Legal Update Article

The Risks of an Operating System Integrated with Artificial Intelligence

By

July 8, 2024

Related Services

Privacy, Data and Cybersecurity
Technology

Artificial intelligence (AI), and especially generative AI, has quickly become one of the hottest topics in the modern age. Where digital footprints are ubiquitous and data has become a valuable commodity, AI has emerged as a focal point of innovation and concern. With AI now being integrated into operating systems (OS) promising enhanced efficiency, it is crucial to recognize that along with these advancements come new risks.

Basics of an AI Model

AI models, which come in various forms, are essentially predictive programs trained to recognize patterns and generate responses. Engineers use vast datasets, ranging from private purchases to publicly available and web-scraped data, to train these models. Much like human learning, AI models retain patterns from their training to respond to queries without revisiting the original source material.

AI on an Operating System

The newest flavor of AI coming to fashion is the integration of an AI model into the OS of devices like phones or computers. Operating as an extension of the OS itself, these AI models primarily access local device data. They are "trained" before installation and continue learning from user interactions to tailor responses. This model is touted to be helpful with scheduling, drafting, searches, and other simple queries. When tasked with a query that is beyond its capacity, the embedded AI model will forward the request to the larger AI model in the cloud for a larger model to handle. Presumably, the larger model will process, return a response, and delete information about that request.

Risks and Exposure

Despite their differences, both integrated and cloud-based AI models pose similar risks to users:

- **Privacy Concerns:** AI often relies on vast amounts of personal information raising concerns about data privacy and data security. When contained to a local device, the risk of sending the proprietary or personal information to another company is reduced, but the risk that a query would allow someone to learn more than they should about sensitive data still exists;
- **Targeted Attacks:** AI systems can be vulnerable to adversaries who manipulate input data to provoke incorrect responses. These systems could potentially act as an attack vector for malicious third parties;
- **Legally Faulty Advice:** AI systems cannot replace an attorney and should not be taken as legally sound advice. Relying solely on that advice could expose an employer to significant legal liability; and
- **Unintentional Bias:** AI systems are only as good as the data they intake. If that data is biased, it will inevitably result in a biased response.

Preemptive Measures

As companies increasingly integrate AI into their OS, it is essential for employers to proactively address these risks. Employers can preemptively prepare for this inevitable change by:

- **Training on Responsible AI Use:** Implement trainings on the responsible and permitted use of AI in the workplace;
- **Internal Policies:** Develop clear policies that govern the responsible and permissible use of AI;
- **Vendor Oversight:** Understand AI vendor's privacy policies, datasets, and security protocols to minimize risk;
- **Vendor Agreements:** Thoroughly vet AI vendor agreements to ensure alignment with organizational policies, transparency in training datasets, and proper disposal of employer data; and
- **Limit Usage:** Restrict access to AI models that have not been properly vetted.

At Jackson Lewis, our Technology Group remains at the forefront of AI innovation in this rapidly evolving industry. As advancements outpace regulatory frameworks, it is crucial to navigate these changes with caution. Contact a Jackson Lewis attorney for expert guidance in navigating this exciting new frontier responsibly.

(Summer Associate Paul Yim contributed to this article.)