WILMERHALE

The Top 10 Legal and Business Risks of Chatbots and Generative AI

February 27, 2023

I. Introduction

It took just two months from its introduction in November 2022 for the artificial intelligence (AI)-powered chatbot ChatGPT to reach 100 million monthly active users—the fastest growth of a consumer application in history.[1]

Chatbots like ChatGPT are Large Language Models (LLMs), a type of artificial intelligence known as "generative AI." Generative AI refers to algorithms that, after training on massive amounts of input data, can create new outputs, be they text, audio, images or video.[2] The same technology fuels applications like Midjourney and DALL-E 2 that produce synthetic digital imagery, including "deepfakes."[3]

Powered by the language model Generative Pretrained Transformer 3, ChatGPT is one of today's largest and most powerful LLMs. It was developed by San Francisco-based startup OpenAI—the brains behind DALL-E 2—with backing from Microsoft and other investors, and was trained on over 45 terabytes of text from multiple sources including Wikipedia, raw webpage data and books to produce human-like responses to natural language inputs.[4]

---

[1] Krystal Hu, *ChatGPT Sets Record for Fastest-growing User Base - Analyst Note*, REUTERS (Feb. 2, 2023), https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/.
[2] *See* Nick Routley, *What Is Generative AI? An AI Explains*, WORLD ECONOMIC FORUM (Feb. 6, 2023), https://www.weforum.org/agenda/2023/02/generative-ai-explain-algorithms-work/.
[3] *See generally* Matthew F. Ferraro, *Decoding Deepfakes*, NATIONAL SECURITY INSTITUTE BACKGROUNDER (Dec. 16, 2020), https://nationalsecurity.gmu.edu/ddf/.
[4] *See* Kindra Cooper, *OpenAI GPT-3: Everything You Need to Know*, SPRINGBOARD (Nov. 1, 2021), https://www.springboard.com/blog/data-science/machine-learning-gpt-3-open-ai/; *see also How Does Chat GPT Work*?, ATRIA INNOVATION (Jan. 5, 2023), https://www.atriainnovation.com/en/how-does-chat-gpt-work/. By comparison, "[i]t has been estimated that 10 Terabytes could hold the entire printed collection of the US Library of Congress, while a single TB could hold 1,000 copies of the Encyclopedia Brittanica [*sic*]." *What is a Terabyte*, TERADATA, https://www.teradata.com/Glossary/What-is-a-Terabyte.

LLMs like ChatGPT interact with users in a conversational manner, allowing the chatbot to answer follow-up questions, admit mistakes, and challenge premises and queries. Chatbots can write and improve code, summarize text, compose emails and engage in protracted colloquies with humans. The results can be eerie; in extended conversations in February 2023 with journalists, chatbots grew lovelorn and irascible and expressed dark fantasies of hacking computers and spreading misinformation.[5]

The promise of these applications has spurred an "arms race" of investment into chatbots and other forms of generative AI.[6] Microsoft recently announced a new, $10 billion investment in OpenAI, and Google announced plans to launch an AI-powered chatbot called Bard later this year.[7]

The technology is advancing at a breakneck speed.[8] As *Axios* put it, "The tech industry isn't letting fears about unintended consequences slow the rush to deploy a new technology."[9] That approach is good for innovation, but it poses its own challenges. As generative AI advances, companies will face a number of legal and ethical risks, both from malicious actors leveraging this technology to harm businesses and when businesses themselves wish to implement chatbots or other forms of AI into their functions.

This is a quickly developing area, and new legal and business dangers—and opportunities—will arise as the technology advances and use cases emerge. Government, business and society can take the early learnings from the explosive popularity of generative AI to develop guardrails to protect against their worst behavior and use cases before this technology pervades all facets of commerce. To that end, businesses should be aware of the following top 10 risks and how to address them.

---

[5] *See* Washington Post Staff, *The New Bing Told Our Reporter It 'Can Feel or Think Things,'* WASH. POST (Feb. 16, 2023), https://www.washingtonpost.com/technology/2023/02/16/microsoft-bing-ai-chat-interview/; Matt O'Brien, *Is Bing Too Belligerent? Microsoft Looks to Tame AI Chatbot*, AP (Feb. 16, 2023), https://apnews.com/article/technology-science-microsoft-corp-business-software-fb49e5d625bf37be0527e5173116bef3; Kevin Roose, *A Conversation With Bing's Chatbot Left Me Deeply Unsettled*, N.Y. TIMES (Feb. 17, 2023), https://www.nytimes.com/2023/02/16/technology/bing-chatbot-microsoft-chatgpt.html. Microsoft announced recently that it will limit the length of chatbot conversations to reduce the likelihood the AI tool will become confused or respond in an unintended style. *See The New Bing & Edge – Learning From Our First Week*, MICROSOFT (Feb. 15, 2023), https://blogs.bing.com/search/february-2023/The-new-Bing-Edge-%E2%80%93-Learning-from-our-first-week.

[6] Andrew R. Chow & Billy Perrigo, *The AI Arms Race Is Changing Everything*, TIME (Feb. 16, 2023), https://time.com/6255952/ai-impact-chatgpt-microsoft-google/.

[7] *Id.*

[8] *See* Danya Bazaraa, *Experts Predict 'Explosion' of Deep Fakes with 90% of Online Content Being AI Generated by 2025*, DAILY MAIL (Feb. 1, 2023), https://www.dailymail.co.uk/news/article-11700593/Experts-predict-explosion-deep-fakes-90-online-content-AI-generated-2025.html (citing experts Nina Schick and Henry Ajder).

[9] Scott Rosenberg, *AI Revolution: Tech Finds Its Next Platform*, AXIOS (Feb. 17, 2023), https://www.axios.com/2023/02/17/chatgpt-ai-next-platform-tech.

II. Risks

1. Contract Risks

Using chatbots or similar AI tools may implicate a range of contractual considerations.

Businesses should be wary of entering into chatbot prompts information from clients, customers or partners that is subject to contractual confidentiality limitations or other controls. This is because chatbots may not keep that information private; their terms of service typically grant the chatbot the rights to use the data they ingest to develop and improve their services.[10] If the bot provides opt-out features, users may want to utilize them before inputting contractually protected information into the prompts, but users should still proceed cautiously.[11] In one exchange with a professor, ChatGPT itself warned that "[i]nformation provided to me [ChatGPT] during an interaction should be considered public, not private" and that the bot cannot "ensure the security or confidentiality of any information exchanged during these interactions, and the conversations may be stored and used for research or training purposes."[12]

Likewise, a business will need to curtail its use of chatbots or AI generally if a contract imposes on the business the obligation to produce work or perform services on its own or by a specific employee, without the aid of AI. To the extent that a chatbot generates contract work product—unlike traditional information technology, which merely provides a platform for generating work product—a chatbot service could be a subcontractor, potentially subject to pre-approval by the ultimate customer.

In both circumstances, the key is to recognize that the relationship between a user and a chatbot is not akin to the relationship between a user and a word processing program or a similar static tool. Chatbots and other generative AI software are learning machines that by default use information entered into them for their own purposes and that produce their own output. (Beware: all of the inputs could potentially be discoverable in litigation.) For these reasons, they pose risks to businesses' contractual obligations, and companies should use these tools circumspectly.

2. Cybersecurity Risks

Chatbots pose cybersecurity risks to businesses along two main axes. First, malicious users without sophisticated programming skills can use chatbots to create malware for cyber hacks.

---

[10] *Terms of Use*, Sec. 3(c), OPENAI (Dec. 13, 2022), https://openai.com/terms/ ("To help OpenAI provide and maintain the Services, you agree and instruct that we may use Content to develop and improve the Services.").
[11] *See id.* (providing email address to contact to request content not be used for service improvement).
[12] @NitaFarahany, TWITTER (Feb. 16, 2023, 8:34 PM), https://twitter.com/NitaFarahany/status/1626394649593085952.

Second, because chatbots can convincingly impersonate fluent, conversational English, they can be used to create human-like conversations that can be used for social engineering, phishing and malicious advertising schemes, including by bad actors with poor English-language skills.[13] Chatbots like ChatGPT typically disallow malicious uses through their usage policies and implement system rules to prohibit bots from responding to queries that ask for the creation of malicious code per se; however, cybersecurity researchers have found work-arounds that threat actors on the dark web and special-access sources have already exploited.[14] In response, companies should redouble efforts to bolster their cybersecurity and train employees to be on the lookout for phishing and social engineering scams.

3. Data Privacy Risks

Chatbots may collect personal information as a matter of course. For example, ChatGPT's Privacy Policy states that it collects a user's IP address, browser type and settings; data on the user's interactions with the site; and the user's browsing activities over time and across websites, all of which it may share "with third parties."[15] If a user does not provide such personal information, it may render a chatbot's services inoperable.[16] Currently, the leading chatbots do not appear to provide the option for users to delete the personal information gathered by their AI models.

Because laws in the United States and Europe impose restrictions on the sharing of certain personal information about, or obtained from, data subjects—some of which chatbots may collect automatically, and some that a user may input into the chatbot's prompt—businesses using chatbots or integrating them into their products should proceed cautiously. Data privacy regulators could scrutinize these systems, assessing whether their user-consent options and opt-out controls stand up to legal scrutiny.[17] For example, the California Privacy Rights Act requires California companies of a certain size to provide notice to individuals and the ability to opt out of the collection of some personal information.[18]

Some data privacy regimes impose regulations on entities that merely collect information, like the AI systems that ingested billions of Internet posts to create their models. In California, for example,

---

[13] Insikt Group, *I, Chatbot*, RECORDED FUTURE (Jan. 26, 2023), https://www.recordedfuture.com/i-chatbot.
[14] *Id.*; *see Usage Policies*, OPENAI (Feb. 15, 2023), https://platform.openai.com/docs/usage-policies/usage-policies (disallowed usages include, *inter alia*, "[i]llegal activity").
[15] *Privacy Policy*, Sec. 1, OPENAI (Sept. 19, 2022), https://openai.com/privacy/.
[16] *See id.*, Sec. 10 ("If you choose not to provide Personal Information that is needed to use some features of our Service, you may be unable to use those features.").
[17] Cassandre Coyer, *Could ChatGPT Soon Find Itself in Data Privacy Regulators' Crosshairs?*, LEGALTECH NEWS (Feb. 1, 2023), https://www.law.com/legaltechnews/2023/02/01/could-chatgpt-soon-find-itself-in-data-privacy-regulators-crosshairs/.
[18] *See* Isha Marathe, *New Year, New Laws: Data Privacy Changes to Watch for in 2023*, LEGALTECH NEWS (Jan. 9, 2023), https://www.law.com/legaltechnews/2023/01/09/the-new-data-privacy-landscape-what-to-watch-in-2023/.

unless an entity is registered as a data broker, it is supposed to provide a "notice at collection" to any California resident about whom it is collecting data.

To mitigate data privacy risks, companies utilizing chatbots and generative AI tools should review their privacy policies and disclosures, comply with applicable data protection laws with regard to processing personal information, and provide opt-out and deletion options.

4. Deceptive Trade Practice Risks

If an employee outsources work to a chatbot or AI software when a consumer believes he or she is dealing with a human, or if an AI-generated product is marketed as human made, these misrepresentations may run afoul of federal and state laws prohibiting unfair and deceptive trade practices. The Federal Trade Commission (FTC) has released guidance stating that Section 5 of the FTC Act, which prohibits "unfair and deceptive" practices, gives it jurisdiction over the use of data and algorithms to make decisions about consumers and over chatbots that impersonate humans.[19]

For example, in 2016, the FTC alleged that an adultery-oriented dating website deceived consumers by using fake "engager profiles" to trick customers to sign up, and in 2019, the FTC alleged that a defendant sold phony followers, subscribers and likes to customers to boost social media profiles.[20] In sum, "[i]f a company's use of doppelgängers—whether a fake dating profile, phony follower, deepfakes, or an AI chatbot—misleads consumers, that company could face an FTC enforcement action,"[21] or enforcement by state consumer protection authorities.

To address this issue, the FTC emphasizes transparency. "[W]hen using AI tools to interact with customers (think chatbots), be careful not to mislead consumers about the nature of the interaction," the FTC warns.[22] Companies should also be transparent when collecting sensitive data to feed into an algorithm to power an AI tool, explain how an AI's decisions impact a consumer and ensure that decisions are fair.[23]

Likewise, the White House's October 2022 *Blueprint for an AI Bill of Rights* suggests developers of AI tools provide "clear descriptions of the overall system functioning and the role automation plays,

---

[19] Andrew Smith, *Using Artificial Intelligence and Algorithms*, FEDERAL TRADE COMMISSION (Apr. 8, 2020), https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms; *see also* Elisa Jillson, *Aiming for Truth, Fairness, and Equity in Your Company's Use of AI*, FEDERAL TRADE COMMISSION (Apr. 19, 2021), https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai (FTC Act gives FTC jurisdiction over algorithms that produce discriminatory results; both the Fair Credit Reporting Act and the Equal Credit Opportunity Act make it illegal to use an algorithm to deny benefits based on protected characteristics).
[20] Smith, *Using Artificial Intelligence and Algorithms*.
[21] *Id.*
[22] *Id.*
[23] *Id.*

notice that such systems are in use, the individual or organization responsible for the system, and explanations of outcomes that are clear, timely, and accessible."[24]

5. Discrimination Risks

Issues related to discrimination can arise in different ways when businesses use AI systems. First, bias can result because of the biased nature of the data on which AI tools are trained. Because AI models are built by humans and learn by devouring data created by humans, human bias can be baked into an AI's design, development, implementation and use. For example, in 2018, Amazon reportedly scrapped an AI-based recruitment program after the company found that the algorithm was biased against women.[25] The model was programmed to vet candidates by observing patterns in resumes submitted to the company over a 10-year period, but because the majority of the candidates in the training set had been men, the AI taught itself that male candidates were preferred over female candidates.

ChatGPT, like other LLMs, can learn to express the biases of the data used to train them. As OpenAI acknowledges, ChatGPT "may occasionally produce harmful instructions or biased content."[26]

Second, users can purposefully manipulate AI systems and chatbots to produce unflattering or prejudiced outputs. For example, despite built-in features to inhibit such responses, one user got ChatGPT to write code stating that only White or Asian men make good scientists; OpenAI has reportedly updated the bot to respond, "It is not appropriate to use a person's race or gender as a determinant of whether they would be a good scientist."[27] In another recent example, at a human's direction, the chatbot adopted a "devil-may-care alter ego" that opined that Hitler was "complex and multifaceted" and "a product of his time."[28]

Federal regulators and the White House have repeatedly emphasized the importance of using AI responsibly and in a nondiscriminatory manner. For example, the White House's *Blueprint for an AI Bill of Rights* declares that users "should not face discrimination by algorithms and systems should be used and designed in an equitable way."[29] Algorithmic discrimination, which has long existed independent of chatbots, refers to when automated systems "contribute to unjustified different

---

[24] *Blueprint for an AI Bill of Rights*, THE WHITE HOUSE (Oct. 2022), https://www.whitehouse.gov/ostp/ai-bill-of-rights/.
[25] Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women*, REUTERS (Oct. 20, 2018, 7:04 PM), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.
[26] *ChatGPT General FAQ*, OPENAI, https://help.openai.com/en/articles/6783457-chatgpt-general-faq.
[27] Davey Alba, *OpenAI Chatbot Spits Out Biased Musings, Despite Guardrails*, BLOOMBERG (Dec. 8, 2022), https://www.bloomberg.com/news/newsletters/2022-12-08/chatgpt-open-ai-s-chatbot-is-spitting-out-biased-sexist-results.
[28] Will Oremus, *The Clever Trick That Turns ChatGPT Into Its Evil Twin*, WASH. POST (Feb. 14, 2023), https://www.washingtonpost.com/technology/2023/02/14/chatgpt-dan-jailbreak/.
[29] *Blueprint for an AI Bill of Rights*, THE WHITE HOUSE.

treatment or impacts disfavoring people" based on various protected characteristics like race, sex, and religion.[30]

"Designers, developers, and deployers of automated systems should take proactive and continuous measures to protect individuals and communities from algorithmic discrimination and to use and design systems in an equitable way," the White House advises. This protection should include "proactive equity assessments as part of the system design," the use of representative data, "pre-deployment and ongoing disparity testing and mitigation, and clear organizational oversight," among other actions.[31]

Similarly, in April 2021, the FTC noted that even "neutral" AI technology can "produce troubling outcomes—including discrimination by race or other legally protected classes."[32] The FTC recommends that companies' use of AI tools be transparent, explainable, and fair and empirically sound so as not to mislead consumers about the nature of their interactions with the company.[33]

Finally, in January 2023, the National Institute of Standards and Technology (NIST) issued a Risk Management Framework for using AI in a trustworthy manner. The Risk Management Framework provides voluntary guidance to users of AI and sets forth principles for managing risks related to fairness and bias, as well as other principles of responsible AI such as validity and reliability, safety, security and resiliency, explainability and interpretability, and privacy.[34]

Bias may arise in AI systems even absent prejudicial or discriminatory intent by their human creators. As urged by emerging US government guidance, companies using such tools should carefully consider the potential for prejudicial or discriminatory impact, be forthright about how they are using chatbots and other generative AI tools, conduct regular testing to judge disparities, and impose a process for humans to review the outputs to ensure compliance with antidiscrimination laws and to safeguard against reputational harm.

6. Disinformation Risks

Chatbots can help malicious actors create false, authoritative-sounding information at mass scale quickly and at little cost. Researchers showed recently that chatbots can compose news articles,

---

[30] *Id.*
[31] *Id.*
[32] Jillson, *Aiming for Truth, Fairness, and Equity in Your Company's Use of AI.*
[33] *See id.*; Smith, *Using Artificial Intelligence and Algorithms*.
[34] *See* Ariel Soiffer & Wei Xiao, *NIST Issues Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, WILMERHALE CLIENT ALERT (Jan. 30, 2023), https://www.wilmerhale.com/en/insights/client-alerts/20230130-nist-issues-artificial-intelligence-risk-management-framework-ai-rmf-10.

essays and scripts that spread conspiracy theories, "smoothing out human errors like poor syntax and mistranslations and advancing beyond easily discoverable copy-paste jobs."[35]

False narratives coursing through the internet already regularly harm businesses. For example, in 2020, the QAnon-inspired theory spread online that the furniture seller Wayfair was connected with child sex trafficking because of the coincidental overlap of the names of some of its furniture pieces and those of missing children.[36] As a result, social media users attempted to orchestrate a large short sale of Wayfair's stock, posted the address and images of the company's headquarters and the profiles of employees, and harassed the CEO.[37]

Now, a single bad actor with access to an effective chatbot could generate a flood of human-looking posts like those that targeted Wayfair and loose them on the internet, potentially harming the reputation and valuation of innocent companies. Add to these false narratives deepfake imagery of, say, the CEO of the targeted business doing something untoward, and the dangers will accelerate.

What is more, malicious actors can teach AI models bogus information by feeding lies into their models, which the models will then spread.[38]

Managing disinformation risk is complex. In short, businesses should plan for disinformation dangers like they plan for cyberattacks or crisis events, proactively communicate their messages, monitor how their brands are perceived online, and be prepared to respond in the event of an incident.[39]

7. Ethical Risks

[35] Tiffany Hsu & Stuart A. Thompson, *Disinformation Researchers Raise Alarms About A.I. Chatbots*, N.Y. TIMES (Feb. 8, 2023), https://www.nytimes.com/2023/02/08/technology/ai-chatbots-disinformation.html.
[36] For example, one social media post suggested that a report about an allegedly missing Ohio teenager named Samiyah Mumin was linked to a Wayfair cabinet called "Samiyah," with a listed price of almost $13,000. *See* Reuters Staff, *Fact Check: No Evidence Linking Wayfair to Human Trafficking Operation*, REUTERS (Jul. 13, 2020), https://www.reuters.com/article/uk-factcheck-wayfair-human-trafficking/fact-check-no-evidence-linking-wayfair-to-human-trafficking-operation-idUSKCN24E2M2?fbclid=IwAR3WNOLt9DsNrMdwLO13mylatPo3CB-X3y7gsC1_H5GJ6yNC4Tj5kmgrFBE.
[37] *See id. See also* Cindy L. Otis, Opinion, *Conspiracy Theorists Targeted Wayfair. Who Will QAnon Hit Next?*, BARRON'S (Jul. 27, 2020), https://www.barrons.com/articles/after-conspiracy-theorists-hit-wayfair-companies-should-ask-will-i-be-next-51595787339.
[38] *See* Ashley Gold & Sara Fischer, *Chatbots Trigger Next Misinformation Nightmare*, AXIOS (Feb. 21, 2023), https://www.axios.com/2023/02/21/chatbots-misinformation-nightmare-chatgpt-ai (describing "injection attacks").
[39] *See Disinformation and Deepfakes Risk Management*, WILMERHALE (Apr. 29, 2022), https://www.wilmerhale.com/insights/publications/20220429-wilmerhale-on-disinformation-and-deepfakes-risk-management.

Companies regulated by professional ethics organizations, such as lawyers, doctors and accountants, should ensure that their use of AI comports with their professional obligations.

For example, in the legal services industry, "legal representation" is explicitly defined in several jurisdictions as a service rendered by a person.[40] Because AI chatbots are not "persons" admitted to the bar, they cannot practice law before a court. Accordingly, the use of AI in the legal industry could elicit charges of the unauthorized practice of law. Case in point: In January 2023, Joshua Browder, the CEO of the AI company DoNotPay, attempted to deploy an AI chatbot to argue before a physical courtroom. But after "state bar prosecutors" purportedly threatened legal action and six months' jail time for the unauthorized practice of law, Browder canceled the appearance.[41]

To avoid potential violations of ethical obligations, companies should ensure any use of AI tools comports with ethical and applicable professional codes.

8. Government Contract Risks

The US government is the largest purchaser of supplies and services in the world.[42] US government contracts are typically awarded pursuant to formal competitive procedures, and the resulting contracts generally incorporate extensive standardized contract terms and compliance requirements, which frequently deviate from practices in commercial contracting. These procedural rules and contract requirements will govern how private companies might use AI to prepare bids and proposals seeking government contracts and to perform those contracts that are awarded.

When preparing a bid or proposal in pursuit of a government contract, companies should be transparent about any intended or potential use of AI to avoid the risk of misleading the government that the work product will be generated in whole or in part by a third party's AI tool. If two competing bidders use the same AI tool to develop their proposals, there is a chance that the proposals will appear similar. Indeed, OpenAI's Terms of Use warn that "[d]ue to the nature of machine learning, Output [from ChatGPT] may not be unique across users and [the chatbot] may generate the same or similar output for OpenAI or a third party."[43] Such similarity could create an appearance of sharing of contractor bid or proposal information, which is prohibited by the Procurement Integrity Act.[44] If competitive proposal information is entered into a third-party AI tool, that information might

[40] *See, e.g.*, N.Y. Judiciary Law § 478 ("It shall be unlawful for any natural person to practice or appear as an attorney-at-law or as an attorney . . . without having first been duly and regularly licensed and admitted to practice law in the courts of record of this state . . . ."); DC App. Rule 49 ("No person shall engage in the practice of law in the District of Columbia or hold out as authorized to do so unless (1) the person is a D.C. Bar Member. . . .").
[41] Sindhu Sundar, *DoNotPay's CEO Says Threat of 'Jail for 6 Months' Means Plan to Debut AI 'Robot Lawyer' in Courtroom is on Ice*, BUSINESS INSIDER (Jan. 26, 2023, 4:40 AM), https://www.businessinsider.com/donotpay-ceo-says-risks-jail-ai-robot-lawyer-used-court-2023-1.
[42] *Contracting Guide*, US SMALL BUSINESS ADMINISTRATION, https://www.sba.gov/federal-contracting/contracting-guide.
[43] *Terms of Use*, Sec. 3(b), OPENAI.
[44] *See* 48 C.F.R. § 3.104-1-11.

actually be used by the tool through a machine learning process to generate another offeror's proposal, which could actually constitute a prohibited sharing of contractor bid or proposal information.[45]

For awarded government contracts, a contractor should review the contract before using AI to create deliverables to ensure that the contract does not prohibit the use of such tools to generate work product.

Thus, government contractors should proceed cautiously and in consultation with counsel before relying on chatbots or generative AI to pursue or perform government contracts.

9. Intellectual Property Risks

Intellectual property (IP) risks associated with using AI can arise in several ways.

First, because AI systems have been trained on enormous amounts of data, such training data will likely include third-party IP, such as patents, trademarks, or copyrights, for which use authorization has not been obtained in advance. Hence, outputs from the AI systems may infringe others' IP rights. This phenomenon has already led to litigation.

In November 2022, in *Doe v. GitHub*, pseudonymous software engineers filed a putative class action lawsuit against GitHub, Microsoft and OpenAI entities alleging that the defendants trained two generative AI tools—GitHub Copilot and OpenAI Codex—on copied copyrighted material and licensed code. Plaintiffs claim that these actions violate open source licenses and infringe IP rights. This litigation is considered the first putative class action case challenging the training and output of AI systems.[46]

In January 2023, in *Anderson v. Stability AI*, three artists filed a putative class action lawsuit against AI companies Stability AI, Midjourney and DeviantArt for copyright infringement over the unauthorized use of copyrighted images to train AI tools. The complaint describes AI image generators as "21st-century collage tools" that have used plaintiffs' artworks without consent or compensation to build the training sets that inform AI algorithms.[47]

In February 2023, Getty Images filed a lawsuit against the Stability AI, accusing it of infringing its copyrights by misusing millions of Getty photos to train its AI art-generation tool.[48]

Second, disputes may arise over who owns the IP generated by an AI system, particularly if multiple parties contribute to its developments. For example, OpenAI's Terms of Use assign the

[45] *See* 48 C.F.R. 3.104-4.
[46] Compl., Doe et al. v. GitHub, Inc. et al., 22-cv-6823 (Nov. 3, 2022, N.D. Cal).
[47] Compl. para. 90, Anderson et al. v. Stability AI, Ltd. et al., 23-cv-00201 (Jan. 13, 2023, N.D. Cal.).
[48] Compl., Getty Images (US), Inc. v. Stability AI, Inc., 23-cv-00135 (Feb. 3, 2023, D. Del.).

"right, title and interest" in the output of the LLM to the user who provided the prompts, so long as the user abided by OpenAI's terms and the law. OpenAI reserves the right to use both the user's input and the AI-generated output "to provide and maintain the Services, comply with applicable law, and enforce our policies."[49]

Third, there is the issue of whether IP generated by AI is even protected because, in some instances, there is arguably no human "author" or "inventor." Litigants are already contesting the applicability of existing IP laws to these new technologies. For example, in June 2022, Stephen Thaler, a software engineer and the CEO of Imagination Engines, Inc., filed a lawsuit asking the courts to overturn the US Copyright Office's decision to deny a copyright for artwork whose author was listed as "Creativity Machine," an AI software Thaler owns.[50] (The US Copyright Office has stated that works autonomously generated by AI technology do not receive copyright protection because the Copyright Act grants protectable copyrights only to works created by a human author with a minimal degree of creativity.) In late February 2023, the US Copyright Office ruled that images used in a book that were created by the image-generator Midjourney in response to a human's text prompts were not copyrightable because they are "not the product of human authorship."[51]

As the law surrounding the use of AI develops, companies seeking to use LLMs and generative AI tools to develop their products should document the extent of such use and work with IP counsel to ensure adequate IP protections for their products. For example, the Digital Millennium Copyright Act requires social media companies to remove posts that infringe on IP, and generative AI systems may have avenues through which rights holders can alert the platforms to infringing uses.[52]

10. Validation Risks

As impressive as chatbots are, they can make false, although authoritative-sounding statements, often referred to as "hallucinations." LLMs are not sentient and do not "know" the facts. Rather, they know only the most likely response to a prompt based on the data on which they were trained.[53] OpenAI itself acknowledges that ChatGPT may "occasionally produce incorrect answers" and cautions that ChatGPT has "limited knowledge of world and events after 2021."[54] Users have

---

[49] Terms of Use, Sec. 3(a), OpenAI.
[50] Compl., Thaler v. Perlmutter et al., 22-cv-01564 (June 2, 2022, D.D.C.).
[51] US Copyright Office to Val Lindberg, Re: Zarya of the Dawn (Registration #VAu001480196) (Feb. 21, 2023), https://media.licdn.com/dms/document/C4E1FAQEbznl_nMcFOQ/feedshare-document-pdf-analyzed/0/1677091630453?e=1678320000&v=beta&t=l9y-aDl5drXoos9aAQBgavEwY_twp_XNZ59E_7aFzAs.
[52] For example, OpenAI provides an email address where rights holders can send copyright complaints, and OpenAI says "it may delete or disable content alleged to be infringing and may terminate accounts of repeat infringers." *Terms of Use*, Sec. 3(d), OpenAI.
[53] Melissa Heikkilä, *Why You Shouldn't Trust AI Search Engines*, MIT Technology Review (Feb. 14, 2023), https://www.technologyreview.com/2023/02/14/1068498/why-you-shouldnt-trust-ai-search-engines/ ("They are excellent at predicting the next word in a sentence, but they have no knowledge of what the sentence actually means.").
[54] *ChatGPT General FAQ*, OpenAI.

flagged and cataloged responses in which ChatGPT flubbed answers to mathematical problems, historical queries and logic puzzles.[55]

Companies seeking to use chatbots should not simply accept the AI-generated information as true and should take measures to validate the responses before incorporating them into any work product, action or business decision.

III. Conclusion

With the pell-mell development of chatbots and generative AI, businesses will encounter both the potential for substantial benefits and the evolving risks associated with the use of these technologies. While specific facts and circumstances will determine particular counsel, businesses should consider these top-line suggestions:

- be circumspect in the adoption of chatbots and generative AI, especially in pursuing government contracts, or to generate work required by government or commercial contracts;
- consider adopting policies governing how such technologies will be deployed in business products and utilized by employees;
- recognize that chatbots can often err, and instruct employees not to rely on them uncritically;
- carefully monitor the submission of business, client or customer data into chatbots and similar AI tools to ensure such use comports with contractual obligations and data privacy rules;
- if using generative AI tools, review privacy policies and disclosures, require consent from users before allowing them to enter personal information into prompts, and provide opt-out and deletion options;
- if using AI tools, be transparent about it with customers, employees and clients;
- if using AI software or chatbots provided by a third party, seek contractual indemnification from the third party for harms that may arise from that tool's use;
- bolster cybersecurity and social engineering defenses against AI-enabled threats;
- review AI outputs for prejudicial or discriminatory impacts;
- develop plans to counter AI-powered disinformation;
- ensure that AI use comports with ethical and applicable professional standards; and
- copyright original works and patent critical technologies to strengthen protection against unauthorized sourcing by AI models and, if deploying AI tools, work with IP counsel to ensure outputs are fair use.

[55] Tasmia Ansari, Opinion, *Freaky ChatGPT Fails That Caught Our Eyes!*, AIM (Dec. 7, 2022), https://analyticsindiamag.com/freaky-chatgpt-fails-that-caught-our-eyes/.

We thank Partners Barry Hurewitz and Kirk Nahra, Counsel Rebecca Lee, and Senior Associate Ali Jessani for their contributions to this article.

Contributors

Matthew F. Ferraro
COUNSEL

matthew.ferraro@wilmerhale.com
+ 1 202 663 6562

Natalie Li
SENIOR ASSOCIATE

natalie.li@wilmerhale.com
+ 1 212 937 7233

Haixia Lin
PARTNER

haixia.lin@wilmerhale.com
+ 1 202 663 6029

Louis W. Tompros
PARTNER

louis.tompros@wilmerhale.com
+ 1 617 526 6886