How Generative AI Generates Legal Issues in the Games Industry

By: James Gatto

Roblox recently underlined announced that it is working on generative artificial intelligence (AI) tools that will help developers who build experiences on Roblox, to more easily create games and assets. The first two test tools create generative AI content from a text prompt and enable generative AI to complete computer code. This is just the tip of the iceberg on how generative AI will be used in games and a variety of other creative industries. Music, film, art, comic books, and literary works are some other uses. AI tools are powerful and their use will no doubt be far reaching. In the near term, so too will the associated legal issues. This article will focus on generative AI and some of the associated legal issues.

Uses of AI in the Game Industry

As covered in a recent article, there are several ways AI is being used in the game industry:

1. **Non-player characters (NPCs)**: AI is often used to control the behavior of NPCs in games. These characters can interact with players in a more realistic and dynamic way, adding to the immersion of the game.

2. **Game design**: AI is being used to design and balance game levels, as well as generate new content such as enemies and items. This helps developers create more diverse and interesting games with less effort.

3. **Gameplay**: AI can enhance gameplay by providing intelligent opponents for players to face off against. This makes games more challenging and rewarding for players.

4. **Virtual assistants**: Some games include virtual assistants that can help players by providing information or guidance during gameplay. These assistants use natural language processing (NLP) to understand and respond to player requests.

5. **Personalization**: AI can personalize gameplay for individual players by adapting to their preferences and playstyle. This helps keep players engaged and motivated to continue playing.

6. **Predictive analytics**: AI can be used to analyze player data and predict how they will behave in the future. This can help developers design games that are more engaging and tailored to the preferences of specific player segments.

7. **Fraud detection**: AI can be used to detect fraudulent activity in online games, such as cheating or hacking. This helps maintain the integrity of the game and ensures players have a fair and enjoyable experience.

Each use of AI can create legal issues. As noted above, this article will focus on some of the issues with generative AI.

Generative AI

Generative AI works by training AI models with huge volumes of data and/or content. This can include text, computer code, images and other content. This content can be obtained, for example, by scraping the web, accessing databases, or mining open source repositories. In the games industry, this content often will include copyrighted materials (e.g., game art, characters, computer code, music, etc.). As an oversimplification, AI models often rely on computer vision, natural language processing, and/or machine learning to recognize and replicate different patterns in the content. Once the model is trained, the AI tool can generate an output based on requested content. Sometimes, the output can be wholly created by the AI tool. In other cases, the output is a derivative of one or more items from the stored content. This raises numerous legal issues. The following are a few examples of those issues:

Sample Legal Issues with Generative AI

- Does use of copyrighted content to train models constitute infringement or is it fair use? The answer, as is often the case, will likely be fact dependent. AI tool makers often focus, in part, on the fact that they are extracting data from the content and thus it is a transformative use. They often cite the *Authors Guild* case where AI was used to scan books and create indices. Copyright owners typically focus on the fact that copies are made, often for commercial purposes, and that the outputs may affect the market for their content.

- Can collection of the content itself create liability? Occasionally, the AI tool will scrape the web for content. Various recent cases have addressed legal issues with web scraping. Some content can be pulled from open source software or data repositories. A challenge with this source of content is that even open source materials are typically subject to license terms. Sometimes, the license prohibits commercial use. In other cases, any derivatives must retain the copyright notice and in some cases give attribution to the original creator. However, not all AI tools do this.

- Is the output of the AI tool protectable by copyright? If the output is purely AI generated, likely not (at least in the U.S. for now). If a game developer uses an AI tool to create a character and the IP in the character is not protectable, that makes it difficult to stop infringers who use the character outside the game. On the other hand, if a developer uses an AI tool but also exercises substantial human involvement in the creative process, that likely will be protectable by copyright. It is not clear where the line of protectability lies between AI generated and significant human involvement.

- Another issue with AI generated output is whether it can give rise to infringement claims. If the output is based on copyrighted work, it may.

- A related question is, if there is infringement, who is liable? Is it the tool provider who stores the work and uses it to train the model? Or the user who requested and uses the output? The AI tool providers have cleverly drafted their terms of service in an attempt to minimize their potential liability and to try shifting liability for the output to users.

- Another issue is license compliance. If the output is based on content subject to a license that permits the intended use but requires, as a condition of use, compliance with certain obligations (retaining copyright, giving attribution to the copyright owner, identifying modifications, etc.), how does this compliance occur? Will tool providers need to identify the source of the generated output? In these cases, even if there is no infringement, could there be a claim for breach of contract?

- What if the content includes trademarks or other well-known brand identifiers that get included in the output? Likely there will be cases where there is trademark infringement.

- If the content used to train the models includes name, image or likeness (NIL) of celebrities, the output may implicate right of publicity issues.

- Depending on the nature of the content used to train the model, privacy issues may arise. One AI tool analyzed human movements of 50,000 players in over 2.5 million VR data recordings of a popular VR game. Within minutes, and sometimes seconds, the AI tool was able to uniquely identify the players with 94 percent accuracy.

- If players' faces are included in the content, biometric privacy and other issues may be implicated. Lensa, a popular AI app that generates avatars, is the subject of a pending class action suit for allegedly using plaintiffs' facial geometry data through the app, which violates Illinois's 2008 Biometric Information and Privacy Act.

The FTC has been one of the most active agencies in addressing AI.[1] The FTC's enforcement actions, studies, and guidance emphasize that using AI tools should be transparent, explainable, fair, and empirically sound, while fostering accountability.

As we addressed in a previous paper on Video Games, AI, and …the Law? the FTC has provided guidance around the use of AI in ways that avoid unfair or deceptive trade practices. For video game publishers, some of the FTC's key considerations include:

- *Accuracy*. AI components of a game or service should be tested prior to implementation in order to confirm it works as-intended.

- *Accountability*. Companies should consider how the use of AI will impact the end-user. Outside experts may be used to help confirm that the data being used is bias-free.

- *Transparency*. End-users should be made aware that the company may use AI, it should not be used secretively. Individuals should know what is being collected and how it will be used.

- *Fairness*. To further concepts of fairness, the FTC recommends giving people the ability to access and correct information.

Why does this matter?

In 2022, the FTC reached a settlement with a company for artificial intelligence/privacy violations by requiring them to destroy various algorithms and models. This is an example of algorithmic disgorgement, a penalty the agency can wield against companies that use deceptive data practices to build algorithmic systems like AI and machine-learning models. Consequently, this deception may result in being forced destroy ill-gotten data and the models built with it. Algorithmic disgorgement traced to illicit data collection/processing is intended to be a strong deterrent against improper data collection and model building using that data. For companies that invest significant amounts of money to collect this data and build these models, this can lead to financial loss plus fines.

How to Minimize Liability

What are some practical steps AI tool providers and game developers can take to minimize liability? Some AI tools take steps to prevent some of these legal issues by:

- judiciously selecting the source and type of content used to train AI models;

---

1 In 2016, the FTC issued a report titled Big Data: A Tool for Inclusion or Exclusion? advising companies using big data analytics and machine learning to reduce the opportunity for bias. It held a hearing in November 2018 to explore the Competition and Consumer Protection Issues of Algorithms, Artificial Intelligence, and Predictive Analytics. In June 2022, the FTC issued a report to Congress on Combatting Online Harms Through Innovation. One of the key takeaways from this report is that the deployment of AI tools, intended to detect or otherwise address harmful online content, is accelerating but that governments, platforms, and others must exercise great caution when either mandating the use of, or over-relying on these tools even to reduce harms.

- recording data provenance, managing metadata, mapping data and creating model inventories;

- filtering out content (e.g., images that include recognizable faces); and

- limiting requests to generate high risk content (e.g., requests for the NIL of well-known figures).

Other tools, filters, and techniques can also minimize certain anticipated legal issues. For example, some technical solutions have been and are being developed. The "Stack" is a dataset for training AI designed to avoid copyright infringement issues. It includes only code with permissive open-source licensing and offers developers an easy way to remove their data on request.

DeviantArt has created a metadata tag for images shared on the web that warns AI researchers not to scrape their content. Sites such as Cohost, have adopted the tag across its site.

Other technologies are in the works and more will likely follow.

Conclusion

The power and potential of AI is irrefutable. However, its use can create significant legal issues. To avoid damages for IP infringement or breach of contract and to avoid loss of significant investments due to algorithmic disgorgement, it is critical for legal departments to work with their data scientists to ensure that AI risk mitigation is designed into AI modeling and data collection.

For further details on generative AI, please contact:

James Gatto
Blockchain and Fintech Team Co-leader
bio
202.747.1945
jgatto@sheppardmullin.com

Sheppard Mullin's Blockchain Technology and Fintech team helps clients develop innovative and comprehensive legal strategies to take advantage of what may be the most disruptive and transformative technology since the Internet. We focus on advising clients on how to meet their business objectives, without incurring unnecessary legal risk. Our team includes attorneys with diverse legal backgrounds who collectively understand the vast array of legal issues with and ramifications of blockchain technology and digital currencies. More Information