

FTC report reveals Commission's position on potential AI harms



July 21, 2022

On June 16, 2022, the Federal Trade Commission (FTC) issued a strongly worded report to Congress, "[Combatting Online Harms Through Innovation](#)," warning that policymakers must use "great caution" when mandating the use of artificial intelligence (AI) as a policy solution to combat online harms. Over-reliance on AI could introduce new harms potentially endemic to AI systems, including inaccuracies, bias, discrimination and commercial surveillance creep, the report claims. It notes that Congress and regulators should focus on developing legal frameworks to ensure that AI tools are transparent and accountable, and do no harm.

The report is the first statement on AI made by the full Commission now that the Democrats hold a majority on the FTC, suggesting that the FTC may be gearing up for anticipated AI rulemaking.¹

Background

In the 2021 Appropriations Act, Congress directed the FTC to examine and report on ways that AI may be used to combat a variety of "online harms" such as online fraud, impersonation scams, bots, deepfakes, hate crimes, cyberstalking and misinformation campaigns aimed at influencing elections, among others. Congress also instructed the FTC to recommend laws that could advance the use of AI to address online harms.

The FTC's concerns regarding the use of AI

While the FTC report addresses the use of AI to combat online harms, the FTC takes the opportunity to discuss its position on the use of AI more broadly.² The report explains how AI tools can be inaccurate, biased, and discriminatory by design, and may incentivize reliance on increasingly invasive forms of commercial surveillance.

- **Inaccuracies:** AI tools used to detect online harms are blunt instruments with built-in imprecision and inaccuracy. Because the datasets supporting the AI tools

Contacts

- If you have any questions about this Legal Alert, please feel free to contact any of the attorneys listed or the Eversheds Sutherland attorney with whom you regularly work.

Mary Jane Wilson-Bilik
Partner
mjwilson-bilik@eversheds-sutherland.com
+1.202.383.0660

Michael Bahar
Partner
michaelbahar@eversheds-sutherland.com
+1.202.383.0882

Alexander F.L. Sand
Counsel
alexandersand@eversheds-sutherland.com
+1.512.721.2721

Roxanne J. Garcia-Quinonez
Associate
Roxannegarcia-quinonez@eversheds-sutherland.com
+1.212.287.6924

Related People/Contributors

- Mary Jane Wilson-Bilik
- Michael Bahar
- Alexander F.L. Sand
- Roxanne J. Garcia-Quinonez
- John S. Pruitt
- Cynthia R. Shoss
- Meghana D. Shah

are trained on previously identified problems, the AI may have difficulty identifying rapidly emerging new phenomena and avoiding false positives or false negatives. Further, the algorithms may have difficulty processing content that is too complex and dynamic for them to capture, meaning that AI tools are necessarily reactive and "need constant adjustment even when they are built to make their own adjustments."³

- **Increased surveillance:** Ironically, the report finds that increasing the accuracy of AI tools has its own downsides and could lead to increased surveillance, requiring more extensive data extraction practices and more invasive forms of shadowing in order to accurately train the AI tools.
- **Bias and discrimination:** The report analyzes how AI tools can reflect the biases of their developers, datasets, and algorithms, leading to illegal discrimination, unfair results and censorship, depending on how the AI tools are used.
- **May not be fit for purpose:** Online harms often result from adversaries with harmful agendas seeking to actively evade or manipulate AI detection tools. While this state of affairs is not going away, the main struggle is to ensure adversaries are not in the lead. The question is whether AI tools can be made sufficiently robust and flexible to meet this challenge, since the report finds that AI tools currently are brittle and can fail even with small modifications to inputs.⁴

The report concludes that legal frameworks should be developed to prevent these harms from occurring and urges Congress, regulators, scientists, developers and users to focus on several related considerations, including:

- **Human intervention:** Trained humans are needed to monitor the use and decisions of AI tools, but even extensive human oversight will not solve for underlying algorithmic design flaws in AI tools used to combat online harms;

- **Meaningful transparency, explainability and contestability:** AI use should be transparent, explainable and contestable, especially when people's rights are involved or when personal data is being collected or used;
- **Accountability:** Platforms and other companies that rely on AI tools must be accountable both for their data practices and for their results, including implementing meaningful consumer appeal and redress mechanisms. The report also recommends the use of independent audits and algorithmic impact assessments.

The report focuses on the importance of the transparency and accountability when relying on AI tools.⁵ It also makes a series of recommendations: require appropriate documentation of datasets and models, keep privacy and security in mind, take responsibility for the both inputs and outputs of AI tools, strive to hire diverse teams and avoid using training data and classifications that reflect existing societal and historical inequities.

These principles and recommendations are similar in many ways to those of other regulators and organizations that have addressed AI, including the Organization for Economic Cooperation and Development (OECD),⁶ the US National Institute of Standards and Technology (NIST),⁷ the National Association of Insurance Commissioners (NAIC),⁸ the European Commission,⁹ United Kingdom government,¹⁰ and the Alan Turing Institute.¹¹

Conclusion

The FTC's discussion of the responsible use of AI applies across sectors. We encourage companies that use, or anticipate using, AI tools to reflect on whether their AI practices align with the FTC's approach and to consider what governance and technical measures might be needed to mitigate legal risk going forward.

¹¹ "The FTC's work has addressed AI repeatedly, and this work will likely deepen as AI's presence in commerce continues to rise." FTC Report at 3.

[2] The FTC hired its first-ever advisors on artificial intelligence in November 2021. See FTC Report at 4.

[3] FTC Report at 6.

[4] FTC Report at 6.

[5] [T]he import of focusing on [transparency and accountability of AI tools] cannot be overstated." FTC report at 7.

[6] OECD, "Recommendation of the Council on Artificial Intelligence," (2020).

[7] NIST, "AI Risk Management Framework," (2022).

[8] NAIC, "Principles on Artificial Intelligence," (2020).

[9] EU Commission, "Proposal for a Regulation... harmonizing rules on artificial intelligence (Artificial Intelligence Act)... " (2021).

[10] UK Secretary of State for Digital, Culture, Media and Sport, "AI Regulatory Policy Paper," (July 2022) (identifying six core principles for UK's regulation of AI: ensure AI is used safely, that it's technologically secure as designed, transparent and explainable, considers fairness, identifies a "legal person to be responsible for AI," and clarifies avenue for redress.)

[11] The Alan Turing Institute, "Common Regulatory Capacity for AI," (2022).

Authors

Mary Jane Wilson-Bilik | [Email](#) | +1 202 383 0660

Michael Bahar | [Email](#) | +1 202 383 0882

Alexander F.L. Sand | [Email](#) | +1 512 721 2721

Roxanne Garcia-Quinonez | [Email](#) | +1 212 389 5053

John S. Pruitt | [Email](#) | +1 212 389 5053

Cynthia R. Shoss | [Email](#) | +1 914 484 8486

Meghana D. Shah | [Email](#) | +1 212 389 5077

Charlotte Walker-Osborn | [Email](#) | + 44 779 907 5756

If you have any questions about this legal alert, please feel free to contact any of the attorneys listed under Related People/Contributors or the Eversheds Sutherland attorney with whom you regularly work.