coming from the UN General Assembly and the Human Rights Council – particularly resolutions such as S*eizing the Opportunities of Safe, Secure and Trustworthy Artificial Intelligence Systems for Sustainable Development* (A/RES/78/265), the *Right to Privacy in the Digital Age* (A/RES/79/175), *New and Emerging Technologies and the Enjoyment of Human Rights on the Internet* (A/HRC/RES/47/23) – along with the work of the Office of the High Commissioner for Human Rights (OHCHR) and the Human Rights Council's Special Procedures, provides critical direction for ensuring that digital and AI technologies are developed and deployed in ways that uphold human rights.

Indeed, human rights frameworks have already provided an essential baseline for assessing AI-related technologies in the UK. For instance, in Bridges v South Wales Police [2020] EWCA Civ 1058, the UK's Court of Appeal held that the police's deployment of live facial recognition technology was unlawful because it lacked adequate safeguards, breaching rights to privacy and equality under Articles 8 and 14 of the ECHR. Keeping human rights frameworks at the centre of AI governance will enable the safeguarding of human rights during the whole lifecycle of the technology.

The Committee's decision to focus this inquiry on rights impacts provides an opportunity for the UK to demonstrate that technological innovation, economic growth, and rights protection are mutually reinforcing, and not competing, objectives. The Committee's approach must also supplement the UK's Government's AI Opportunities Action Plan (January 2025), which focuses on economic growth and adoption, without sufficient reference to human rights safeguards, such as enforceable accountability mechanisms, independent oversight structures, or clear remedies for individuals adversely affected by AI.

Existing Legal and Regulatory Frameworks Relevant to AI

The UK already has a number of legal and regulatory tools relevant to AI and its possible human rights impacts, including:

- UK GDPR and the Data Protection Act 2018, overseen by the Information Commissioner's Office (ICO).
- Equality Act 2010, enforced by the Equality and Human Rights Commission (EHRC).
- Consumer Rights Act 2015, Competition Act 1998, overseen by the Competition and Markets Authority (CMA) and its Digital Markets Unit (DMU).
- Sector-specific regulations: The Financial Conduct Authority (FCA) in finance; the Medicines and Healthcare products Regulatory Agency (MHRA) in healthcare; and Ofcom in communications and online safety.

While these existing frameworks already apply to AI in many contexts, they were designed before the emergence of advanced AI models, including foundation models and agentic AI systems with autonomous decision-making capabilities.

A few examples may help to illustrate how existing laws may apply and where they may be insufficient to address real world, AI-related impacts:

- Recruitment: Research by the UK's Centre for Data Ethics and Innovation (CDEI) found that recruitment platforms using automated tools risk embedding gender and racial biases, even when anonymisation techniques are applied. This illustrates how equality law intersects with AI governance.
- Policing: Live facial recognition technologies trialled by UK police forces raised significant privacy and equality concerns. Existing laws, such as the Data Protection Act 2018 and equality law can be applied, but have not provided clear, tailored standards for biometric AI.
- Financial services: Credit scoring and fraud detection increasingly rely on machine learning. These fall under the Financial Conduct Authority's remit, as well as consumer protection law, but current rules do not always require transparency about how algorithmic decisions are made, creating risks around due process and fairness.

The UK must ensure that the development of any new regulations or institutions remain consistent with international human rights obligations and in line with the approach that has been pursued in the setting of the UN AI governance mechanisms, and the commitments in the Sustainable Development Goals, the Pact for the Future and the Global Digital Compact.

Any laws, regulations, or policies developed to fill existing gaps or create new authorities and/or institutional capacity related to AI governance, must be consistent with the UK's domestic and international human rights obligations.

Ofcom's role under the Online Safety Act exemplifies how statutory duties, codes of practice, and enforcement authority can be structured in a dynamic and technically intricate field. However, concerns persist regarding whether Ofcom possesses sufficient capacity – and any future AI-focused regulator would likewise demand substantial expertise and resources to be effective. The Act's requirement for Human Rights Impact Assessments for each proposed mitigation is a commendable practice that the UK's AI Governance Framework could adopt, along with the emphasis on coordination among multiple regulators.

In September 2024, the UK signed the Council of Europe's Framework Convention on AI, Human Rights, Democracy and the Rule of Law. The Convention requires member states to integrate safeguards on rights, democracy, and rule of law into AI governance, and its provisions on risk assessment, transparency, and remedies should guide domestic implementation. This may be a useful and grounding framework as the UK buildings AI governance frameworks.

Some elements that a UK AI Governance Framework might consider, consistent with human rights principles and practice, include:

- Encouraging Human Rights Due Diligence: A human rights framework would ensure that AI governance is principles-driven, not solely risk-driven. Human rights due diligence (HRDD) is an established methodology and good practice that is set out in the OECD Guidelines and the UNGPs. HRDD is, at its core, a methodology for conducting ongoing, human rights-centred risk management. This approach has helped companies and other non-governmental actors across a wide range of contexts identify and address potential harms before they occur. It also highlights the importance of engaging with key rights holders, especially those who are particularly vulnerable to human rights impacts, thereby strengthening public trust, facilitating responsible innovation, and aligning UK leadership with its international obligations.

- Clear accountability and transparency across the AI lifecycle: Require documentation, transparency and traceability of training data sources, and disclosure of system capabilities and limitations (proportionate to risk).

- Effective grievance redressal: Provide individuals with accessible pathways to challenge AI-driven decisions, obtain meaningful explanations, and seek remedies, including collective redress for systemic harms.

- Participatory, multistakeholder, and multidisciplinary participation: Involve civil society, academia, and affected communities in the design, implementation, and review of AI governance measures. Ensure inclusion of traditionally marginalised groups and diversity of perspectives and fields of expertise from hard to social sciences.

These are some ingredients that would be useful as a starting point for the UK to ensure that they adopt a human rights-led, adaptable AI governance model anchored in human rights, capable of responding to emerging AI risks, and designed to foster public trust alongside innovation. GNI remains eager and open to engage in dialogue with the Committee and to support the development of such a framework by sharing insights from our multistakeholder membership and experience across diverse regulatory contexts.