KPMG

Regulatory Alert

Regulatory Insights

April 2023

Ensuring Trust in AI: Commerce Department Request for Comment

KPMG Regulatory Insight:

- *Amidst growing global societal and regulatory focus on AI transparency and safety, regulators are focused on ensuring that businesses, governments, and the public can trust that AI algorithms, tools, and products work as claimed and do so without causing harm (financial or otherwise) to users.*
- *Companies utilizing AI, including generative AI, should consider during the design, use, and deployment of AI: safety and effectiveness (e.g., protections against unintended or inappropriate use); protections against, and ongoing testing for, bias; data governance and privacy; transparency (including what and how information is being used and potential impacts to the business/consumer); and accountability and oversight.*
- *Regulators will use existing regulations (e.g., UDAP, data privacy/safeguards) as they enhance scrutiny over the development and use of AI across all industries, with continued heightened focus on consumer protections, false advertising, data governance, and bias.*

An agency of the Department of Commerce issued a request for comment (RFC) on artificial intelligence (AI) accountability measures and policies with a focus on how to provide "reliable evidence to external stakeholders—that is, to provide assurance—that AI systems are legal, effective, ethical, safe, and otherwise trustworthy." The comments, along with other public engagement, will be used to draft and issue a report on AI accountability policy development, focusing particularly on the "AI assurance ecosystem".

The Commerce Department agency, the National Telecommunications and Information Administration (NTIA), hopes that comments provided on the RFC will help to identify:

- Current AI accountability "processes and tools", including assessments and audits, governance policies, documentation and reporting, and testing and evaluation, that support AI accountability and provide AI "assurance".
- Gaps and barriers to creating and implementing "adequate and meaningful accountability" mechanisms.
- Any "trustworthy AI" goals that might not be amenable to requirements or standards.
- How certain accountability measures might mask or minimize AI risks.
- The value of accountability mechanisms to compliance efforts.
- Ways governmental and non-governmental actions might support and enforce AI accountability practices.

Below are highlights from the RFC.

RFC on AI Accountability

Terms. The RFC uses the terms "AI", "algorithmic", and "automated decision systems" without specifying "any particular technical tool or process", but does indicate the term incorporate and reference terms used by the White House and the National Institute of Standards and

Technology's (NIST – also a Commerce Department agency), including:

— **AI.** As covered by the White House Blueprint for an AI Bill of Rights, the scope and use of the term "AI" encompasses a broad set of technologies, including "automated systems" with "the potential to meaningfully impact the American public's rights, opportunities, or access to critical resources or services." (For more information on the Blueprint, see KPMG Regulatory Alert, here.)

— **AI System.** In its voluntary AI Risk Management Framework, NIST defined an "AI system" as "an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments."

— **Trustworthy AI.** This term is "intended to encapsulate a broad set of technical and sociotechnical attributes of AI systems such as safety, efficacy, fairness, privacy, notice and explanation, and availability of human alternatives. According to NIST, 'trustworthy AI' systems are, among other things, 'valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy-enhanced, and fair with their harmful bias managed.'"

Questions. The RFC poses thirty-four (34) questions across the following six (6) topics for public comment:

1. **AI Accountability Objectives**, such as the purpose, function, and value of AI accountability measures (including certifications, audits, and assessments).
2. **Existing Resources and Models**, such as current policies, procedures, frameworks, definitions, and requirements (under U.S. and non-U.S. laws and regulations) as well as possible accountability models based on U.S. and non-U.S. financial assurance systems or ESG assurance systems.
3. **Accountability Subjects**, such as where in the value chain should accountability efforts focus; how should accountability mechanisms consider the AI lifecycle management; should measures be based on the risk of the technology and/or the deployment context.
4. **Accountability Inputs and Transparency**, such as records, documentation, and retention periods for accountability and transparency; reporting of accountability results to different stakeholders; issues related to data quality and data voids.
5. **Barriers to Effective Accountability**, such as the lack of federal laws and regulations; the role of legal entitlements (e.g., intellectual property rights, terms of service, contractual obligations); cost burdens for AI audits and assessments; or the lack of measurable standards or benchmarks.
6. **AI Accountability Policies**, such as the role of government policy in the AI accountability ecosystem; whether policies/regulations should be sectoral or horizontal; incentives to promote AI accountability measures or documentation practices.

Comment Deadline. The deadline for comment submission is June 10, 2023.

Related FTC Blogs on AI

The Federal Trade Commission (FTC), which enforces laws affecting commerce, is similarly focused on AI and recently published two Business Blogs highlighting AI-related issues of fairness, equity, and fraud, including:

— The application of UDAP prohibitions to development, sale, or use of AI products designed to deceive—even if not the intended or sole purpose—including chatbots, deepfakes, and voice clones.

— Advertising considerations around AI products and related claims.

For more information, please contact Amy Matsuo or John Kemler.

Contact the author:

Amy Matsuo
Principal and National Leader
Regulatory Insights
amatsuo@kpmg.com