TEN QUESTIONS ON AI RISK

Gauging the Liabilities of Artificial Intelligence Within Your Organization

Artificial intelligence and machine learning (AI/ML) generate significant value when used responsibly - and are the subject of growing investment for exactly these reasons. But AI/ML can also amplify organizations' exposure to potential vulnerabilities, ranging from fairness and security issues to regulatory fines and reputational harm.

The questions below are meant to serve as an initial guide to gauging these risks, both during the build phase of AI/ML endeavors and beyond. This document was prepared by bnh.ai, a boutique law firm specializing in AI/ML and analytics, in collaboration with the Future of Privacy Forum.

1. ***How many AI/ML models does your company deploy (including third-party models or those that serve as inputs into other models)?***

2. ***What types of outputs or recommendations is each model making and where is documentation about these models stored?***

3. ***How many people or organizations does each model potentially impact?***

4. ***How are your organization's models audited for security or privacy vulnerabilities?***

5. ***Incidents, such as attacks or failures of AI/ML models, can cause substantial harm. Does your company have response plans in place to address AI/ML incidents?***

6. ***Does your company audit models for AI/ML-related liabilities before a model is deployed? Are different audit processes applied for different types of models?***

7. ***Does your company monitor models for AI/ML-related liabilities during deployment? Are different audit processes applied for different types of models?***

8. ***Have you quantified sociological bias in your company's AI/ML training data and model predictions? Is your company aware of how each model affects different demographic customer segments?***

9. ***Several organizations have published detailed standards or best practices for "trustworthy AI."[1] Does your company utilize any of these resources when implementing AI/ML? If so, which ones?***

10. ***Have any independent third parties or other external experts (legal, security, or others) been involved in your company's procedures to address the known liabilities of AI/ML?***

About the 10 Questions

These questions were adapted from written letters sent by Sens. Cory Booker and Ron Wyden to the heads of major healthcare companies in December of 2019.[2] The letters arose in response to research that indicated a widely used algorithm was also discriminatory.[3]

These types of questions are indicative of increased regulatory oversight of AI/ML in the short- to medium-term. Note that both senators were sponsors of the 2019 Algorithmic Accountability Act, introduced in each chamber of Congress, which would delegate increased powers to the FTC to regulate AI/ML.[4]

For further information about how to manage the risks of AI/ML, please reach out to contact@bnh.ai. For further information about the Future of Privacy Forum, please contact info@fpf.org.

---

[1] See, for example, Responsible AI Practices – Google AI or 7010-2020 - IEEE Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being. Similar standards may also be referred to as practices for "ethical AI."

[2] The full text of these letters, which focus more overtly on bias, is available online.

[3] Discrimination was discovered by Obermeyer et al. and published in *Science*.

[4] The text of the Algorithmic Accountability Act is available online. The FTC in April 2020 also publicly signalled an increased willingness to regulate AI.