APRIL 11, 2023 • 8 MIN READ

AI chatbots and the workplace: risks and best practices for employers

AUTHORS

 Molly Reynolds

 Lisa K. Talbot

 Rebecca Wise

 Nic Wall

Consumer AI services like chatGPT, Bing and Bard are chatbot-like tools that use language processing models based on AI technology to answer questions. In recent months, these tools have exploded in popularity, being typically free, easy to access through a browser, user-friendly—and in many cases quite impressive in what they can produce in response to question prompts.

The popularity of these tools as well as their early stage of development and recent nascent regulatory action have raised a number of concerns about how employees may use these tools in the workplace. The concerns range from confidentiality and privacy to accuracy, workplace harassment and work product ownership.

We set out below key considerations for employers in creating guidance on the use of these services in the workplace.

What you need to know

- Employers should determine whether to permit any use of consumer AI services for business purposes and communicate with employees about this policy.
- Where some use is permitted, internal guidance should focus on:
  - Education about the risks to individuals and the organization
  - Integration with existing workplace policies
  - Organizational and technological compliance controls
  - Impact on workplace complaints and investigative processes
- Businesses should be prepared to regularly update internal guidance on the use of consumer AI services as the regulatory landscape continues to rapidly evolve.

Understanding the risks of consumer AI tools

Although even Members of Parliament are now using chatGPT to write their questions for House of Commons speeches (and comment on its accuracy or inaccuracy in doing so)[1], regulators in Canada and abroad are raising concerns about what happens to the data that these tools collect. The Italian privacy regulator issued a ban on chatGPT in March 2023 pending an investigation into compliance with the EU privacy law, and the Canadian Office of the Privacy Commissioner opened an investigation into the same tool in April following a consumer complaint. The Federal Trade Commission is reviewing a similar complaint in the U.S.

In addition, there are broader concerns about the impact on companies when employees use these tools to assist in their job duties. Examples of these impacts include:

- **Confidentiality and privacy breaches.** Consider a scenario where an HR employee asks a consumer AI tool to draft a termination letter. Even where employee and company names are not included in the prompt, the parameters given to the tool may reveal confidential corporate or personal data. Once inputted into the tool, the company has little visibility or control over how this information may be used, distributed, or associated back to the business.
- **Inaccurate information.** A business analyst may ask a consumer AI tool for an analysis of industry economic trends to support an internal research paper. The tool may return a detailed and plausible analysis, complete with citations. However, the sources cited may be inaccurate, incomplete, outdated or completely made up. The answer may also be drawn from sources that are not disclosed, making it impossible to verify its accuracy or neutrality. The analyst's research paper may therefore be based on unreliable information, compromising company decision-making and the employee's own performance quality. In addition, if inaccurate information is used to make decisions about individuals, there could be human rights- or consumer protection-based claims against the company.

- **Work product and IP ownership.** As with the above example, employees that rely on information from consumer AI tools do not have visibility into how the information was developed, and from which sources. The underlying information may be subject to third party ownership claims, such as where it has been scraped from websites that limit who can access the data and for what purposes. This has already been the source of commercial litigation across North America (see our article here). Employees that unknowingly incorporate proprietary data into their work product may expose the company to IP challenges and commercial litigation. For example, where a developer asks a consumer AI tool for coding assistance, the company's claim to ownership of the resulting code in its own products could be at risk.
- **Workplace harassment.** While the above examples focus on risks from well-intentioned use, there is also potential for malicious use of consumer AI tools in the workplace. These services can be used to generate misleading or defamatory content about coworkers, such as fake or inaccurate biographies, public statements or sexual images. Employers should be aware of the potential use of such tools in the context of anti-harassment training and investigations.
- **Workplace investigations.** Similar to the above example, employers should be aware that freely available AI tools could be used to generate false information that forms the basis of workplace complaints or that may be submitted as evidence by respondents in internal investigations. Employers should ensure their investigators have appropriate training and resources to identify potentially false, AI-generated information and address it in the course of existing investigative processes.
- **Legal compliance risk.** Beyond these examples of particular risks, organizations should monitor the development of laws or regulatory orders in various regions that may prohibit the use of consumer AI tools altogether. For example, a company with operations in Europe should consider whether the recent ban on chatGPT by the Italian data protection authority means it should prohibit all use of the service by employees in Italy, in the EU, or worldwide, to avoid accusations or negative press about permitting conduct in violation of a regulatory order.

Employee guidance considerations

Businesses in Canada and the U.S. should consider creating policies, guidance or training tools on the appropriate use of consumer AI tools in the workplace to mitigate the above risks. Some organizations may choose to prohibit the use of these tools for business purposes unless they are integrated into software that has been vetted and licensed by the company. Others may focus on educating employees of the risks and identifying potentially appropriate uses. Such guidance should consider the following elements:

Awareness and education

Employee guidance should explain why the use of consumer AI may create risks for the company and its staff. For example, employees may not understand that the information they input as prompts for these tools may be used indefinitely in the model, for various undefined purposes outside the control of the company, and may be easy to associate back to the company, its customers or its employees. They may not make the connection between the use of these services and their employee confidentiality obligations.

Similarly, employees may not appreciate that the seemingly sophisticated answers provided by these tools may be inaccurate. The difference between these tools and company-vetted research products should be explained so that employees understand the risks of using them to assist in their work.

Integration with existing workplace policies

Employers should reiterate the application of their existing privacy, confidentiality, acceptable IT use and workplace conduct policies and explain how they may limit or prohibit the use of consumer AI tools, and how the disciplinary consequences discussed in those policies may apply to unauthorized use of these services.

Organizational and technological compliance controls

Employers should consider whether awareness and policies are sufficient in ensuring compliance with their position on consumer AI, or whether monitoring, audits, attestations of compliance or restricting access to the tools' websites are needed.

Impact on workplace conduct and investigations

As mentioned above, employers should be mindful of how advances in consumer AI may change the nature of common workplace complaints. Companies should consider whether their workplace conduct training and investigation processes should be updated to address these technological developments.

Need for regular review

Given the rapid development of both the technology and the regulatory response to consumer AI, employers should be clear in their internal communications that workplace guidance may change. Companies should also designate a person responsible for updating such policies and controls as the risk landscape evolves, such as in the event a regulator prohibits the use of such a tool within the country.

While many businesses will see advantages to some employee use of consumer AI services, the scope of any permitted use should be clearly explained, and organizations should be prepared to adjust their practices as this technology and regulatory landscape develops.

FOOTNOTES

To discuss these issues, please contact the author(s).

TAGS

Privacy | Data Governance and Strategy | Pensions and Employment | Employment and Pensions Litigation | Technology | Technology Contracting | Intellectual Property | Intellectual Property Litigation | Cybersecurity | Advisory and Regulatory | Transactions | Consumer and Retail