CARLTON
FIELDS

Four Key Cybersecurity and Privacy Considerations for Organizations Using Generative AI

July 19, 2023

Generative AI has captured the public's attention and promises to transform the way we live and work. The technology, however, implicates a number of important cybersecurity and privacy considerations for organizations. This alert details four of the most prominent considerations and outlines steps for addressing those issues.

1. Increased Cyber Threats. Cyber threat actors may use generative AI to further their schemes. Potential uses are limitless and include creating malware exploiting previously unknown (or "zero-day") vulnerabilities, creating malicious websites that appear legitimate, personalizing phishing emails, generating deep fake data, and inundating security systems. Additionally, a business's own AI models can create risks of exploitation.

   Mitigating This Risk. To mitigate this risk, organizations need to redouble their focus on cybersecurity. They can begin with the basics, such as drafting and testing an incident response plan, conducting risk assessments that contemplate these emerging threats, and making cybersecurity an enterprisewide focus. As part of this prep work, organizations should consider identifying and taking action against fraudulent domains that spoof their legitimate domains. As to the security of a business's own AI models, it may want to focus on regularly patching any third-party models, bug-fixing any internal models, and training employees on acceptable use.

2. Privacy Compliance Generally. States are passing new privacy laws on a near-monthly basis. Among other things, those laws regulate how consumer data is collected, processed, and shared and impose new consumer rights. Those laws often impose disclosure and consent requirements, opt-out rights, and contracting obligations. Generative AI impacts compliance with these laws, particularly if the tool processes consumers' personal information for automated decision-making purposes or if the tool might constitute "selling" or "sharing" under state privacy laws. Additionally, some regulators, such as the National Labor Relations Board, have started to provide guidance on the use of AI models for workplace monitoring, and the city of New York has even passed a law prohibiting the use of automated decision-making for hiring and promotion unless the company takes certain anti-bias steps.

   Mitigating This Risk. Addressing this risk requires an understanding of the tools involved, the underlying data and its sources, the laws implicated, and the tool's potential impact on consumers. Compliance might start with a review of the terms of use or other contracts from the company offering the AI product that may touch an organization's data. Additional compliance steps can involve preparing notices and consents, conducting risk assessments and testing, securing opt-out rights, ensuring appropriate recordkeeping, developing the means for reviewing and overriding the tool's decisions, and putting in place appropriate contractual provisions with vendors and service providers. If any of the AI products touch employee data or if the company is subject to special industry regulations (such as health care, government contracting, or financial services), consider whether any regulator guidance may be implicated and check practices against that guidance.

3. Avoiding Blind Spots. Companies must also consider their vendors' potential use of AI tools. Contracts often impose on the business itself the obligation to provide requisite notices and secure consumer consent for a vendor's processing of the business's personal information. If a vendor has not disclosed its use of an AI tool to the business, the business may not realize the full scope of this obligation and potential liability to individuals whose personal information the vendor is processing.

   Mitigating This Risk. Before entering into any agreement, businesses should understand the type of processing and tools used by their vendors, as well as what opt-out rights the vendor may already have exercised (e.g., opting out of an AI tool's using the business's data to improve itself). An initial step could be including in vendor due diligence questions about that vendor's use of AI tools to process personal information from the business, alongside other questions about data processing.

4. Avoiding Deceptive Trade Practices. The Federal Trade Commission, state attorneys general, and plaintiffs' attorneys are focused on pursuing alleged deceptive trade practices, particularly when it comes to purported deviations between an organization's privacy policy and its privacy practices. In a recent example, the FTC accused online counseling service BetterHelp of sharing sensitive health information with third-party advertising platforms, in violation of the company's privacy policy. A company that uses generative AI to process data in a way that is allegedly inconsistent with its privacy policy and other public-facing statements may find itself the subject of enforcement actions and litigation.

   Mitigating This Risk. Use a multidisciplinary approach when vetting and implementing generative AI. This approach involves stakeholders from multiple groups collaborating to understand current practices and tools, mitigate risk, and increase transparency. Some initial steps here would be to survey the known uses of generative AI tools within the organization, review the contracts and terms of use surrounding that use, and then compare that work to the business's actual privacy policy disclosures.

Generative AI heralds opportunities and risks for organizations. Cybersecurity and privacy risks are among the most prominent. By identifying and addressing the risks above, organizations can make the most of this exciting technology while mitigating their exposure.

Authored By

Patricia M. Carreiro

John E. Clabby

Related Practices

Cybersecurity and Privacy
Technology

Related Industries

Technology

©2024 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.