

PUBLICATION

A Baker's Dozen: Top Questions In-House Legal Counsel Should Consider Asking to Better Understand AI including ChatGPT

Authors: Alisa L. Chestler, Justin S. Daniels, Vivien F. Peadar

April 21, 2023

Artificial Intelligence (AI), including ChatGPT, has now ushered its way regularly into management conversations. How can AI benefit an organization, provide it with a competitive advantage, or make it more efficient? At the same time, what questions should in-house counsel be asking to assess how to balance AI benefits versus its legal risk? With those questions in mind, we bring you the Baker's Dozen; where we provide you with questions that run the gamut from general to more specific covering employment, intellectual property, privacy, and security. Asking good questions is the initial step we are taking to kick off our series of articles and webinars to help your organization better understand AI and its impact on your business and appreciate its benefits while managing its risks.

General Questions:

Many organizations are distributing affirmative statements and guidelines to inform their workforce regarding AI. Some are even prohibiting the use of certain AI tools, including ChatGPT, until more is understood about its functionality. Affirmative notices of an organization's current guidelines should be considered and that requires analysis of how the issues will impact the organization (short term and long term).

1. Do you know which of your vendors is using AI to analyze or modify your data; and do you have prohibitions in your vendor agreement about using your data for their AI tool?
2. Have you considered how you protect your ownership rights in AI-generated output which usually includes your organization's data?
3. How do you verify AI answers to ensure their accuracy, as opposed to misleading you, or lying to you convincingly?
4. In plain English, how do you explain the origin of your AI tools (i.e., developed in-house or procured from a 3rd party)?
5. What ethical and legal factors should be considered as part of your policy for AI decision-making, and how can companies guarantee that their AI systems are transparent, just, and responsible?

Employment:

We have already seen employees use AI without guardrails, resulting in negative consequences for the organization. Should you prohibit access to this tool? How can your organization have guardrails around its use by your employees?

6. What workplace policies are in place regarding the use of AI, especially as it relates to employees sharing confidential company or client information with AI tools?

7. In what ways will the growing adoption of AI impact your workforce, especially day-to-day HR functions, like applicant screening and hiring, and what measures can you take proactively to avoid AI tools creating new liabilities?

We previously released an [alert](#) regarding AI and workplace discrimination lawsuits that you may find helpful in answering some of these questions.

Intellectual Property:

Intellectual property (IP) rights are a key consideration when it comes to utilizing AI output. If the data set used by the AI infringes third-party rights, how does that impact your use?

8. Have you considered how you protect or otherwise comply with privacy law in data used to generate AI?
9. Does your company plan to leverage generative AI to create original works or inventions for which the company will thereby seek copyrightable or patentable protection?

We previously released an [alert](#) regarding IP and AI which you may find insightful regarding this topic.

Privacy:

The use of AI can raise numerous privacy issues from informed consent and data collection limitation to implicit bias and individual rights (such as rights to delete and to opt-out) under various privacy laws. How can you maximize the benefits of implementing AI effective solutions while protecting the privacy rights of individuals?

10. What is the source of data that your internal teams or service providers use to train and develop AI tools?
11. Does your usage of AI (and the underlying data) comply with applicable privacy laws?

Cybersecurity:

Every new technology comes with a new cyber threat. In an era of deep fakes and data manipulation, how do you assess whether you are employing AI securely?

12. Do you have a policy to prevent your company's confidential information, sensitive information, or trade secrets from inadvertently being entered into AI tools?
13. How is your company preparing for next-generation cybersecurity threats (such as stealing training data or compromising data integrity) to skew AI output?

If you have any questions regarding AI, including ChatGPT, in the workplace, please contact [Alisa L. Chestler](#), [CIPP/US](#), [Justin Daniels](#), [Vivien F. Peaden](#), [CIPP/US](#), [CIPP/E](#), [CIPM](#), [PLS](#), or any of our AI team members: [Zachary B. Busey](#), [Edward D. Lanquist](#), [Dominic Rota](#), or [Matthew G. White](#), [CIPP/US](#), [CIPP/E](#), [CIPT](#), [CIPM](#), [PCIP](#).