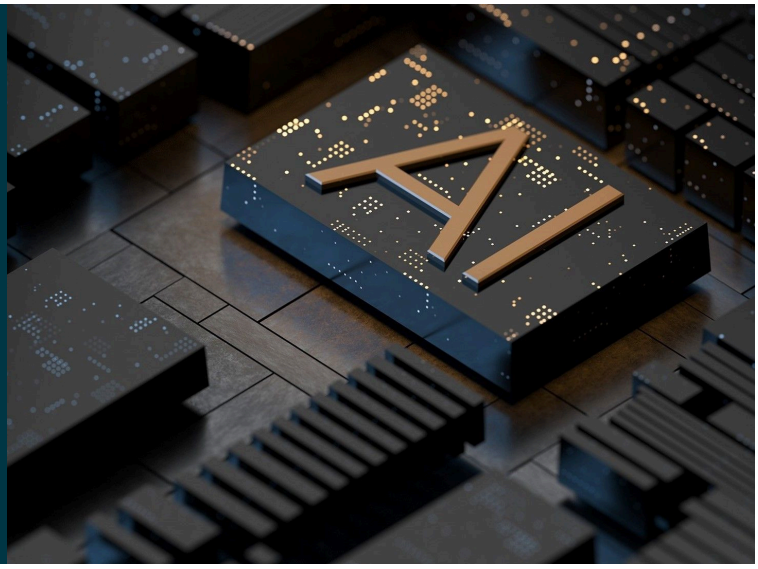
WILSON SONSINI



EU Commission Issues Guidelines on Prohibited AI Practices Under EU AI Act

CONTRIBUTORS


Laura De Boel


Maneesha Mithal


Christopher N. Olsen


Rossana Fol


Roberto Yunquera Sehwani

ALERTS

February 11, 2025

On February 4, 2025, the European Commission (EC) issued draft guidelines clarifying the AI practices that are prohibited under the European Union's (EU) Artificial Intelligence (AI) Act. While non-binding, the guidelines offer valuable clarifications and practical examples to help businesses navigate their obligations under the AI Act. The EC has approved the draft guidelines, but is still to formally adopt them, which is expected in the near term.

Background

On February 2, 2025, the AI Act's provisions on prohibited AI practices became effective, along with other provisions on AI literacy (see here).

Article 5 of the AI Act prohibits certain AI practices that are considered to raise unacceptable risks, such as AI systems that manipulate or exploit individuals, perform social scoring, or infer individuals' emotions at the workplace or in education. The ban applies to both companies offering such AI systems, as well as to those using them. The guidelines provide concrete examples of practices that are classified as prohibited, as well as those that are not.

The AI Act may apply to companies based outside the EU if they make an AI system or general-purpose AI (GPAI) model available on the EU market, or if the output generated by the AI system is used in the EU.

Prohibited AI Practices

Below is an overview of the main prohibitions under the AI Act, as interpreted by the guidelines:

1. **Social Scoring.** The AI Act prohibits offering or using AI systems that assess individuals' social behaviors to determine their treatment in an unrelated context. For example, AI systems used to recommend the price of an insurance premium or to assess people's creditworthiness could amount to social scoring, if the assessment is based on unrelated personal characteristics. AI-enabled scoring is not covered by the prohibition when it involves offering certain privileges to online shoppers with a strong purchase history and a low rate of product returns. Individual ratings by users also fall outside the scope of the ban (e.g., a user's rating of a driver on a car-sharing platform, or a user's rating of a host on an accommodation platform).

2. **Manipulation and Exploitation.** The AI Act prohibits offering or using AI systems that use subliminal techniques or exploit individual vulnerabilities to influence their behavior and cause harm. According to the guidelines, this includes, for example, the use of AI in games to encourage

excessive play and compulsive usage by exploiting children's vulnerabilities in a way that seriously harms them. Additionally, AI-driven scams targeting older persons by exploiting their cognitive limitations also fall under this prohibition. The ban does not extend to AI systems that do not manipulate users, exploit vulnerabilities, or cause significant harm. For example, an AI system designed to assist with language learning using subliminal techniques is allowed, provided it operates transparently and respects user autonomy without deceptive or coercive elements. Also, the ban does not cover AI systems using personalized recommendations based on transparent algorithms and user preferences and controls.

3. **Facial Recognition and Biometric Identification.** The AI Act bans the practice of building facial recognition databases through untargeted scraping of images from the internet or CCTV footage. The guidelines refer to the example of an AI company that scrapes facial images from social media platforms to build a facial recognition database: such practice would be prohibited. The guidelines also clarify that the ban does not apply to scraping of data other than facial images (e.g., voice samples) or to AI systems that do not engage in biometric identification. In particular, the guidelines make it clear that facial image databases that are not used for the recognition of persons are not prohibited, such as those used for AI model training where the persons are not identified.
4. **Emotion Recognition in Workplaces and Educational Institutions.** Using AI to recognize emotions in workplaces and educational settings is generally prohibited. According to the guidelines, examples include a call center using webcams and voice recognition to track employees' emotions (such as anger), an education institution using an emotion recognition AI system to infer the interest and attention of students, and emotion recognition AI systems used during the recruitment process. Emotion recognition for medical and safety purposes is exempted (e.g., detecting fatigue in pilots or drivers). The prohibition does not cover emotion recognition outside work and education, such as in a commercial context. Thus, AI chatbots detecting emotions of customers based on keystroke or voice messages, or intelligent billboards which tailor advertisements based on the detected emotions of the passerby, do not fall under this ban.
5. **Biometric Categorization.** The categorization of individuals based on sensitive attributes such as race, political opinions, or sexual orientation using biometric data is forbidden. For example, the guidelines indicate that it is prohibited to offer or to use AI systems that categorize people based on such sensitive attributes by analyzing biometric data from their pictures (e.g., photos published on social media) to send them political messages or advertising. However, the ban does not extend to cases where the categorization is purely technical and necessary for a commercial service, for example, a facial filter on an online marketplace to allow them to preview products on them. Similarly, the labelling of biometric data for datasets used for AI training to ensure an adequate representation of ethnic groups is not prohibited, if the labeling aims to ensure diverse representation and prevent discrimination.

Responsibilities for AI Providers

The guidelines stipulate that providers of AI systems (i.e., those who develop AI systems or have them developed and make them available in the EU) are responsible for not releasing a system that is "*reasonably likely*" to be used for a prohibited purpose, as well as for adopting safeguards to prevent reasonably foreseeable misuse (e.g., via technical safeguards, user controls, restrictions of use).

The EC expects providers to clearly exclude the use of their AI system for prohibited practices in their terms, and to provide clear instructions for use e.g., guidance on appropriate oversight and prohibited practices. In practice, this means that AI providers are expected to anticipate potential uses of their AI systems and implement safeguards accordingly. This applies even when those systems are intended for general use (i.e., systems powered by GPAI models).

Providers must ensure continuous compliance, which includes ongoing monitoring of and updates to AI systems they placed on the market (which, however, should not reach the level of a general monitoring of deployers' activities). In the event that an AI provider becomes aware—for example, because the system is operated through a provider's platform—that an AI system has been misused for a prohibited purpose, they are expected to take appropriate measures.

Next Steps

Companies that engage in prohibited AI practices may face significant fines, which can reach up to EUR 35 million or seven percent of their global annual turnover, whichever is higher. The first enforcement actions are expected to kick off in the later half of 2025 as EU countries finalize their enforcement regimes. Companies offering or using AI in the EU should review their AI systems and terms in light of these guidelines and address any compliance gaps in the first half of 2025.

For more information on how to ensure your AI systems and models comply with the EU AI Act, please contact Cédric Burton, Laura De Boel, Yann Padova, or Nikolaos Theodorakis from Wilson Sonsini's data, privacy, and cybersecurity practice. Please also see our FAQs, 10 Things You Should Know About the EU AI Act, which provides more details on the prohibited uses of AI.

Wilson Sonsini's AI Working Group assists clients with AI-related matters. Please contact Laura De Boel, Maneesha Mithal, Manja Sachet, or Scott McKinney for more information.

Rossana Fol, Roberto Yunquera Sehwani, and Karol Piwonski contributed to the preparation of this Alert.