Navigating AI and the Law in the Travel Industry:
An Introduction to Legal Implications for DMOs (Part 1)

May 1, 2024

By Kara Franker & Roxanne Steinhoff

Table of Contents

Introduction 1

A. Breaking Down How AI Works: Understanding Liability through Inputs and Outputs 2

B. The Juxtaposition of AI and Data Privacy 3

C. Intellectual Property Issues & Ethical Considerations: Copyrights, Use and Likeness, Trademarks 4-5

D. Other Issues 6

E. Conclusion and Call for Industry Guidelines 7

Introduction

Innovation invariably attracts legal scrutiny, and as destination marketing organizations (DMOs) delve into the burgeoning realm of artificial intelligence (AI), we find ourselves navigating a legal landscape that is as evolving as it is challenging.

Let's face it: we are in a new world regarding the use of AI in the travel industry. Sprinkle in plenty of gray areas, and a world of legal conundrums awaits. And that is the last thing most DMO leaders want to decipher, considering the long list of political minefields we all face daily. At the same time, harnessing the power of AI can give DMO teams the ability to work smarter and more efficiently. For example, see Visit Estes Park's recently published white paper[1] on how they are using the technology.

What's more, the law hasn't really caught up with the technology and how we use it, which puts everyone in liability limbo. Sure, there are some stars we can look to as we sail the sea, but finding the Northwest Passage through these uncharted waters will take time and, unfortunately, a few failed expeditions to mark the dangers.

Two things we do know for sure: (1) there's no turning back, and (2) there's no reward without risk. AI can give your DMO team superpowers, but successfully navigating these waters requires both bravery and assiduousness. What follows is a celestial chart of sorts, briefly plotting out the legal concepts surrounding DMO use of AI and the obstacles to be on the lookout for.

It is easy to get overwhelmed by the legal liability and ethical considerations of AI, but that is not our intention. Instead, we plan to start the conversation by recommending a few guardrails and thoughts in this area, but ultimately, DMOs will need their own tailored legal advice from a licensed attorney. And the industry needs guidelines to address legal and ethical concerns related to privacy, bias, fairness, transparency, and accountability in AI systems. This paper is not legal advice but is merely a conversation starter to consider the underlying concerns for those future guidelines.

[1]Franker, Kara, and Heidi Barfels. "From the Base of the Rocky Mountains to the World" Visit Estes Park, [1] May [2024], www.visitestespark.com/ai/.

A Breaking Down How AI Works: Understanding Liability through Inputs and Outputs

We can use AI inputs and outputs as references to understand liability. But first, we need to understand how AI works and how it is accessed. Generative AI processes input data through learning algorithms and models to produce a requested output. In short, generative AI creates content from the data on which it was trained. Input data could be words, images, sounds, videos, location, preferences, browsing or usage history, etc., or anything you can imagine that could be captured and quantified in the digital world.

The first key question to keep in mind: where does the input data come from?

Because when it comes to AI, (almost) everything comes from something else. Input data is not just that which is scraped from the internet and other public sources, but it is also that data that users provide.

One of the main issues in the legal landscape surrounding AI right now is the regulation and treatment of input data. Specifically for DMOs, these concerns center around data privacy and intellectual property (IP) rights. Other concerns could involve violations of contractual obligations. More on that in a minute.

Similarly, the output could be text or pictorial content (e.g., marketing copy and design), or decisions expressed in a human-understandable format (e.g., travel recommendations).

The second key question: how could the data outputs be used, and who owns them?

Again, for DMOs, the concern here is the implications for IP rights both in use and ownership, as well as the liability associated with illegal biases, inaccurate information, and contractual obligations.

Still thinking in the context of inputs and outputs, another critical component in understanding liability is the contractual relationship, or the "license," to use a legal term that exists between the AI provider and your organization.

There are basically two ways for DMOs to access AI (assuming most DMO's don't have AI developer engineers on staff currently to develop their own models, but maybe that's the next big thing): (1) publically available AI models where any member of the public can upload content and type a prompt for a desired output (e.g., ChatGPT and its competitors by Google, Microsoft, Meta and Amazon, among others); and (2) a private AI model managed and curated by an AI service provider.

Early AI models like ChatGPT-2 were open to the public in every sense of the phrase: they were free to access and are widely distributed, the source code itself is accessible, and the license granted allowed for use for virtually any purpose, including distribution of modified versions of the software. (Note that ChatGPT-3 remains freely accessible to the public, with the exception of its proprietary source code.) However, this also means that any input data uploaded to a public AI is used by the platform to enhance the services it provides, and that data could potentially be accessed and used by anyone else using the AI model. (E.g., see OpenAI's terms and conditions[2].)

In contrast, the license associated with a private AI model will be more restricted and governed by a lengthy contract that your organization enters into with the service provider. In these cases, the input data is more protected and may not even be used to train the underlying AI model (e.g., see Intentful's description for HappyPlaces[3]).

In assessing your organization's liability, you should be thinking not only about the input data your team uploads but also about where the AI model you're using gets any other input data. You should also consider how the outputs could be used and whether your organization has the legal right and ethical ability to use them for your intended purpose.

[2]Privacy Policy, OpenAI, 14 Nov. 2023, openai.com/policies/privacy-policy.
[3]"Happyplaces Ai." Intentful, www.intentful.ai/ai-for-dmo.

B The Juxtaposition of AI and Data Privacy

It is no coincidence that the rise of AI happened in the age of unprecedented data collection, as it is AI's ability to analyze and leverage vast amounts of data that essentially gives superpowers to human marketing teams. Never has it been easier for DMOs to collect visitor information at such volume and in such granular detail as it is now. But where the law on AI plays a bit of catchup, data privacy regulation is out of the gate.

Data privacy protection laws are somewhat unique from other regulatory schemes as many are extraterritorial in nature. In non-lawyer speak, the laws apply to businesses outside of the physical territory of the governments that enacted them. Given our cross-border purpose of drawing visitors to our destinations, this means that DMOs are subject to the data privacy laws of where their website visitors reside in addition to the jurisdiction where the DMO is physically located. So far, the California Consumer Privacy Act (CCPA) and European Union General Data Protection Regulation (GDPR) are the most comprehensive regulatory schemes, but there are a handful of laws regulating data privacy currently on the books in the United States with many states considering passing their own legislation.

The good news is that the CCPA, GDPR, and other laws are substantially similar in nature, and it's likely that any future proposed laws will follow in the same vein for the sake of ensuring compliance in our interconnected digital world. Generally speaking, data privacy laws require transparency and responsible stewardship: organizations collecting personal data must protect that data from unauthorized access, state what data the organization is collecting, what that data is used for, how long that data is retained, and allow for individuals to "opt-out" of the data collection and to request deletion of any past-collected data.

However, AI and data privacy create a juxtaposition: AI is built and trained to learn from input data to segment audiences, predict individual preferences and create personalized marketing messages to target specific people, while data privacy laws aim to restrict the use of personal data, ensure that the use of personal data is transparent, and allow for deletion of personal data.

So, in the context of DMOs collecting visitor (aka consumer) data for use by AI models, issues arise with data security, retention and use. **First, AI generally retains base and training data**: if a visitor's information is used as part of the underlying dataset, it may be extremely difficult to "wipe" that data from the AI model.

Second, data privacy laws limit the processing of personal information to the disclosed purposes only. However, it can be nearly impossible to accurately predict to an exact degree what the AI will learn and how the outputs from that underlying data will be used in the future. These issues are especially of concern where visitor data is uploaded to open source AI, which by its very nature is unsecured and its uses seemingly infinite.

In short: do not upload visitor data to public AI models.

And in the case of private AI providers, make sure you understand how that data will be used and if it could be potentially shared.

Data privacy isn't just a visitor issue. So far, much of the focus on data privacy and the use of AI has been on employment law issues. For example, some employers are using AI to screen potential job applicants. AI can crawl the internet for information about employees and prospective employees, some of which is off-limits during an interview or on an employment application (such as marital status, political orientation, sexual orientation, race, nationality, or religion.) The underlying data set can create subconscious biases that are actually enhanced by the use of AI and lead to discriminatory outcomes. See, for example, lawsuits against IBM[4] and an US Equal Employment Opportunity Commission (EEOC) settlement with iTutorGroup[5] for AI-based age discrimination.

Here's the bottom line:

Your DMO's use of personal data must be transparent, and that includes how it is used in conjunction with AI. This means that your team should ensure that its data privacy policies and AI policies are aligned. Additionally, you should ensure that your private AI provider has adequate safeguards in place to prevent breaches, as well as the ability to erase or anonymize personal data if and when needed.

[4]Atkinson, Khorri. "Rising AI Use Paired with Layoffs Invites Age Bias Litigation." Bloomberg Law, 17 Oct. 2023, news.bloomberglaw.com/daily-labor-report/rising-ai-use-paired-with-layoffs-invites-age-bias-litigation.

[5]"ITutorGroup to Pay $365,000 to Settle EEOC Discriminatory Hiring Suit, U.S. Equal Employment Opportunity Commission, 11 Sept. 2023, www.eeoc.gov/newsroom/itutorgroup-pay-365000-settle-eeoc-discriminatory-hiring-suit#:~:

C Intellectual Property Issues & Ethical Considerations: Copyrights, Use and Likeness, Trademarks

Here's the basic rule of thumb of U.S. copyright law that most of us already know, given our day jobs: to be able to use a creative work, you must have the right to (1) use that work (2) for the purpose for which you intend to use it. For work that the staff of a DMO does not create itself (e.g., creative produced by independent contractors, photographers, travel writers, ad agencies, etc.), a license will govern the DMO's rights to that work.

Here's the first big IP issue in AI right now: what is the copyright status of the input data AI uses to generate creative works, and who is liable for infringement?

Let's tackle public AI models. Platforms like OpenAI's ChatGPT and DALL·E gained their source data inputs by scraping the internet for information. Novels, images, and other creative works were used to train these AI models, seemingly without the permission of the original authors. At the time of writing, there are a number of lawsuits in process to determine whether this scraping constitutes copyright infringement.

What about inputs from open-source licenses or royalty-free sites like Unsplash or Creative Commons? Wouldn't input data scraped from those sites be protected from infringement? The short answer is no, because content subject to these licenses is still copyright-protected. Just like all creative works, the terms of the license will grant the appropriate use and attribution requirements.

What does this mean for DMOs? The upshot is that if these suits are successful for the plaintiffs, certain creative outputs generated by AI could be considered illegal derivative works based on copyright infringement. At best, the AI companies will face the brunt of the liability; at worst, your organization could be on the hook for infringement.

These same issues also apply to any AI users who upload copyrighted works, whether the AI platform is public or private. The benefit of using private AI is that while there may be some underlying data sets that allow the models their base functions, the input data usually comes primarily from your organization. This means you have much greater control over the dataset and, therefore, ostensibly greater protection from infringement claims. Additionally, your service agreement will also likely contain greater protection for your organization if the use of underlying data is found to be infringing. However, your service agreement will assuredly require your organization to indemnify the service provider for third-party claims of copyright infringement for inputs you upload. (The terms of use of public AI sources likely require this as well, but these terms may not be as clearly enforceable as in a private contract.)

Here's the bottom line:

You must own or have the appropriate license permissions to use whatever reference material you feed to your AI model or any public AI model. Otherwise, you risk infringing on the original owner's copyrights if you then use the AI outputs trained on impermissible reference materials. The risk of copyright infringement is also greater when you don't know what data is used to train the AI model you're using, or your organization is otherwise not protected by contractual terms limiting your liability.

This brings us to the next big IP issue in AI: what are the copyrights of work created using AI?

One thing is clear: the U.S. Copyright Office, as well as most courts, have determined that only human authors may receive copyrights. What this seems to mean is that creative works generated entirely by AI tools are ineligible for copyright protection, but what remains less clear is the required extent of human control over AI for a work created using AI to be copyrightable.

It would seem then that ad copy generated from an AI model that is then subsequently edited by a human would be copyrightable (assuming the underlying input material is not infringing), while AI-generated images would not be. While it is unclear how much editing by humans would be required for images, it would seem to be more than minimal. These considerations are important for those projects where your organization wants ownership of its creative work.

Right to Publicity: Name, Image & Likeness

We've all seen the videos depicting deep fakes. The fact is, it is easier than ever before to create lifelike images, videos and audio impersonations of people. Not only does this have profound societal implications, but it also has ethical marketing implications. Do you want to run a silly destination ad starring an AI version of Scarlett Johansson[6]? Or maybe you want to create a new song "performed" by Drake or Ariana Grande[7]? Well, now you can, but should you? You should not.

Most of us have encountered publicity rights in our daily work, most commonly in our use of photographs and video. A refresher: every person has a right to control the commercial use of their name, image, likeness, or any other personal characteristics indicia of persona, and therefore an individual's persona cannot be used for commercial purposes without their consent. State law governs publicity rights, so while some nuances depend on the state, generally speaking, you must obtain permission from a person before using their likeness for advertising purposes.

The risks with using AI-generated human impersonation are the same as any other "old school" use of likeness: **if you do not have permission, don't do it.** And besides the legal considerations, it would be unethical to use the likenesses of others without their consent. These seem relatively straightforward (so far) for images and voices, but what about music?

Thanks to AI, the days of tediously sampling royalty-free track after track for the right background music are coming to an end, or at least allowing users to generate their own jingles in a quicker time. And some AI tools can even mimic artists to create spoofs or new music. Have you ever heard Johnny Cash sing Barbie Girl[8] or the AI mashup of Drake and The Weeknd[9]?

Spoiler:

Musicians and their estates are suing AI for these music creations. However, there's been a lot of movement here in the past year, and it appears that Google and Universal Music Group are in talks to license artists/ voices, lyrics and sounds to generative AI[10] which would make navigating this issue much easier. But in the meantime, the takeaway is that if you use AI to create music, you or the AI platform provider must have the rights (the permission), to use that underlying music or to imitate an artist's voice.

[6]Zielaznicki , Karl M., et al. "The Intersection of Generative AI and Copyright Law." Troutman Pepper - The Intersection of Generative AI and Copyright Law, Aug. 2023, www.troutman.com/insights/the-intersection-of-generative-ai-and-copyright-law.html.

[7]Johnson, Arianna. "Ai-Generated Music Is Here-'sung' by Stars like Drake and Ariana Grande-but It May Be Very Illegal." Forbes, Forbes Magazine, 5 May 2023, www.forbes.com/sites/ariannajohnson/2023/05/03/ai-generated-music-is-here-sung-by-stars-like-drake-and-ariana-grande-but-it-may-be-very-illegal/?sh=731e43ba3aa3.

[8] "Johnny Cash - Barbie Girl (A.I. Cover by There I Ruined It) Restoration." YouTube, YouTube, 22 Sept. 2023, www.youtube.com/watch?v=MAFdzBTe2Ig.

[9] "A.I Generated Song 2023| Drake Ft. the Weekend Heart of My Sleevelldaigo." YouTube, YouTube, 20 Apr. 2023, www.youtube.com/watch?v=gaxgpqAdUYM.

[10] Roush, Ty. "Google and Universal Music Group Negotiating AI-Generated Music Tool, Report Says." Forbes, Forbes Magazine, 5 Oct. 2023, www.forbes.com/sites/tylerroush/2023/08/08/google-and-universal-music-group-negotiating-ai-generated-music-tool-report-says/?sh=20bc376822e7.

Trademarks

Say you're hosting an event and you need a logo, or you want to create a modified version of your main DMO logo for a specific ad campaign. You upload your logo to a generative AI platform and ask it to create something new based on your prompts and input examples.

Here's the risk: logos are trademarks, and continued protection under trademark law depends on policing unauthorized use. Remember that on an AI platform, any inputs become part of the model's dataset. So, when you upload your logo, you may unintentionally authorize use by others, or otherwise dilute your right to protection from infringement.

Like many legal issues surrounding AI, this is another unanswered question. The greatest danger certainly lies in uploading logos or other trademarks to public AI models. Still, private AI models may also have some risks as well where your inputted data becomes part of the model's overall training.

D Other Issues

If you take anything away from this article, let it be this:

Your DMO's use of AI does not exist in a vacuum. Inputs are governed by law, contractual obligations, and ethical considerations, as are your use of outputs. This means you should be looking at your use of AI in the context of your entire organizational ecosystem.

When using AI, consider how it affects other agreements your organization has. For example, take any agreements with your partners regarding their benefits. If you're using AI to direct visitors to partners, you need to ensure that your model equitably represents partners to ensure their benefits are being met. (Visit Estes Park learned this lesson quickly when they asked their board members to try out their new visitor-facing AI tool, Rocky Mountain Roamer, and it turns out the AI model didn't have information on the board members' businesses, so the Vist Estes Park team had to train it.) And, because AI constantly evolves based on its inputs and feedback, your team should be continually monitoring for unintentional partner biases.

Another potential example involves AI unintentionally creating false advertising on its own or by providing false facts to your team. Because AI is built on models of statistical satisfaction, it can perpetuate biases and mislead users or otherwise point to non-existent facts or experiences. This requires constant double-checking and revising by your team to avoid these kinds of visitor-facing issues and for any internal use.

E

Conclusion and Call for Industry Guidelines

There are a lot of unknowns when it comes to governing legal obligations for AI use. Many of these questions will be answered in the next few years as current legal challenges make their way through the courts and lawmakers catch up with the present. But with careful planning, execution, and constant revision, **there is no reason DMOs shouldn't be using AI to promote and manage their destinations.** Remember the discussion about inputs and outputs. Using an AI model to brainstorm ideas for website or social media content is a completely different and fine use, versus feeding it proprietary data, which is not a safe use. DMO staff needs to understand the differences.

To use AI in a way that also accounts for these legal and ethical implications, DMOs need a guiding light. The industry needs a set of guidelines and principles governing AI use. These guidelines could include commitments to fairness, accountability, transparency, and privacy. For example, Google has AI principles that guide its development and use of artificial intelligence, and Microsoft has an AI framework that emphasizes fairness, reliability and safety, privacy and security, inclusiveness, transparency, and accountability.

And while a set of industry guidelines would not take away all the risk and liability, it would at least provide a starting point. Until then, **keep the principles and issues discussed here in mind, and remember the best bet to limit liability is for each DMO to seek the advice of legal counsel.**

Kara Franker

As CEO of Visit Estes Park, Kara Franker is an advocate for innovation and leadership in the tourism industry. She is a licensed attorney, serves on the board of delegates for the U.S. Travel Association, and serves on advisory boards for Simpleview and eTourism Summit. A Certified Destination Marketing Executive (CDME) through Destinations International, she recently obtained her executive certificate in artificial intelligence and business strategy from MIT.

Already in 2024, Kara has spoken on panels about AI for destination marketers during International Media Marketplace's (IMM) TravMedia Summit in New York City, as well as the Marketing Outlook Forum in Houston with the Travel and Tourism Research Association (TTRA), among others. She is also serving as an expert advisor in the AI Opener for Destinations program by Miles Partnership and Group NAO.

Roxanne Steinhoff

Roxanne Steinhoff is an attorney with almost a decade of experience in destination marketing and sports tourism. Her boutique law and consulting firm – Steinhoff Law – services DMOs and sports commissions. With a focus on collaborative consultation, Roxanne's practice centers on empowering her clients.

Her background includes serving as lead sports consultant and heading the legal department at Civitas, a firm specializing in providing funding solutions to DMOs. As part of the Chicago Sports Commission team, she hosted major international sports events like the 2020 NBA All-Star Game. Roxanne began her career working on Boston's bid for the 2024 Olympic and Paralympic Games.

Roxanne earned her J.D. from the Michigan State University College of Law, graduating in the top 2% of her class. She holds an M.A. in International Relations from Boston University, and a B.A. from Lake Superior State University. She is also a published author and adjunct college professor. Roxanne resides with her partner and fellow attorney Rob in Michigan's Upper Peninsula.