Principles for Effective and Reliable Artificial Intelligence in the Americas

The independent third-party conformity assessment industry recommends clear, enforceable principles for the application of Artificial Intelligence to support safe, reliable, and secure consumer use.

Over the next decade, artificial intelligence (AI) will transform the industry of technology assisted living, providing consumers with tools to make their lives easier and more efficient.[1],[2] From self-driving cars and autonomous vehicles to smart algorithms helping consumers find the best prices online, track their health and wellness, and more; consumers will benefit greatly from the advancement of AI.

As with all technological advancements, AI presents risks as well as benefits. Autonomous vehicles whose AI is not working properly or can be cyber-hacked raise concerns of public health and safety. Smart AI which discriminates against protected classes such as the elderly, racial groups or the underserved, would be a detriment to the public good. These risks will require careful review, monitoring, and mitigation to support a system that's benefits outweigh the risks.

A necessary first step to the application of safe[3], reliable, and trusted AI is the establishment of clear and enforceable AI principles. These principles should be applicable to all potential use cases of AI and readily accessible and enforceable by all stakeholders. For these purposes, the TIC Council and its members recommend the following principles for the safe, reliable, and secure use of AI in the consumer space:

1. Fairness – Applications of AI in systems and products should be free from bias to the extent possible and measureable by external evaluators. "AI learns from the data sets used to train it, and if those data sets contain real-world bias then AI systems can learn, amplify, and propagate that bias at digital speed and scale."[4] Through third-party evaluation of AI use cases and using established benchmarks for performance, AI can be tested, inspected, and certified as having the necessary safeguards in place so as not to provide inequitable results to protected classes and disadvantaged groups.

2. Trust and transparency – How applications of AI work should be explainable to include the data considered and the expected outcomes of the AI system based on the data provided.[5] Evaluation of these inputs and outputs by independent third-party conformity assessment bodies builds serves as a beneficial check on the reliability of such use cases, supporting industry in its efforts to bring new products and systems to market and building trust among consumers.

---

[1] ARTIFICIAL INTELLIGENCE AND THE FUTURE OF HUMANS, Pew Research Center, https://www.pewresearch.org/internet/2018/12/10/improvements-ahead-how-humans-and-ai-might-evolve-together-in-the-next-decade/

[2] NIST, Cultivating Trust in AI Technologies, https://www.nist.gov/artificial-intelligence

[3] Artificial Intelligence and Machine Learning in Consumer Products, CPSC, 2021, https://www.cpsc.gov/s3fs-public/Artificial-Intelligence-and-Machine-Learning-In-Consumer-Products.pdf

[4] 'Trustworthy AI' is a framework to help manage unique risk, MIT Technology Review, 2020, https://www.technologyreview.com/2020/03/25/950291/trustworthy-ai-is-a-framework-to-help-manage-unique-risk

[5] Transparency and explainability, OECD.AI, https://oecd.ai/en/dashboards/ai-principles/P7

3. Accountability – Tracking and verification of all steps of the supply chain which lead to the development of AI systems including the application to products and systems is needed to confirm compliance with established cybersecurity, functionality, and safety requirements. Each step should be accessible and traceable, allowing for identification and correction when risks and vulnerabilities are identified. Independent third-party conformity assessment can play a critical role in confirming the compliance of each step in the supply chain, eliminating the need for each manufacturer, software developer, retailer, government agency, or consumer from needing to independently evaluate each step.

4. Privacy and security – Clear and assessable requirements for the protection of data used in AI applications is needed to protect the privacy and security of the data. Additionally, AI applications require careful evaluation to ensure they do not create a cyber vulnerability which could lead to an instance of hacking and cyber intrusion. Use of independent third-party conformity assessment bodies in confirming that AI applications meet necessary safeguards for privacy and security reduces the risk to communities and helps to protect the private data of consumers.

Independent third-party conformity assessment bodies employ over one million individuals (often in high-wage STEM jobs) scattered in more than 160 countries around the globe offering conformity assessment services. [6] Through these highly skilled technical experts, the independent third-party testing, inspection, and certification ("TIC") industry provides governments and industry with access to expertise they may be unable to staff themselves and provides a check on services and products by an impartial arbiter of compliance to government and industry requirements. Through which, consumers can trust and rely on the services and products they purchase.

Incorporating the use of independent third-party TIC organizations into compliance programs for the safe, reliable, and secure application of Artificial Intelligence systems is a cost-effective strategy to protect and support consumers' use of AI-enhanced products and systems.

Contact person: Karin Athanas (kathanas@tic-council.org)

TIC Council is a global association representing over 90 international independent third-party testing, inspection, certification and verification organizations. The industry represents an estimated one million employees across the world with annual sales of approximately USD 200 billion

[6] Value of TIC, TIC Council, https://www.tic-council.org/report-tic