WFA

Managing IP Risk when using Generative AI in Marketing

January 2025

Managing IP Risk when using Generative AI in Marketing: Executive Summary

In September 2024, **WFA member research of 48 multinational brands revealed that 63% are already using generative AI ("Gen AI") for marketing purposes.** From content creation, ideation and production to task automation, strategic planning and media optimisation, Gen AI is already transforming the marketing industry, holding promises of more effective, efficient and personalised marketing communications.

However, despite these opportunities, **66% of brands state that legal challenges continue to be the main barrier to Gen AI adoption,** with **77% claiming they are most concerned about intellectual property (IP) and copyright risks.** This is corroborated by the cautious approach brands are taking when it comes to using AI-generated content in marketing assets. **In fact, only 40% of those adopting Gen AI today are using AI-generated content in user-facing marketing communications.**

To support members as they navigate Gen AI's challenges and leverage the opportunities of this technology with confidence, this document aims to clarify some of the key IP concerns brands may face in the context of its use for marketing purposes. It also puts forward some proposed voluntary guidance on the steps they could take to mitigate identified IP risk.

This document does not address other risks, such as data privacy and regulatory risks, risks of bias and discrimination, or contractual risks, the latter of which is covered in this WFA Generative AI Contact Best Practice.

Please note that nothing in this document serves as legal (or other) advice, but rather as support for brands' own identification and mitigation of risk. The voluntary guidance, drafted with the support and expertise of WFA members, may not be appropriate for all companies, so we recommend that you seek advice from your lawyers and other advisers before relying on the voluntary guidance in this paper.

"Addressing Gen AI's legal risks is a top priority for brands. This report comes at a crucial time, providing brands with a clearer understanding of the IP challenges they face when using Gen AI in marketing and actionable insights on how they could tackle them. Our goal is to empower marketers to unlock the technology's potential as part of our steadfast commitment to providing members with the knowledge and voluntary best practice they need to protect their brands and drive more effective and efficient marketing."
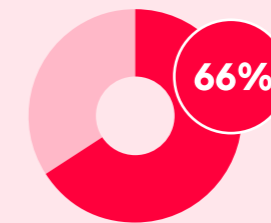
Stephan Loerke, CEO, WFA

63% of WFA members are already using generative AI
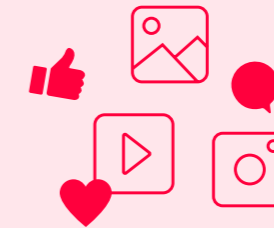
Of that 63%, only 40% are using AI-generated content in user-facing marketing communications

66% State that legal challenges are the main barrier to adoption...

77% are concerned about IP and copyright risks

Contents

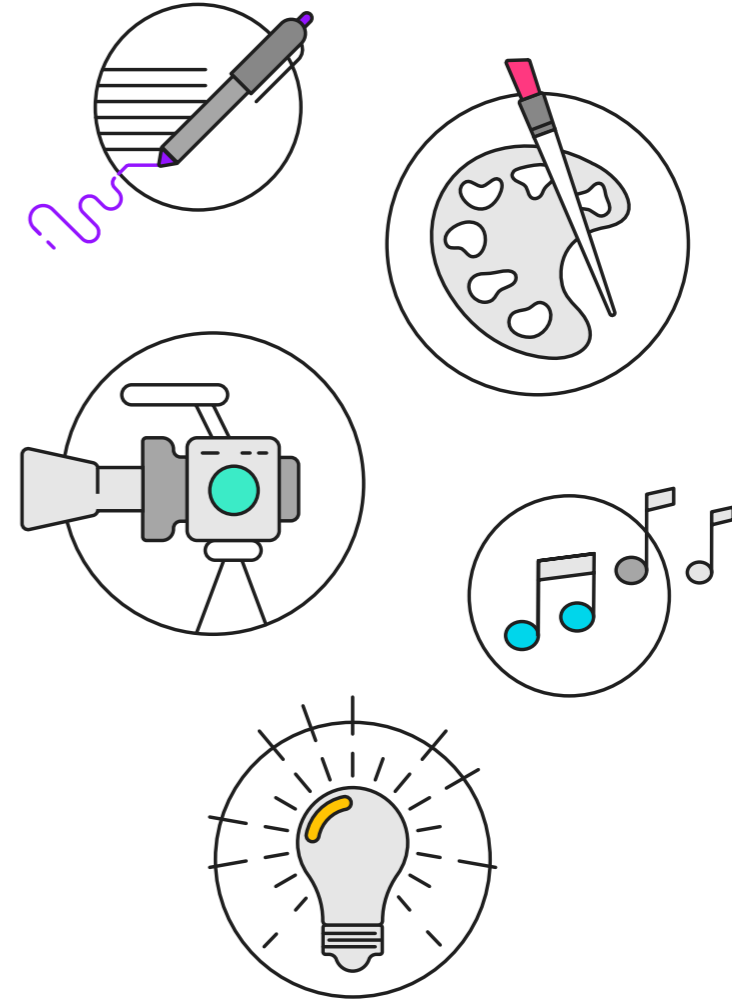# What is Gen AI and why might it involve IP risk?

generative artificial intelligence

At its most basic, Gen AI can be defined as a form of AI which produces new content ("outputs") on the basis of the patterns it has learned through training data and user prompts ("inputs").

Gen AI tools have captured the attention of people all around the world in a way that no other technology has not only because of their broad utility, but also because of their ability to emulate content and conversation in a way that closely resembles that produced by humans. Gen AI's ability to write text, compose music, create digital content and more is revolutionising all fields where creation and innovation are key, including marketing.

However, the widespread adoption of Gen AI tools has led to many complex IP concerns (both 'technical IP' such as patent and novelty requirement, trade secrets and 'marketing IP') and the future of Gen AI's technological development and adoption will, in large parts, be influenced by the outcome of current IP debates, especially in industries like marketing, content creation and entertainment.

**But what are the IP risks and why do they pose such an issue?**
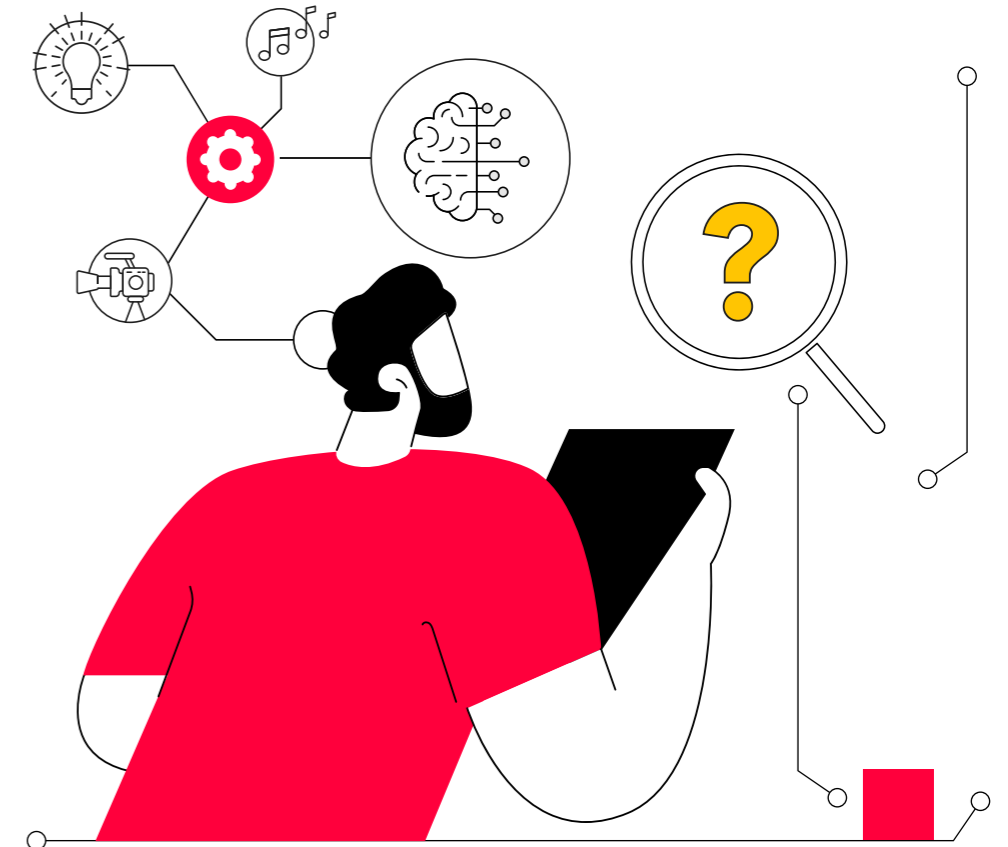
Features of Gen AI tools
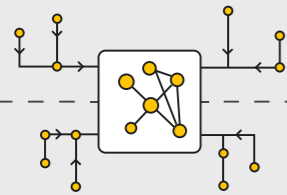
Training Datasets

- Models are trained on vast amounts of data, often scraped from the open web.

- This training data typically includes IP-protected works, sometimes without necessary permissions.

- Once models have been trained on particular datasets, it is very difficult and sometimes even impossible to remove particular content, due to limited traceability of what happens to that data.
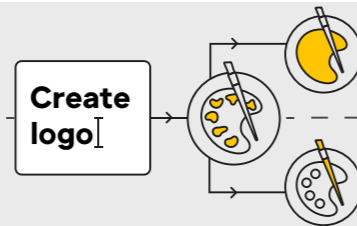
Outputs that Resemble Inputs

- Gen AI models are generally predictive, relying heavily on recognising and replicating patterns from the data they were trained on and prompted with.

- The outputs can therefore closely resemble the original works they were trained on, leading to IP infringement risk.
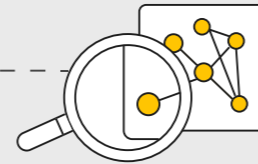
Lack of Model Training Transparency

- Most Gen AI model providers do not share details of their underlying datasets. This means there is an inherent lack of traceability regarding what inputs were used to produce them.

- Very few provide indications about the sources that were used to generate particular responses (and those that do are often incorrect).

- This fact complicates determining where content came from and whether an output potentially violates any existing IP rights.
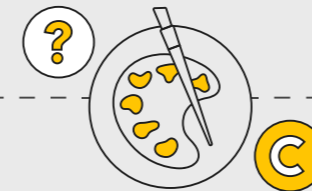
Questions around Ownership of Outputs

- Questions remain about who owns rights in AI-generated content; the user, the AI developer, the machine, or whether any rights exist at all.

- Current IP laws rely on the concept of human authorship, a concept which is being challenged by machine generated works.

- Questions remain about the level of human involvement required to establish IP rights.

Divergent Contractual T&Cs

- Terms and conditions under which tools are offered can vary widely between providers.

- T&Cs are often "click to accept" or "use to accept". In particular, oftentimes user inputs are used for continuous model training, but this is not always explicit and control may be lacking to limit such activities or opt-out entirely while still retaining use of the particular solution or tool.
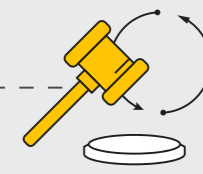
### Evolving Legal Landscape

- Global regulation and case law around IP matters relevant to Gen AI are still in flux and often differ from one jurisdiction to another.

- This poses challenges for legal teams to navigate the complex and shifting legal terrain to mitigate risk.

With these common features in mind, WFA has identified six IP risks most relevant to the use of Gen AI in marketing...

WFA

Key IP Risks relevant to the use of Gen AI in marketing

1 — Loss of control over brand IP input into tools
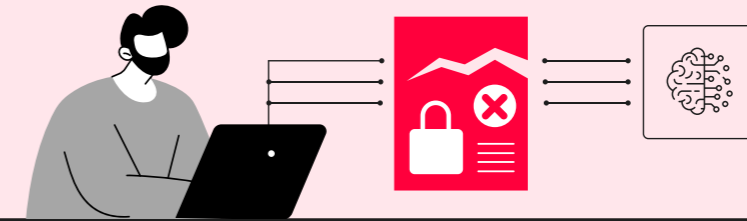
2 — Breach of third-party IP rights via inputs
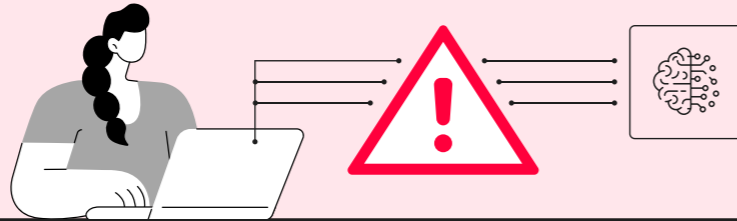
Loss of control over your brands' IP and data input into Gen AI tools by your staff, agency staff and/or other suppliers: Many providers of AI tools automatically ingest any data inputs into their (or third parties') learning algorithms and training datasets. Once this information has entered into an AI model, it may be extremely difficult to delete or change the information, meaning that any damage to IP may be practically irreversible. This means that data input into the tool can become accessible by third parties using the tool in the future:

- The confidentiality of brand's inputs and outputs can be lost and valuable brand data and IP (such as trade secrets) can become public knowledge.
- The opportunity for the brand to register some types of IP protection (such as patents, where novelty is required) can also be lost.

In addition, some providers take broad rights to use any inputs or outputs for any purpose. This means brands may inadvertently grant broad licences to use brand assets and data to third parties, just by their use of a Gen AI tool.

Example: Samsung ChatGPT case, where Samsung staff put the company's source code into ChatGPT in an attempt to fix some broken code. They used a version of ChatGPT that ingested the data into the learning algorithm, meaning the source code could, in theory, be accessed by anyone using the tool.

Breach of third-party IP rights or confidentiality by inputting third-party IP or data into a Gen AI tool without necessary permissions: Gen AI tools ingest a wide variety of data sources and can easily plug into third party databases via APIs. This means it is easy to accidently provide third-party data / IP to a Gen AI tool without the necessary permissions from the rights holder. As above, once this information has entered into an AI model, it may be extremely difficult to delete or change the information, meaning that any damage to IP may be practically irreversible.

Example 1: Marketer looking for deeper consumer insights feeds a Gen AI tool with data licensed from a data insights provider to generate a report on current consumer trends. The license with the insight provider does not extend to sharing the data with a Gen AI tool and the brand is now in breach of the license.

Example 2: Agency uploads a photograph of a model taken for a particular campaign into a Gen AI tool and alters the original photo for a new campaign. The model's original consent did not extend to the use of their image in a Gen AI tool or a new campaign and the brand now faces an infringement/breach of contract claim.

Key IP Risks relevant to the use of Gen AI in marketing

**3** **Breach of third-party IP rights in outputs**
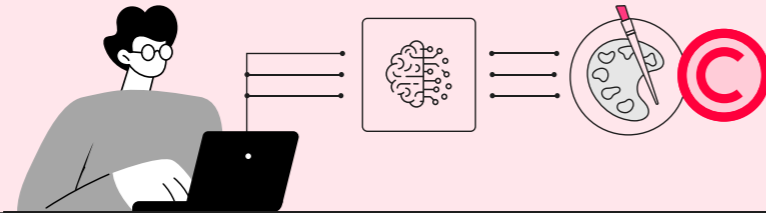
Generating brand outputs that inadvertently infringe third-party IP rights:
Gen AI tools can create outputs that unintentionally incorporate elements resembling third-party intellectual property or copyright-protected works. This occurs because AI models are often trained on large datasets that may include copyrighted or other IP protected material without the underlying IP owners' permission, making it difficult to ensure that the output is entirely original and free of legal risks.

Example: A marketer uses an image generator to create a visual for a new campaign. The generated image closely resembles a well-known logo or design owned by another brand. Despite no intention to copy, this output could still violate copyright or trademark laws. For instance, a stylised animal in the generated image might look very similar to an existing mascot of a popular brand. If this image is used in promotional materials, the brand could face legal action for infringement, even though the resemblance was unintentional.

4 **Lack of clarity around ownership of Gen AI**
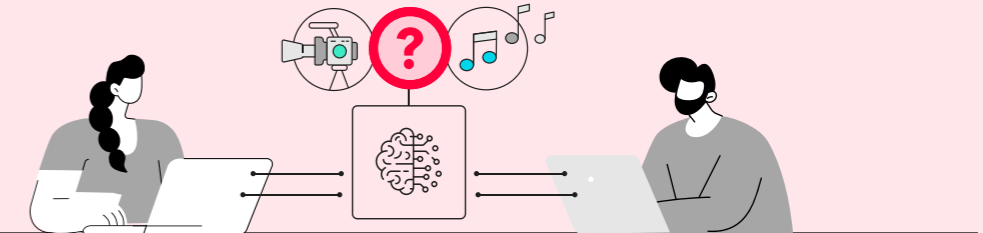
Lack of ownership or exclusive rights over IP in outputs created by Gen AI tools:
It is easy to assume that a brand will automatically own IP rights in the outputs they generate through Gen AI tools, but this is not always the case. Depending on the terms of service of the AI tool/agency and the legal frameworks involved (which vary by country), there may be no path to ownership or exclusive rights to outputs:

- Some AI tools providers do not assign IP ownership in outputs to the user, or if they do, they may seek broad rights to use the outputs themselves, making it difficult for brands to fully control or protect the content they are using.
- AI tool providers will not guarantee that outputs are unique or capable of ownership, which can lead to issues such as the inability to prevent others from using similar outputs.
- Many important IP rights embodied in law rely on the concept of human authorship; a challenging concept when the AI tools are "creating" outputs.

Example: A marketing team uses a sound/music generator to create music as the central audio identity of their campaign. However, due to the terms of the AI tool, the rights to the audio are not exclusively owned by the brand. After campaign launch, another company uses the same tool to product a video ad with an identical background voiceover and score. Because the brand doesn't have exclusive rights to the audio, they are unable to prevent the other company from using it.

WFA

# Key IP Risks relevant to the use of Gen AI in marketing

5 Fraudulent AI generated paid-for-Ads
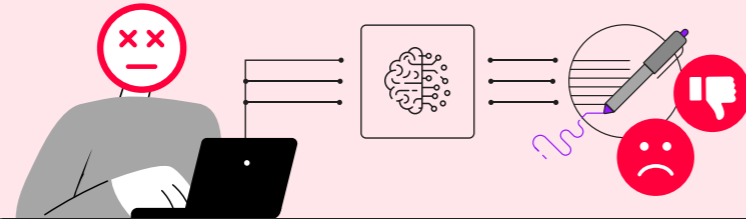
Third-party AI-generated fraudulent ads impersonating your brand (paid media): Fraudulent advertising remains a gateway to illicit online sales and a threat to both advertisers and consumers alike, challenging brands intellectual property protection efforts. Gen AI, with its ability to produce content at scale and replicate the styles and likeness of established brands, amplifies this risk. Malicious actors can now create deceptive campaigns that closely mimic legitimate brands at unprecedented scale and speed, making it easier to place fraudulent media that misleads consumers and undermines brand trust and their IP rights.

Example: An individual uses Gen AI to create a fraudulent ad that mimics a brands logo and style. The ad, which is bought and placed on several social media platforms, promotes a fake sale and directs consumers to a counterfeit website. Consumers who engage with the ad provide payment information, damaging trust in the legitimate brand. This type of impersonation deceives customers but also infringes the brand's IP rights, leading to reputational harm.

6 Fraudulent AI generated organic content
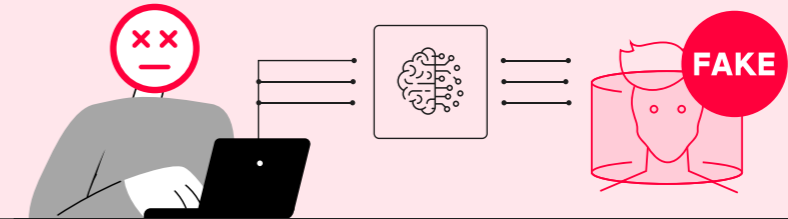
Third-party organic content impersonating your brand (brandjacking/brand disinformation): As above, Gen AI represents an opportunity for malicious actors to impersonate and manipulate a brand's likeness or identity, falsely implying the brand is engaged in or endorsing certain activities. The content may misleadingly suggest that the brand supports a controversial issue, endorses a political figure, or aligns with a specific cause, which may be reputationally damaging or entirely false. These actions can erode consumer trust, damage brand equity, and create legal liabilities, especially if the brand is portrayed in a way that contradicts its values or business principles.

Example: An individual creates an AI-generated video that features a popular celebrity endorsing a brand product. In the video, the celebrity falsely claims that the brand supports a controversial political stance, despite the brand never making such a statement. The video spreads rapidly on social media, causing public backlash. Neither the celebrity nor the brand had any involvement with the making of the video. This misrepresentation damages the brand, alienating part of its customer base and forcing the brand to conduct damage control and clarify the false claims.

Key mitigation tactics

Policies and Processes

This section focuses on the potential policies, processes and training that could be implemented to help ensure teams understand the IP risks of Gen AI in marketing and how to use the technology responsibly.

Interactive: **Roll over the mitigations below to see our risk reducing actions**

Key mitigation tactics

Contract and Supplier Management

This section focuses on how contracts and relationships with AI providers, agencies and other partners could potentially be calibrated with a view to mitigating IP risks.

Interactive: Roll over the mitigations below to see our risk reducing actions

Key mitigation tactics

Oversight and Monitoring

This section focuses on the types of tracking and oversight tools that could be adopted to monitor the use of AI tools and identify any potential IP or copyright violations.

Interactive: **Roll over the mitigations below to see our risk reducing actions**

World Federation of Advertisers
London, Brussels, Singapore, New York

wfanet.org

info@wfanet.org

+32 2 502 57 40

twitter @wfamarketers
youtube.com/wfamarketers
linkedin.com/company/wfa

Competition compliance policy

The purpose of the WFA is to represent the interests of advertisers and to act as a forum for legitimate contacts between members of the advertising industry. It is obviously the policy of the WFA that it will not be used by any company to further any anti-competitive or collusive conduct, or to engage in other activities that could violate any antitrust or competition law, regulation, rule or directives of any country or otherwise impair full and fair competition. The WFA carries out regular checks to make sure that this policy is being strictly adhered to.

As a condition of membership, members of the WFA acknowledge that their membership of the WFA is subject to the competition law rules and they agree to comply fully with those laws. Members agree that they will not use the WFA, directly or indirectly, (a) to reach or attempt to reach agreements or understandings with one or more of their competitors, (b) to obtain or attempt to obtain, or exchange or attempt to exchange, confidential or proprietary information regarding any other company other than in the context of a bona fide business or (c) to further any anti-competitive or collusive conduct, or to engage in other activities that could violate any antitrust or competition law, regulation, rule or directives of any country or otherwise.

Please note that the recommendations included in this document are merely meant as suggestions or proposals. They are not binding in any way whatsoever and members are free to depart from them.