Principles on Artificial Intelligence Adoption in the Telecommunications Industry

Joint statement between the United Kingdom, Australia, Canada, Japan and the United States of America on Artificial Intelligence (AI) adoption by the telecommunications industry.

Through the Global Coalition on Telecommunications (GCOT),[1] the United Kingdom, Australia, Canada, Japan and the United States of America are cooperating to support innovation in telecommunications technologies in a way that will enable security, growth and societal benefits in all our jurisdictions.

GCOT partners recognise that the use of AI in telecommunications represents a significant opportunity for innovation. These include improved network performance and efficiency, strengthened security, and enhanced customer experiences, as well as new applications and revenue opportunities. At the same time, GCOT partners are committed to ensuring AI is adopted in a safe, secure and trustworthy way, protective of individual rights and respectful of intellectual property rights. This joint statement sets out principles for the responsible use of AI in telecommunications operations, and is intended for industry leaders, researchers and those developing AI solutions for telecommunications. GCOT partners would welcome further efforts from industry and academia to progress AI in telecommunications in line with these principles.

Context

Since the mid-2000s, telecommunications companies have adopted AI technologies and their precursors, deploying them across different aspects of operations to improve performance and reduce costs, from network design to optimisation of customer experiences. In the next decade and beyond, as Future Networks are developed, AI's role is expected to expand significantly as telecommunications networks become "AI native," meaning that AI and data infrastructure will be fully integrated across all components, rather than as add-ons to existing non-AI-based entities.

This integration of AI across public and private telecommunications networks promises to help manage network complexity and service delivery, and optimise resource allocation. One component of these improvements is edge inferencing, which allows AI to process data locally, enabling real-time decision-making and reducing latency. These advances can support the industry by providing faster, more reliable, and secure connectivity, driving economic growth, promoting digital inclusion, and enhancing infrastructure resilience. At the same time, the adoption of advanced AI systems into telecommunications networks should address safety, security and privacy. The adoption of AI advances the complexity of network security and potential attacks,

[1] https://www.gov.uk/government/publications/global-coalition-on-telecommunications-joint-statement-of-intent-between-uk-australia-canada-japan-and-us/global-coalition-on-telecommunications-joint-statement-of-intent

introducing new risks or potentially exacerbating existing ones. These risks necessitate management of the integrity, confidentiality and accessibility of AI systems being implemented.

To realise the benefits identified while mitigating the risks, GCOT partners share the view that telecommunications providers need to take appropriate measures to ensure the safe, secure and trustworthy integration of AI technologies in their operations. This includes working with our respective domestic regulatory bodies, where appropriate, to ensure compliance and responsible implementation.

There have been several international efforts in recent years with the aim of ensuring the safe and responsible development of AI as a technology. The OECD's AI Principles,[2] adopted in 2019 and revised in 2024, have been pivotal in establishing a global framework for AI governance, emphasising inclusivity, transparency, robustness and accountability. Since then, the G7 leaders' commitment on the Hiroshima Process International Guiding Principles and Code of Conduct for Organizations Developing Advanced AI Systems,[3] the Bletchley Declaration,[4] and the Seoul Declaration[5] have focused on advanced AI systems and addressed specific challenges these systems pose, with an emphasis on risk management, international cooperation, safety, privacy and accountability. The UK's National Cyber Security Centre has also published its Guidelines for Secure AI System Development,[6] developed with the United States Cybersecurity and Infrastructure Security Agency (CISA) and agencies from 17 other countries, including Australia, Canada and Japan.

In parallel, there have been significant industry efforts regarding adoption of AI in telecommunications. The ETSI Technical Committee on Securing Artificial Intelligence (SAI)[7] has been instrumental in developing technical specifications aimed at mitigating security threats, including guidelines for securing AI models and an ongoing technical report on security aspects of using AI/ML techniques specifically within the telecom sector.

The Next Generation Mobile Networks Alliance has published its guidance *Automation and Autonomous system Architecture Framework – Phase 2*[8] which provides guidance on the use cases, requirements, and architectural principles for implementing AI-driven autonomous networks. The Global System for Mobile Communications Association has

---

[2] https://oecd.ai/en/ai-principles
[3] https://www.soumu.go.jp/hiroshimaaiprocess/en/index.html
[4] https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023
[5] https://www.gov.uk/government/publications/seoul-declaration-for-safe-innovative-and-inclusive-ai-ai-seoul-summit-2024/seoul-declaration-for-safe-innovative-and-inclusive-ai-by-participants-attending-the-leaders-session-ai-seoul-summit-21-may-2024
[6] https://www.ncsc.gov.uk/collection/guidelines-secure-ai-system-development
[7] https://www.etsi.org/committee-activity/activity-report-sai
[8] https://www.ngmn.org/publications/automation-autonomous-framework-phase-2.html

launched the *Responsible AI Maturity Roadmap,*[9] a structured governance framework designed to help the industry adopt responsible AI practices.

Principles

The aim of these principles is to support relevant stakeholders involved in the development and deployment of Future Telecommunications technologies as AI systems and tools are used across their operations.

This joint statement sets out the principles that will help align and guide our shared efforts on AI adoption in telecommunications, identifying how to seize the opportunities presented by AI alongside mitigating harms and security risks. Their purpose is to highlight the importance of these considerations and the evaluation of the trade-offs involved when adopting AI systems and processes in telecommunications operations. Those deploying and developing AI for use in communications should consider the use cases and operations to which these principles are relevant.

1. Innovation and Competition

> *AI systems in telecommunications should be leveraged to drive innovation and promote a competitive, innovative telecommunications market, while respecting Intellectual Property Rights*.

Promoting innovation and competition is crucial for technological advancements that support a dynamic market and address the commercial challenges faced by the industry. Innovation in telecommunications means optimising network performance, enhancing security, and automating resource management across diverse platforms, promoting flexibility and scalability. AI-driven solutions should be flexible enough to scale up without sacrificing performance, ensuring that AI can manage both small local networks and different types of large, global telecom infrastructures, especially 5G and future generations of networks where devices - such as IoT devices, machines, and autonomous systems - scale up exponentially. Collaborative practices, such as federated learning, enable SMEs to train AI models while maintaining data privacy by avoiding direct data sharing. Competition ensures a diverse market with multiple players, leading to better services and prices for consumers, and reducing dependency on a few suppliers. GCOT partners encourage investing in the infrastructure, access to data, skills, and R&D that drive innovation, promote interoperability, respect intellectual property rights, and support the scaling of new market entrants within telecommunications supply chains. Regulatory measures applicable to AI systems used in telecommunications networks should be non-discriminatory and no more trade restrictive than necessary to achieve legitimate objectives.

[9] https://www.gsma.com/solutions-and-impact/connectivity-for-good/external-affairs/responsible-ai/

2. Transparency, Explainability and Human Oversight

> *AI systems in telecommunications should prioritise transparency and explainability in a timely manner, ensuring clear disclosure and understandable decision-making processes to build trust and accountability.*

Ensuring AI systems in telecommunications prioritise meaningful transparency and explainability is crucial for building trust, accountability, and means of redress, especially due to telecommunications' role handling critical functions, such as traffic management, resource allocation and security responses. Transparency can involve disclosing AI use and providing clear information about AI-driven decision making and training data lineage. This is valuable for a range of stakeholders, including end-users, network operators, intellectual property owners, regulators and other entities with legitimate interests. For example, when customers are interacting with an AI system to answer billing questions, it ensures that customers know they are interacting with an AI system, understand how it comes to its decisions, and have means of redress should a mistake occur. Transparency should be prioritised across the telecommunications supply chain, ensuring suppliers of AI systems provide clear information about who developed the system, the methods used in its creation, the sources of training and test data, and the best practices and standards followed.

Important practices include establishing robust governance structures, engaging stakeholders throughout the AI lifecycle, implementing regular audits, third-party tools, information sharing across the value chain, clear documentation, and independent evaluations and providing public redress for affected individuals through simple and effective mechanisms when an organisation has caused or contributed to adverse impacts.

Explainability refers to the extent to which it is possible for relevant stakeholders to access, interpret and understand the decision-making processes of an AI system. For example, when systems reroute network traffic to prevent congestion or allocate bandwidth to prioritise certain services, it ensures decision-making can be understood and allows results to be challenged.

Another important consideration is to ensure AI systems retain human oversight and intervention for critical functions and decisions with large-scale implications. This means balancing support for real-time automated recovery and self-healing with fail-over mechanisms, including 'kill-switch' scenarios, so that humans can intervene or override AI decisions. This allows human expertise to maintain meaningful control over an autonomous system, able to guide or make alternative decisions affecting the workflow and execution of these functions.

3. Privacy

> *The use of AI systems in telecommunications should uphold privacy, safeguarding user data and protecting individual rights.*

Ensuring user privacy in AI systems is essential for the telecommunications industry to uphold individuals' rights, protect the assets of providers when using or sharing data with third parties, and maintain regulatory compliance and legal obligations. Privacy involves robust and appropriate governance measures that inform users of data collection, safeguards user data and ensures that AI systems - especially those leveraging advanced capabilities like joint sensing and communications strands - handle personal information responsibly, if it needs to be handled at all. In practice, this means using privacy-preserving technologies and implementing robust data governance and management practices, including data minimisation and continual monitoring and auditing processes. It also means adopting continuous improvement practices that will enable safeguards and ensure that AI systems align with evolving normative and legislative privacy requirements.

4. Fairness

> *The use of AI systems in telecommunications should uphold fairness, striving to minimise unwanted bias for equitable outcomes.*

In telecommunications, fairness ensures that AI systems address the specific needs of diverse user groups, mitigating disparities and fostering inclusivity across different economic statuses and geographic locations. Fairness involves implementing governance measures that identify and mitigate biases in AI systems, ensuring that all individuals and groups are treated justly. In practice, this will include engaging with a broad range of stakeholders to define what constitutes fair and equitable outcomes, conducting pre- and post-release audits, using diverse and representative datasets, and ensuring transparency in decision-making processes. This will involve efficient transparency disclosure between developers of AI systems and those deploying them in the telecommunications sector. This includes information on the provenance of training data used to create it, how the AI system was tested, if and how bias mitigation has been applied, and the scope of the system in question. This information sharing will enable telecommunications providers to fully contribute to fostering trust and inclusivity in their operations.

5. Security and Resilience

> *AI systems in telecommunications should be designed to protect against cyber threats, ensuring data integrity and maintaining operational stability.*

AI-driven systems can monitor traffic patterns and detect anomalies indicative of potential security risks, enabling faster responses to breaches. AI can also be leveraged to enhance resilience against a variety of hazards, including natural disasters and

system failures, ensuring continuous operation and rapid recovery in diverse scenarios. At the same time, we must ensure that AI systems and processes are deployed with security built in by design and by default. Security and resilience requirements in AI systems are crucial for telecommunications operators to protect against cyber threats and maintain operational stability, ensuring minimal interruption to service delivery for business continuity and national critical services continuity plans. Without security, the continued rapid adoption and embedding of AI could result in vulnerabilities to adversarial attacks, such as poisoning of training datasets and backdoor attacks. These systems must also be able to withstand and recover from disruptions, maintaining continuous operation and avoiding over-dependence. Resilience also requires addressing inherent problems of concept and data drift in AI models, ensuring they remain accurate and effective over time. In practice, resilience entails implementing advanced AI-enabled cybersecurity measures, such as real-time threat detection and automated response systems. It also means deploying models from trusted sources, conducting regular security audits, as well as testing, validation, and verification of adopted AI models before, during and after deployment. It also means sharing, where possible, information on security incidents and vulnerabilities in telecom AI systems affecting multiple networks or operators.

Finally, AI provides new avenues for cyber criminals to conduct fraudulent or malicious activities, such as voice cloning scams or defeat of voice authentication, over telecommunications systems and networks. Telecommunications service providers and operators must continue efforts to implement trusted caller identity programs, share information or indicators of fraudulent activities enabled by AI, and find new ways to cooperate across operators and sectors on timely response.

6. Environmental Sustainability

> *AI systems in telecommunications should be used to improve the environmental sustainability of the network and designed to minimise their own environmental impact.*

The adoption of AI in telecommunications, particularly generative AI, can increase energy consumption and carbon emissions, posing environmental challenges. On the other hand, AI and machine learning algorithms can improve the sustainability of networks by optimising energy consumption and improving efficiency in network design and operations. To achieve this, telecommunications companies will require comprehensive sustainability information from developers, including on AI systems' energy consumption and training data sources. Integrating environmental concerns into cost/reward decisions ensures that AI adoption not only enhances operational efficiency but also aligns with corporate sustainability goals. Environmental sustainability involves minimising the environmental impact of AI systems by improving efficiency, reducing energy consumption and promoting the use of renewable energy

sources. In practice, this means deploying more energy-efficient AI systems and processes, limiting unproductive uses of AI, minimising energy consumption during inference and periods of low activity, using machine learning to optimise data centre operations, and where possible, investing in low or no carbon energy to power AI infrastructure.