IEEE-USA

POSITION STATEMENT

Privacy, Equity, and Justice in Artificial Intelligence

Adopted by the IEEE-USA Board of Directors (November 2024)

The ubiquitous presence of artificial intelligence (AI) in our society challenges our ability to protect privacy and ensure equity and justice. Generative AI has exacerbated these challenges; such AI systems gather, analyze, and create data independent of existing legal and public policy frameworks around data, privacy, speech, and property. The foundational principles proposed below provide a legal, technical, and public policy framework to address these challenges and resolve problems embedded in existing AI systems – such as when AI systems are trained with data embedded with patterns of inequality and human bias. IEEE-USA recommends updating, harmonizing, and streamlining federal laws, public policies, and guidelines as follows:

1. Data ownership, data rights, and privacy

Equitable AI practices require a clear legislative framework for data ownership, confidentiality, and rights of access to data used in and by AI systems – all essential to protecting privacy and autonomy. The absence of a comprehensive data protection law at the federal level in the United States is a missed opportunity to shape and address data rights, practices, and privacy globally. The current patchwork of federal and state laws lacks coherence and is insufficient.[1]

Internet platforms, apps, and devices routinely collect or infer health, financial, and biometric information without user knowledge, control, or consent. The U.S. sectoral approach to data regulation leaves vast amounts of intimate data unprotected leading to inefficiencies and confusion. Comprehensive data regulation through legislative action should incorporate principles such as Fair Information Practice Principles (FIPPs) that:

- establish data collection and data use limitations, data quality standards, and security safeguards.
- mandate transparency and user control over individual data (Users should have the right to access, review, store, and delete personal data, including behavioral data used for tracking and AI recommendation systems, with an option to opt-out of tracking.),
- require clear notice of data collection practices with effective opportunities for user consent,
- inform users of persistent AI mechanisms that may collect or use their data, and provide options to disable these mechanisms, and
- establish frameworks to hold parties responsible for breach or loss of collected data liable for nonfeasance in practices, to ensure cybersecurity, or customer data privacy.

2. Mitigate disparate impacts of AI

When AI systems are developed and deployed, objectives of accuracy and a lack of algorithmic bias toward marginalized or vulnerable groups can conflict, resulting in disparate impacts and lack of public confidence. To mitigate these harms, objectives must be balanced by means requiring clarity, transparency, and protecting all stakeholders. IEEE-USA recommends:

- mandating metrics and standards for fairness, privacy, safety, and security for AI systems,

- establishing transparency mechanisms for stakeholders. For example, requiring third-party access to data in standardized, machine-readable format,
- investing in research on how the use of algorithms may disparately impact or disadvantage certain individuals and groups,
- establishing mandates against pricing surveillance in accessing online goods and services, and
- restricting dynamic pricing; prohibiting surveillance pricing in accessing goods and services.

3. Ongoing verification and validation of AI systems

Increasingly, AI systems directly impact human life, individual rights and societal well-being, and must be evaluated throughout their lifecycles. When AI systems are deployed in critical applications, such as employment, credit/finance, criminal justice, health systems, and allocation of public resources, IEEE-USA recommends:

- requiring transparency about the training data and other developmental inputs,
- requiring and encouraging use of mechanisms for independent verification and validation,
- investing in research to understand and probe AI decision-making processes (such as research) in explainable AI -- to enable algorithm functionality analyses, outputs and outcomes, and
- disclosing the use of AI decision-making processes to impacted parties, when a decision is made affecting them.

4. Redress

When AI systems make life-impacting decisions, individuals must be informed about, and permitted to, question decisions, and have access to systems enabling redress. IEEE-USA recommends:

- defining pathways for all stakeholders to report problems, question results, provide additional information relevant to automated decision making, and receive redress, when harmed,
- defining pathways for individuals to review, verify, and question input data about themselves,
- requiring human teams to investigate errors with clear communication pathways for stakeholders, ensuring timely response,
- requiring systems to produce output explanations human decision makers, and other stakeholders, can examine, and
- providing clear statutory culpability and civil redress means for entities in the AI supply chain responsible for harm.

5. Baseline Standards for Platform Governance

Access to, and use of, online platforms is essential for modern citizenship (e.g., education, taxes, banking). To protect both domestic and national security interests and user constitutional rights (speech and privacy), baseline standards should be created for:

- verification procedures for account creation,
- account deactivation and removal criteria, and
- content removal and warning labeling.

6. Anti-Manipulation

When AI systems are built with detailed, fine-grained information about individuals, they can deliver customized suggestions. Without limitations, microtargeting and behavioral advertising can lead to manipulation outside of vulnerable users' awareness and control (e.g., delivering a suggestion for unhealthy food or addictive substances, or conspiracy theories), thus enabling exploitation, manipulation, and radicalization. *Subtle-to-the-user practices have huge societal impacts*. For example, voting misinformation and messaging (how "my friends" voted) can sway elections, or enabling an autoplay feature on streaming services could lead to seamless radicalization of viewers. IEEE-USA recommends legislation to:

- require clear information about why a suggestion is being being offered – and who is paying for it,
- require disclosure of whether the user is interacting with a human or AI,
- require proactive steps to prevent harmful manipulation and abuse,
- require data and access necessary for independent research/evaluations of anti-manipulation measures,
- require verified identity for entities/persons paying for content or ad distribution, and
- invest in research and development of technologies to identify and counter synthetic media.

See related statement at *Democratic Use of Artificial Intelligence*

This statement was developed by the IEEE-USA Artificial Intelligence Policy Committee and represents the considered judgment of a group of U.S. IEEE members with expertise in the subject field. IEEE-USA advances the public good and promotes the careers and public policy interests of the nearly 150,000 engineering, computing, and allied professionals who are U.S. members of the IEEE. The positions taken by IEEE-USA do not necessarily reflect the views of IEEE or its other organizational units.