IEEE-USA

POSITION STATEMENT

Privacy, Equity, and Justice in Artificial Intelligence

Adopted by the IEEE-USA
Board of Directors (November 2021)

AI's ubiquitous presence in society has challenged our ability to protect privacy and ensure equity and justice. The foundational principles below provide a legal, technical, and policy framework to address these challenges going forward and resolve problems embedded in existing AI uses and systems, such as when AI systems are trained with past data embedded with patterns of inequality and human bias. Building this framework requires updating, harmonizing, and streamlining federal laws, policies, and guidelines as follows:

1. Data ownership, data rights, and privacy

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

- ***Enact clear and comprehensive data protection law(s) at the federal level*** Internet and other communication-related 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 swaths of individuals' intimate data unprotected and fails to provide a clear framework of permissible operation for AI

[1] Our current federal and state patchwork of data laws lends to confusion and inefficiencies and precludes the U.S. from shaping private and government sector data practices on a national and international level. At the federal level, there is a sectoral-based approach to data regulation by both public and private sectors (e.g., health – Health Insurance Portability and Accountability Act; and financial – Gramm-Leach-Bliley Act). Given current data collection practices (communication platforms, apps, and devices routinely collect health, financial, and biometric data, and PII), the existing sectoral approach leaves vast swaths of individuals' intimate data unprotected in the current federal legislative scheme. At the state level, all 50 states have passed varying forms of data breach laws and a myriad of states have enacted comprehensive data regulation and biometric laws, such as the California Consumer Privacy Act (CCPA) and the Illinois Biometric Information Privacy Act. California, via CCPA, and the European Union's General Data Protection Regulation Act (GDPR) both provide legislative frameworks that have altered private sector data practices on a global scale.

systems and their operators, leading to inefficiencies and confusion. Comprehensive data regulation through legislative action should incorporate principles like Fair Information Practice Principles (FIPPs) that:

- **Establish data collection and data use limitations, data quality standards, and security safeguards.**
- **Require clearer notice of data collection practices with truly effective opportunities to consent (or not) to such data collection.**
- **Mandate transparency and user control in use of individual data**. Consumers are often unaware of how their data is collected and used; long, complex Terms of Use and privacy policies obscure actual data practices. Mandate that users have the right to access, review, store, and delete personal user data, including behavioral data used for tracking and AI recommendation systems, and require an option to opt-out of tracking.

2. **Mitigate disparate impacts of AI**

When AI systems are developed and deployed, objectives of accuracy and lack of algorithmic bias towards marginalized or vulnerable groups can conflict, resulting in disparate impacts and lack of public confidence. To mitigate, objectives must be balanced by means that require clarity, transparency, and protection of all stakeholders.

- ***Establish and mandate metrics and standards.*** AI systems and their operators must comply with standards for fairness, privacy, safety, and security.
- ***Establish transparency mechanisms for stakeholders.*** For example, require third-party access to data in standardized, machine-readable format.
- ***Create research investments on how the use of algorithms may disparately impact or disadvantage certain individuals and groups.***

3. **Ongoing verification and validation of AI systems**

Increasingly, AI systems directly impact human life, individual rights and societal well-being and, like other systems that do so, must be evaluated throughout their lifecycle, i.e., design, implementation, and deployment. When AI systems are deployed in critical applications such as employment, credit/finance, criminal justice, health systems, and allocation of public resources:

- ***Require transparency about the training data and other developmental inputs.***
- ***Require mechanisms for (and permit) independent verification and validation***.

4. **Redress**

When AI systems make life-impacting decisions, preserving privacy, equity, and justice requires that individuals be informed about, and permitted to, question decisions and have access to systems that enable redress.

- **Define pathways for all stakeholders to report problems, question results, provide additional information relevant to automated decision making, and receive redress when they are harmed.**
- **Define pathways for individuals to review, verify and question input data about them as individuals.**

- **Require human teams be tasked to investigate errors with clear pathways for stakeholders to communicate with teams and require timely response.**
- **Require systems to produce explanations of their output that can be examined by human decision makers and other stakeholders.**
- **Provide clear statutory culpability and means of civil redress for entities in the AI supply chain responsible for harm to individuals, groups, or the environment.**

5. **Baseline Standards for Platform Governance**

AI systems are ubiquitous, and access to and use of online platforms is a requirement to be an effective citizen of the modern world (education, taxes, banking - all require online participation with platforms, devices, and apps that operate with and rely upon AI systems). **To protect both domestic and national security interests and the constitutional rights (speech and privacy) of users**, baseline standards should be created for: verification procedures for account creation; when accounts can or should be removed or deactivated for a period of time; and when content can or should be removed or labeled with warnings

6. **Anti-Manipulation**

When AI systems are built with detailed, fine-grained information about individuals, they can use this information to deliver customized suggestions to individuals. Without limitations, microtargeting and behavioral advertising can permit and enable manipulation outside a user's awareness and explicit control (e.g., *delivering a suggestion* for unhealthy food or addictive substances or conspiracy theories *exactly when a person is vulnerable to them*), thus, enabling systems or human operators to exploit, manipulate, and radicalize others. *Subtle-to-the-user practices have huge societal impacts*, e.g., voting misinformation and voting messaging (how "my friends" voted) sways elections; having an autoplay feature in YouTube (enables seamless radicalization of viewers). Legislation to mitigate such effects would:

- ***Require clear information about why a suggestion is being offered to an individual and about who is paying to deliver that suggestion.***
- ***Require disclosure of actor*** (human or AI) with whom the user is interacting.
- ***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.***

This statement was developed by IEEE-USA's 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 IEEE. The positions taken by IEEE-USA do not necessarily reflect the views of IEEE, or its other organizational units.