From Creativity to Liability: Exploring the Legal Dangers of Using Generative AI Websites, Applications, and Chrome Extensions

Devin Bates
dbates@mwlaw.com
(501) 688.8864

Lizzi Esparza
eesparza@mwlaw.com
(479) 464.5660

06/05/2023

Reflective of the reality that the buzz around ChatGPT was just one first step in the AI revolution, there are now hundreds of applications and extensions that leverage generative AI to perform a whole host of tasks. But many commentators promoting the vast adoption of generative AI seem to do so with the assumptions that: (1) efficiency is king, (2) faster is better, and (3) the more the better. While there are certainly some tremendous gains to be recognized by adopting these new technologies, doing so hastily opens adopters to tremendous liability. This blog post explores that potential liability.

But first, what do you mean by hundreds of applications and extensions that apply generative AI? You can visit a variety of websites that put generative AI to work for you, but easier still, you can also download Chrome extensions that essentially link your web browser to these various programs. With extension, they "plug in" to your web browser and are always working in the background, processing data and doing their services.

So what can these generative AI applications and extensions do for me? The better question might be—*what can't they do for you?* You can get AI products to record and transcribe all of your meetings, summarize your documents and e-mails, summarize news, summarize Youtube videos, synthesize complex and technical text and give you simple explanations, translate between languages, check your grammar, write for you, create videos and images, create powerpoints, build websites, write code, and so much more.

So what's the problem? Where to start. To emphasize, the potential here is unimaginable. But when using emerging technologies online for free, sometimes as a Guinea pig, there needs to be some healthy recognition of the risk and the potential liability that using these tools opens up. Some of those risks include:

1. **Privilege**. Some professionals are bound by privilege and should therefore have an innate aversion to releasing any client data to anyone other than pursuant to a contractual arrangement where privilege is preserved, and safeguards are in place. Even if you are not bound by ethics rules and privilege concerns, especially if you are in possession of HIPAA, FERPA, GLBA, FCRA, COPPA, ECPA, VPPA, and/or DPPA protected information you have legal duties to safeguard that data. When downloading and using AI, if you check a box that allows the program to release this data there are significant legal consequences that can attach.

2. **Privacy**. Generative AI chrome extensions may require access to user data, such as browsing history and personal information. The privacy risks and liabilities there are manifold and prevalent. But even beyond the readily observable concerns, it is safe to assume, until proven wrong, that anything and everything that you are feeding to free online technologies is, or could be, feeding into larger sets of data that go into black boxes used by AI. However, a growing number of jurisdictions provide their residents with the right to delete their personal information even after they have provided consent. Put simply, machine learning works by building on mass quantities of data. Removing data from a generative AI system may not be so easy, as we have not quite cracked the code on "machine unlearning." In addition, even in the context of AI and machine learning, the human element cannot be ignored. We have already seen vulnerabilities that allowed bad actors to "talk" the AI model into revealing email addresses and payment information of other users. No system is 100% secure, but early adopters of generative AI should consider the ramifications of inputting content that contains another's personal information into an AI system where it may live and remain vulnerable indefinitely.

3. **Massive Amounts of Retained Data**. For the applications of AI that record and transcribe all of your meetings, or that otherwise create a record of activity where previously there might not have been a record, the use of AI creates a vast amount of data that can be staggering. Forget what you remember about gigabytes or terabytes, this amount of data can easily be measured in petabytes. (One petabyte (PB) is equivalent to 1,000 terabytes (TB) or 1,000,000 gigabytes (GB)). This data can become relevant and likely discoverable in lawsuits, and is arguably *the* issue that litigators of the future will need to deal with. As AI continues to evolve and is widely adopted, lawyers and other professionals will have AI for AI, and that vast amount of data will become easier to handle. But still, that data—*your* data—will be out there being stored, bundled, sold, and applied in various AI black boxes.

4. **Unexpected and Unknown Applications by Employees, Contractors, and Affiliates**. Do you know where your data goes, who inputs it into AI, and what happens to that data? No, you don't. And if you are an employer or otherwise overseeing others, you need to be aware that they may be trying out these new technologies. Navigating these issues in the workplace is a minefield, but there are tangible steps that employers can take to protect their business. How you handle adopting these new technologies, and shepherding your organization as it works with employees seeking to do so, raises many issues of supervisory liability.

5. **Intellectual Property Infringement**. Just as its name advertises, generative AI *generates* content, but not in a vacuum. It does so by drawing on existing examples and datasets, whether intentionally input by a user or automatically scraped from a website without the creator's consent. If generative AI chrome extensions generate content, there is a risk of infringing upon intellectual property rights. Even where a user of an AI tool does not intend to infringe on another's rights, a machine learning model that relies on another's content to generate new works presents the risk of reproducing another's content without their consent. Companies and individuals alike spend significant resources protecting their intellectual property rights through trademarks, copyrights, and patents. They also enforce those rights. Unauthorized use or reproduction of protected content can result in legal disputes and liability.

6. **Regulatory Compliance**. Organizations must ensure compliance with applicable laws and regulations. This includes adhering to consumer protection laws, advertising regulations, data protection laws, and any specific regulations related to the industry or sector in which the

organization operates. Many of the issues raised here have no consensus in the courts, which exposes you to, at minimum, the cost of litigating those unsettled questions. If you are allowing generative AI to draw from your data and do tasks for you, you need to be aware that this generative AI likely does not know about all of the federal, state, and local laws, rules, regulations, and codes that govern what you do. But your name will be on the finished product.

7. **Misinformation and Liability**. Generative AI models may produce inaccurate or misleading outputs. If users rely on the information generated by the extension and suffer harm or loss as a result, there could be potential liability issues for the organization responsible for creating the extension. But for the person who inputs information into generative AI and claims the output as their own without ensuring the accuracy of its content, there is oversight happening and judgment being exercised. There could later be liability if that oversight and judgment are called into question.

The AI revolution is upon us, and it is undeniable that there are certainly some tremendous gains to be recognized by adopting these new technologies. However, a human being sitting at the computer pushing the buttons and flipping around the output as work product creates potential legal liability. Thus, we caution clients against adopting this technology too rapidly and without guard rails lest the adopter expose themselves to tremendous liability.