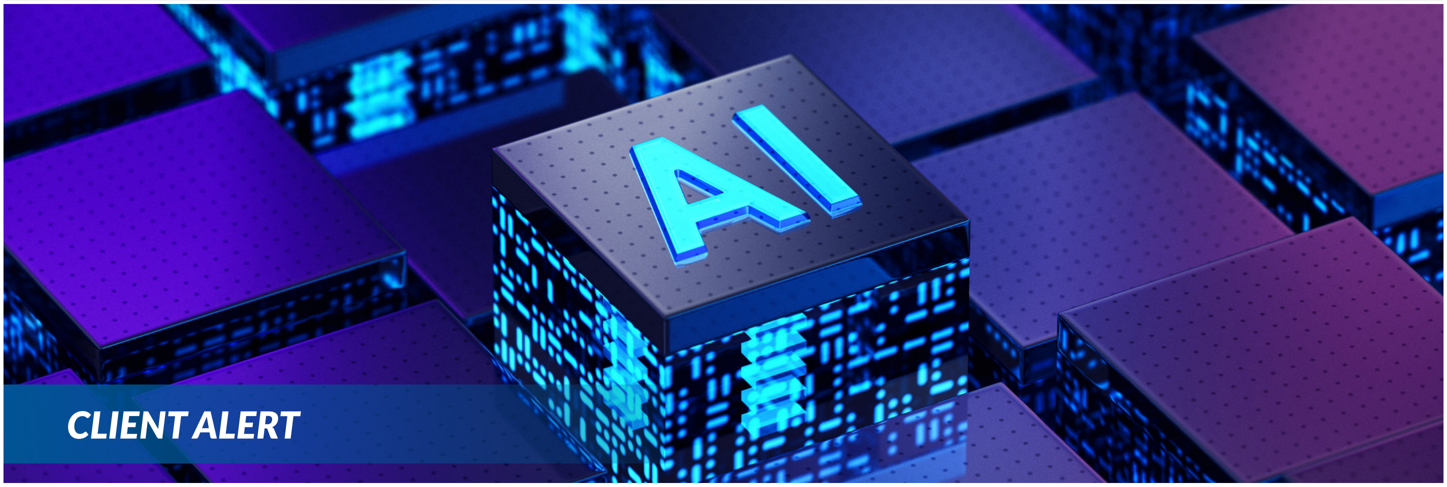
SheppardMullin



AI Technology - Governance and Risk Management
Why Your Employee Policies and Third-Party Contracts Should be Updated

By: Yasamin Parsafar & Wynter Deagle

AI technology is a powerful tool and "with great power comes great responsibility." Use of AI technology can give rise to various forms of liability that may not even occur to you. And use of generative AI impacts not only your liabilities but also your rights.

If you are developing or using products that use AI technology, it is important to understand the legal implications and factor them into your governance and risk management policies as soon as possible, if you have not yet done so. And even if you do not use or develop AI-driven products as a company, whether known or unknown to you, it is likely you have employees or vendors who are using generative AI tools in the performance of their duties. They may be using these tools to do anything from writing code to creating images, music, apps, or your marketing content. Your employees' and vendors' use of AI tools can impose liability and vulnerabilities on you in a significant way. As the FTC explained: "If something goes wrong – maybe it fails or yields biased results – you can't just blame a third-party developer of the technology. And you can't say you're not responsible because that technology is a 'black box' you can't understand or didn't know how to test."[1]

Below is a high level overview of some AI-related liabilities and vulnerabilities to factor into your governance and risk management, including by updating your employee policies and third-party agreements, now.

Violations of Consumer Protection Laws May Result in Algorithmic Disgorgement

Have you ever heard of algorithmic disgorgement? If your employees or service providers use AI tools (and they probably do, or will soon), you should be aware of this severe penalty imposed by the FTC when consumer protection laws are violated in the process of collecting information used to train AI models.

Companies who use data that was unlawfully acquired or unlawfully used to train algorithms used in machine-learning models or other AI tools may be required to destroy ill-gotten data as well as the algorithms or models that were trained using such data.

[1] Michael Atleson, *Keep your AI claims in check*, Federal Trade Commission Business Blog (Feb. 27, 2023) (available at https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check).

In 2022, the FTC brought an action for alleged violations of the Children's Online Privacy Protection Act ("COPPA") against a provider of a weight management and wellness app and services that was allegedly marketed to and collected information about children. COPPA prohibits unfair or deceptive acts or practices in connection with the collection, use, or disclosure of personally identifiable information from and about children on the Internet. Pursuant to the FTC's settlement agreement, the defendant was required to "delete or destroy any Affected Work Product," which was broadly defined as "any models or algorithms developed in whole or in part using Personal Information Collected from Children through [defendant's weight management and wellness service and app]."[2]

Similarly, in a prior case against a photo app developer, the FTC alleged that the defendant had deceived consumers about its use of facial recognition technology and its retention of photos and videos of users who deactivated their accounts, which constituted unfair or deceptive acts or practices, in or affecting commerce, in violation of Section 5(a) of the Federal Trade Commission Act. The FTC ordered defendant to "delete or destroy any Affected Work Product," which was defined as "any models or algorithms developed in whole or in part using Biometric Information Respondent collected from Users of the 'Ever' mobile application."[3]

As defined, "Affected Work Product" is very broad, and the deletion or destruction of the same can have profound financial and practical consequences for the companies who develop and use these tools.

Practical Tips: (1) Ensure your contractor agreements include appropriate reps and warranties and indemnities related to the vendor's training and use of AI tools used in the provision of services to you or licensed to you; (2) consider how you will be impacted if the model is no longer available mid-contract and include appropriate contingencies.

Civil Rights and Other Discrimination-Based Violations

The FTC has made clear that you may not only be liable based on what you use to train the algorithm and how you got that data, but you may also be liable under various statutes for your sale or *use* of the algorithm, including potential violations of Section 5 of the FTC Act for using racially biased algorithms, violations of the Fair Credit Report Act for using an algorithm to deny people employment, housing, credit, insurance, or other benefit, or violations of the Equal Credit Opportunity Act for using a biased algorithm in a way that results in credit discrimination on the basis of race, color, religion, national origin, sex, marital status, age, or receipt of public assistance.

The FTC is not the only agency that is tuned into alleged harms that may result from the use of AI technology. The U.S. Equal Employment Opportunity Commission (EEOC) has AI on its radar as well. The EEOC launched an agency-wide initiative focused on ensuring compliance with federal civil rights laws when using various technologies, including AI and machine learning tools, in hiring and employment decisions. The EEOC has published a document entitled, The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees, which includes examples of ways that an employer's use of AI decision-making tools may violate the ADA, including, among other things, the tools *unintentionally* screening out individuals with disabilities, even where the individual is able to do the job with a reasonable accommodation, or failing to provide a reasonable accommodation necessary for the individual to be rated fairly and accurately by the algorithm.

Importantly, the EEOC makes clear: Yes, in many cases, an employer may be liable for ADA violations for its use of AI decision-making tools even if the tools are designed or administered by a third party, such as a software vendor.

[2] Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief, United States of America v. Kurbo Inc. et al., No. 3:22-cv-00946-TSH (N.D. Cal. Mar. 3, 2022), ECF No. 15. (available at https://www.ftc.gov/system/files/ftc_gov/pdf/wwkurbostipulatedorder.pdf).

[3] Decision and Order, In the Matter of Everalbum, Inc. et al., No. 1923172 (Federal Trade Commission May 6, 2021) (available at https://www.ftc.gov/system/files/documents/cases/1923172_-_everalbum_decision_final.pdf).

Practical Tips: (1) Require your employees to seek approval before using algorithmic decision-making tools so that you can appropriately vet the tool provider, including understanding what they have done to eliminate discrimination and bias, and (2) ensure your employees get proper training on how to use these tools in a way that minimizes risk.

Intellectual Property Vulnerabilities and Risks

There are many intellectual property issues implicated by the use of generative AI technologies. Below are just some examples to consider when updating your employee policies and third-party agreements.

First, if you want enforceable intellectual property rights in your creative works and inventions, you and your employees need to understand that you may not own rights in AI-generated outputs. The Copyright Office has made clear that AI cannot be an author of a copyrighted work. And the work is only the product of human authorship, and thus eligible for copyright protection, to the extent it is the *human*, not the AI technology, that "determines the expressive elements of its output."[4] Similarly, both the United States Patent and Trademark Office (USPTO) and U.S. federal courts have made clear that an inventor must be a human.[5] Thus, to the extent you want to have enforceable intellectual property rights in your employees' or contractors' creations, you should understand and control the use of generative AI via your employee policies and third-party agreements.

Second, many models are trained based on works involving third-party intellectual property rights, which may be identifiable in the outputs of those models. Regardless of whether you are aware of the third-party IP rights, to the extent you use outputs that may arguably contain third-party IP, you may be subject to an IP infringement claim, whether your use was fair or not. Fair use is a defense and while you can win a lawsuit based on fair use, you cannot *avoid* a lawsuit if the rights holder disagrees that your use is fair. IP lawsuits can be very expensive, and your potential exposure should be factored into your internal and external risk management.

Third, depending on which generative AI tools your employees or contractors are using, and the respective Terms of Service, you may not own your outputs or you may be giving rights to your outputs or even your inputs (e.g., proprietary code or confidential customer information) to the tool provider and/or others who use the tool. You may also be contractually restricted in what you can do with your outputs.

Practical Tips: (1) Consider an acceptable use matrix for various generative AI tools that lets your employees know for what purposes each tool may or may not be used that takes into account the tools' terms of service – this can be similar to what companies use for managing use of open source software; (2) restrict your employees' inputs into AI tools, including requiring anonymization of content, in order to avoid disclosing confidential information or giving away IP rights; (3) consider restricting or prohibiting the use of generative AI tools for employees and contractors in connection with works in which you want to have enforceable rights or where there is a significant IP infringement concern based on your use; (4) make sure you have adequate reps and warranties, indemnities, and restrictions for your contractors' use of AI technology.

[4] 88 Fed. Reg. 16190 (Mar. 16, 2023. (available at https://www.federalregister.gov/documents/2023/03/16/2023-05321/copyright-registration-guidance-works-containing-material-generated-by-artificial-intelligence).

[5] Thaler v. Vidal, 43 F.4th 1207 (Fed. Cir. 2022) ("[T]here is no ambiguity: the Patent Act requires that inventors must be natural persons; that is, human beings."); *see also In re Application of Application No. 16*/524350, 2020 Dec. Comm'r Pat. 3-4; MPEP § 2109 (explaining the inventorship requirement for patent applications and noting that "[u]nless a person contributes to the conception of the invention, he is not an inventor.").

Advanced and Sophisticated Cybersecurity Threats

AI tools are being used by hackers to create believable phishing emails [*that users will likely click on*], quickly generate malicious code and perform malicious code error-checking [*to make sure everything works*]. AI tools are lowering the bar for inexperienced hackers and significantly decreasing the time it takes for malware built by experienced hackers to move from proof-of-concept to being production-ready. Aside from the ability to create malware, AI can be used to create different iterations of malware which are less likely to be picked up by advanced endpoint detection and response (EDR) software.

Here are 10 ways that attackers can use AI:

1. *Write scripts (code snippets that perform a specific function) that can do almost anything*
2. *Rewrite malicious code to be more stealthy*
3. *Write code in multiple programming languages*
4. *Perform error checking or optimization for code that has already been written*
5. *Write phishing scripts that users will actually click on*
6. *Perform documentation and explanation on how scripts works*
7. *Identify and potentially exploit vulnerabilities (through code that is written in AI)*
8. *Impersonate voices in order to perform social engineering attacks*
9. *Create deepfake videos in order to perform social engineering attacks*
10. *Draw conclusions or identify patterns in data (for reconnaissance or decision making on which entity to attack)*

Practical Tips: Hopefully, you already train your employees on cybersecurity and privacy threats, company policies, and industry best practices. It is vitally important to update each module of your company's training to provide guidance on the use of AI, ensure that employees are aware of the advantage that AI gives to hackers, and provide the tools your employees need to level the playing field.

Data Privacy Risks

Your employees' inputs are not confidential! Sharing personal information about customers, clients or employees on AI platforms can create various privacy risks. A few considerations are discussed here.

First, AI tool providers may use your inputs to improve their systems. Depending on the nature of the personal information being shared with tools such as ChatGPT, you may have obligations under US federal or state privacy laws to update privacy policies, provide notices to customers, obtain their consent and/or provide them with opt-out rights, etc.

Second, in order to comply with various regulations, you should be able to explain to end users (who may not be well-versed in the state of the art) how the AI system you are using makes decisions. The Federal Trade Commission has issued guidelines for data brokers that advise them to be transparent about data collection and usage practices and to implement reasonable security measures to protect consumer data. Both requirements are not easy to live up to when trying to translate and anticipate algorithmic predictions.

Third, you should understand how you will allow individuals to exercise their data privacy rights. One such important and globally-proliferating right is the "right to be forgotten," which allows individuals to request that a company delete their personal information. While removing data from databases is comparatively easy, it is likely difficult to delete data from a machine learning model and doing so may undermine the utility of the model itself.

Practical Tips: Consider the following as part of your generative AI adoption and policy program: (i) documenting lawful reasons for processing data, (ii) ensuring transparency, (iii) mitigating security risks, (iv) whether you were a controller or processor of personal data, (v) preparing a data protection impact assessment, (vi) working out how to limit unnecessary processing, (vii) deciding how to comply with individual rights requests, and (viii) determining whether generative AI would make solely automated decisions and how to opt-out individuals who object.

Advertising Law Violations Based on AI-Related Claims

Due to all the news and media coverage, "AI" is a buzz word used in marketing strategy to capitalize on the hype.

Just as with any other advertising claim, you need to be careful about what you say in consumer-facing materials about your company's use of AI. The FTC published a blog reminding companies to ""Keep Your AI Claims In Check". Claims about what your AI product can do, how it compares to other products, and how your company uses AI must be supported by *evidence*. The FTC cautions that "In an investigation, FTC technologists and others can look under the hood and analyze other materials to see if what's inside matches up with your claims."[6] As an example, it explains: "[b]efore labeling your product as AI-powered, note also that merely using an AI tool in the development process is not the same as a product having AI in it." *Id.*

Practical Tips: Make your advertising and marketing teams aware of the FTC's guidance and require adequate documentation or other evidence to support the claims.

Conclusion

The above is not a comprehensive list of legal issues to consider with respect to the use of AI tools. These are just examples and there are many more considerations, including but not limited to potential contractual violations, additional IP issues, liability stemming from inaccuracies, and further practical considerations. Some of the issues are specific to the type of AI tool involved. For example, with AI-based code generators, there are also open source issues that should be considered. To learn more about any of these issues, please do not hesitate to contact us.

For More Information, Please Contact:

Yasamin Parsafar
Partner
415.774.2927
yparsafar@sheppardmullin.com

Wynter Deagle
Partner
858.720.8947
wdeagle@sheppardmullin.com

This article is provided for information purposes only and does not constitute legal advice and is not intended to form an attorney client relationship. Please contact your Sheppard Mullin attorney contact for additional information.

[6] Michael Atleson, *Keep your AI claims in check*, Federal Trade Commission Business Blog (Feb. 27, 2023) (available at https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check).