A New Holiday Playbook: AI, Sustainability, and the Evolving Retail Landscape

Retail and Fashion
Holiday Guide 2025

Hogan Lovells

Contents

Whether you're decking the halls of a luxury boutique or managing a global e-commerce empire, this guide will help you navigate the holiday season and bring confidence into 2026.

Introduction

As the holiday season ushers in its busiest months, retailers and fashion brands are confronting a marketplace reshaped by rapid technological disruption, shifting regulatory expectations, and increasingly savvy consumers. AI has taken on roles from behind-the-scenes efficiency and design tools to a front-line driver and instrument of customer engagement, marketing and payment facilitation. At the same time, regulators across the U.S., UK, EU, and Asia are accelerating rules around retailers' use and marketing of AI tools and revisiting existing regulations around data privacy, green claims, pricing, packaging, and platform conduct.

This year's guide brings together key legal and regulatory developments shaping the retail and fashion landscape this festive season. The insights that follow highlight the trends, risks, and opportunities most relevant as retailers close out the year and look ahead to 2026.

In particular, we look at:

- **AI in the consumer journey** – agentic payments, AI marketing claims, chatbots, and GenAI in ad campaigns.
- **AI, IP, and fashion** – copyright in AI-generated designs and the latest case law on protection for functional goods.
- **Data, cookies, and privacy** – cookie enforcement, evolving AI/privacy rules, and new sensitive data restrictions.
- **Sustainability and product rules** – rules for textiles, green claims, and food labelling for plant-based and alcohol-free products.
- **Pricing and competition** – delivery fee transparency, dynamic pricing tools, and antitrust risks.
- **Online platforms and market conduct** – China's updated rules for online business activities and platform responsibilities.
- **Brand protection and emerging risks** – deepfakes, dupes, and gray market goods in a high-pressure trading season.
- **Governance, fraud, and compliance** – the UK "Failure to Prevent Fraud" offence and practical guidance on gifts and hospitality.

As the year draws to a close, this guide offers a timely overview of the legal trends affecting retailers this holiday season and into 2026.

Kelly Tubman Hardy
Consumer Sector Head,
Washington D.C.

Meryl Bernstein
Retail and Fashion
Co-Head, New York

Sahira Khwaja
Retail and Fashion
Co-Head, London

AI in Consumer Purchases: Navigating the Risks of Agentic Payments

As we head into this holiday season, one thing that has changed is who is doing the shopping: Agentic AI is emerging as a transformative force in the consumer marketplace, particularly through the rise of AI agents and introduction of agentic payments. Merchants and financial institutions are increasingly exploring how these technologies can drive innovation, improve customer experience, and streamline operations, and regulators are already beginning to take notice. This development signals a new era of greater speed, efficiency, and personalization, but it also introduces a complex web of legal and regulatory questions.

Global

What is agentic AI – and what are agentic payments?

Agentic AI refers to autonomous systems capable of making and executing decisions with minimal human oversight. This technology is starting to be used to create consumer AI agents– software programs which effectively act on a consumer's behalf as a virtual agent or assistant. While generative AI (such as chatbots and virtual assistants) is already embedded across many areas of the retail industry, agentic AI and the use of AI agents represent a more significant development. Rather than simply responding to prompts, these agents can act independently and make decisions on behalf of the consumers. For retailers, this means that this year's holiday shoppers might be algorithms rather than people.

AI agents could potentially be used to initiate, manage, and execute payments for consumers. Instead of a consumer manually browsing online for a holiday gift, they might instruct their AI agent to find the best options based on set parameters (e.g. gift recipients' interests, price, delivery time), and the agent would scan online retailers, compare prices, check availability, arrange payment, gift wrapping and delivery and then send a short summary of the action taken, including the payment and delivery details and cost.

With the recent launch of an "Agents Payments Protocol" from a global tech provider and the growing activity from major payment networks and companies, innovation in agentic commerce is gaining momentum. For instance, one leading global payments provider has recently partnered with OpenAI to enable instant checkout within the chat interface, allowing users to purchase products from online marketplaces without leaving the chat.

Key risks and considerations

While this technology holds considerable promise, it also introduces novel legal and commercial risks – particularly given that existing payment infrastructure is typically designed for human-initiated transactions. These developments raise a range of legal and regulatory challenges, including:

- **Platform access:** As AI agents begin to interact with both merchants and financial services providers autonomously, these institutions will need to consider how to securely and reliably allow third-party agents to interact with their systems. Should they provide interfaces which are open to any agent acting on behalf of a verified user, or should institutions vet and whitelist specific agent providers? How can merchants and financial institutions confidently verify the identity of an AI agent acting on behalf of a consumer? Building technological infrastructure that supports agentic payments at scale will require collaboration across legal, compliance, and technology teams, as well as engagement with regulators to help shape and respond to emerging standards.

- **Liability:** Agentic payments introduce new complexities to the application of consumer protection laws and liability more broadly. If an agent makes an unauthorized or erroneous transaction, who bears responsibility – the institution, the agent provider, or the consumer? How will critical information, such as disclosures or advice, be delivered to the customer in a way that ensures it is properly understood? Should AI agents be permitted to effectively bind consumers by entering into new legal relationships on their behalf? To navigate these risks, merchants and financial institutions should consider putting in place appropriate contractual protections that effectively clarify liability allocation.
- **Loss of customer relationship:** If consumers increasingly rely on external AI agents to manage financial decisions and execute transactions merchants risk losing direct engagement with their customers. This could lead to diminishing brand loyalty and goodwill in favor of efficiency and data-driven interactions. But it can also create opportunities for fraud, and from this perspective, cybersecurity is key. Merchants and financial institutions will have to develop methods to deal with these new risks.
- **Systemic risk:** Unlike human users, AI agents operate continuously and could be instructed to respond instantly to market signals, news events, or data anomalies, which each introduce new forms of risk. For example, if thousands – or even millions – of agents simultaneously react to a sale or the availability of a product, it could overwhelm that merchant. Merchants will simply not be prepared for this type of instant upscaling and change in risk profile. To avoid this, there may need to be limits on transactions initiated by AI agents.

These risks must be considered within the broader context of the consumer products and financial services ecosystem and the regulatory framework. While most jurisdictions have yet to specifically address risks associated with AI – let alone agentic payments – nearly all have well-established, complex regulations governing payments, from customer onboarding to transaction authorization and liability. To enable responsible innovation, lawmakers and regulators will soon need to confront the challenge of balancing innovation with robust consumer protection in this space.

John Salmon
Partner, London

Elizabeth Greaves
Senior Associate, London

From Sleigh Bells to Red Flags – Why Holiday Ads Must be Truthful about AI

'Tis the season to deck the halls – but retailers should think twice before decking them out with bold "AI-powered" claims

U.S., EU, UK

The rapid technological developments of recent years are apparent in all sectors, including the retail space. Most recently, the focus has been on artificial intelligence, where it is becoming increasingly important for companies to use AI and, where technically possible, to integrate it into their sales channels. This is not just to capitalize on the efficiencies AI can bring, but also to remain competitive in a market where consumers are drawn to AI-driven innovations.

Internally, retailers have become increasingly reliant upon AI to manage inventory, increase efficiencies, and manage customer support (among other applications). Externally, retailers promote the benefits of automation and AI in their advertising. But as the holiday season approaches, retailers should be mindful of "AI washing," or Santa may deliver regulatory fines instead of presents.

What is AI washing?

Similar to "greenwashing," which refers to misleading or inaccurate advertising in the context of environmental claims, "AI washing" relates to misleading or inaccurate marketing claims for products or services involving AI.

AI washing means that companies present themselves or their products as more advanced than they actually are, with respect to the development, application, or incorporation of AI into their products. This practice is primarily used to win new customers, who are increasingly focused on whether a product or service is "AI-enabled", and it comes with legal risks.

Legislative background – UK and EU

Under UK and EU law (and its national implementations), AI washing is considered a misleading commercial practice within the meaning of, respectively, Regulation 226/7 of the UK Digital Markets, Competition and Consumers Act 2024 and Article 6 of the EU Unfair Commercial Practices Directive (Directive 2005/29/EC). Under these regulations, anyone who engages in misleading commercial practice, which is likely to cause consumers to make a commercial or transactional decision that they would not otherwise have made, is acting unfairly. A commercial practice is misleading if it contains false information or misleading facts that are likely to be decisive, or if it omits material information about a product. In the context of AI, this could be that advertising material with respect to a product or service implies that AI (or a particular type of AI) is used when it isn't, or which exaggerates the capability of the product or service by overstating its AI capabilities.

The key question is whether the average consumer would be misled by the marketing claim. In general, if advertisement for a product relates to AI, the consumer is expecting a product or services that does "more," or does it "better," than a product without AI.

Regulatory framework – U.S.

In the United States, various government agencies have acted in recent years to ensure that claims made to the public around the use and benefits of AI technology are accurate and substantiated, consistent with consumer protection and other applicable U.S. laws.

In September 2024, the U.S. Federal Trade Commission ("FTC") announced a law enforcement initiative aimed

at AI washing called "Operation AI Comply." The FTC brought cases against various companies claiming to sell certain AI-based services or using AI tools to mislead consumers. The FTC made clear that using AI to deceive consumers constitutes an unfair trade practice enforceable by the FTC under Section 5 of the FTC Act. In addition, the U.S. Securities and Exchange Commission ("SEC") has taken enforcement actions against investment advisors relating to allegedly false statements around the use of AI, and the U.S. Department of Justice ("DOJ") has brought criminal charges around AI investment fraud schemes involving false or exaggerated claims around AI technology.

AI marketing claims – naughty or nice?

To stay off Santa's "naughty" list this holiday season, there are a number of practical steps that retailers can take:

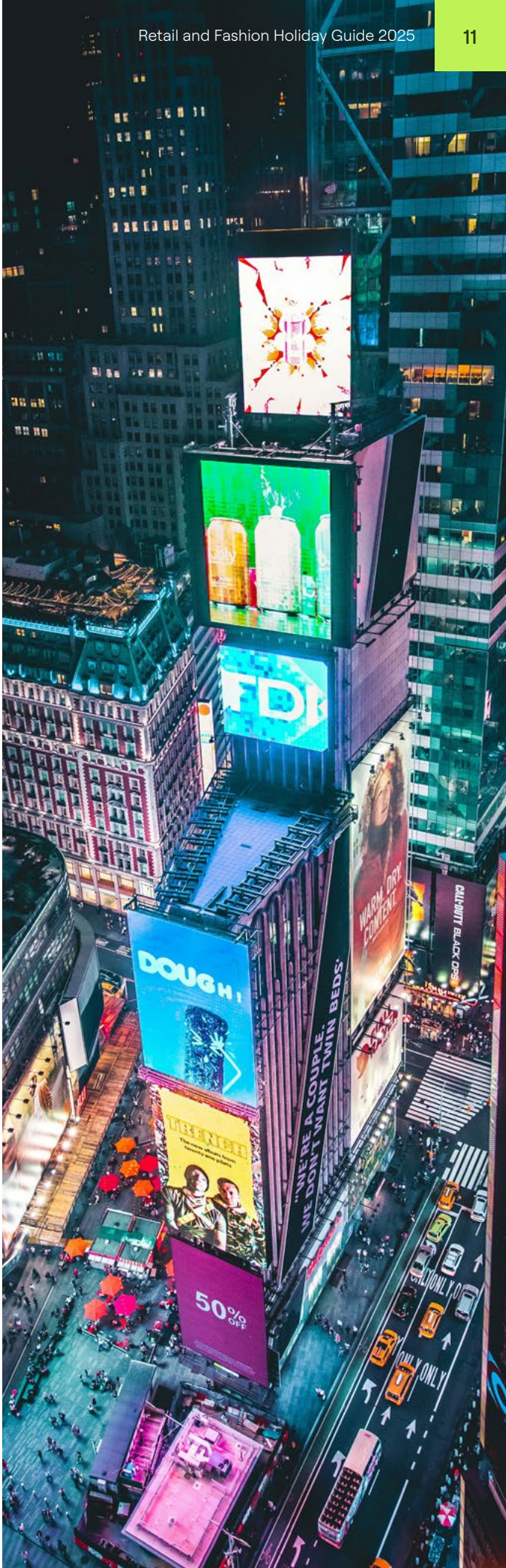
- In your advertising, only include accurate claims which can be substantiated through documented due diligence.
- Avoid using vague or generalized language, particularly when promoting how a technology performs (where such performance is being marketed as improved via use of AI).
- Think about how your claim will be perceived by consumers. Before using the terms "AI" or "AI-powered" (or similar), consider whether the consumer's experience of that product will align with such consumer's expectations.
- Keep up-to-date with applicable regulations and recent enforcement actions brought by the FTC, DOJ, and SEC.

By following these steps, retailers can avoid allowing "AI washing" to turn their marketing magic into regulatory coal. Be clear and truthful, and may your holiday campaigns deliver goodwill to customers – not headaches from regulators.

Meryl Bernstein
Partner, New York

Jennifer Crust
Senior Associate, London

Dr. Theresa Hager
Associate, Munich



Season of Discovery: How AI Chatbots Shape Consumer Choices

As the year draws to a close and holiday shopping takes center stage, consumer behavior is evolving in ways that matter for brands. AI chatbots are increasingly shaping how people discover products and make purchasing decisions—bringing new legal considerations for brands into play. Instead of relying on traditional search engines, users are turning to AI tools for direct recommendations, asking questions like "What's the best ice cream shop nearby?" or "Which sneakers go best with a new outfit?"

EU

Whether and how a company's products appear in these AI responses depends on several factors, some of which businesses can influence.

While much of the relevant information stems from the training data used to develop the underlying AI model, many chatbots now integrate live internet search functions. This means that an AI chatbot may use current content from the web to answer a user question.

If consumer brands find that their products or services are mentioned less often than expected or do not stand out sufficiently from their competitors' offerings, they may analyze the underlying sources the chatbot draws from, such as company websites, blog posts, or product information. Subsequently, targeted attempts are made to optimize this content in order to achieve a better rating for future enquiries.

The line between optimization and manipulation

The central question is where to draw the line between targeted optimization of AI responses and unacceptable surreptitious advertising. After all, users expect neutral recommendations. However, case law in most jurisdictions has already clarified in the context of search engines that technical or editorial optimizations of websites—for example, to improve findability or higher placement in search lists—are not misleading. The same will likely apply to chatbots in most jurisdictions. Therefore, every effort should be made to provide structured content on the website that is optimized for AI chatbots. This includes, among other things, FAQ pages, product comparisons, and knowledge graph-compatible data.

However, the legal assessment would likely be different if companies deliberately place false or exaggerated claims on their websites, e.g., in a hidden form visible only to web crawlers but not to human visitors, in order to manipulate AI responses. For example, a company might falsely claim that a certain product was an "award winner" solely to influence a chatbot's output.

Managing brand mentions and trademark risks

Problems can arise if the chatbots name the brand incorrectly. AI chatbots can, of course, mention brand names in their responses. However, problems arise when AI chatbot responses lead to confusion between brands.

In some jurisdictions, trademark law allows brand owners to request clarification when a mark is used generically by third parties. According to the wording of some trademark acts, this rule applies only to dictionaries and other reference works. It is not yet clear whether future legislation or case law will extend this protection to AI chatbots.

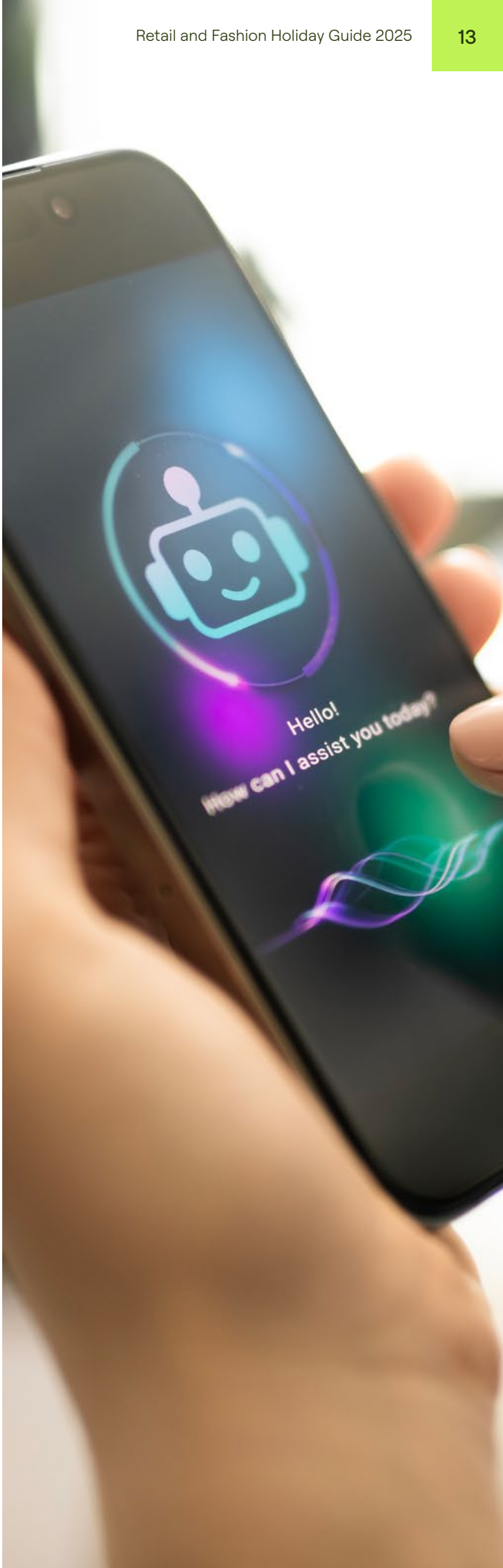
Recommendations and best practices

Companies should keep an eye on the extent to which their own brands appear in the responses of popular AI chatbots during this busy holiday shopping season. If the average visibility in AI responses is insufficient, legally permissible measures should be taken to promote the relevant brands, bearing in mind customers' increasing adoption of AI chatbots. At the same time, appropriate measures should also be taken to ensure that relevant brands are not used by AI chatbots in a way that could cause customer confusion or trademark dilution. By combining sound legal strategy with responsible digital practices, companies can leverage AI's reach while maintaining compliance and protecting brand integrity.

Dr. Burkhart Goebel
Partner, Hamburg, Madrid

Nico Kuhlmann
Senior Associate, Hamburg

Johannes Großekettler
Senior Associate, Hamburg



Embracing GenAI to Execute Ad Campaigns – But at What Cost?

As holiday ads abound and companies look to utilize artificial intelligence to create and enhance their marketing campaigns, questions arise as to the impact of that use of the protectability of the resulting materials. From twirling dreidels to dancing trees, is your AI-generated advertising a protectable holiday miracle, or a Grinch-like trick subject to unrestricting copying and use by competitors?

U.S.

Renowned computer scientist Fei-Fei Li once said, "Artificial intelligence is not a substitute for human intelligence; it is a tool to amplify human creativity and ingenuity." Recent guidance issued by the United States Copyright Office tends to agree – upholding the principle that only human-created works are eligible for copyright protection and carefully delineating the protectability of works created entirely by, or with the assistance of, artificial intelligence with varying degrees of human oversight.[1] This guidance, issued in January 2025, carries significant implications for marketing and advertising professionals who use artificial intelligence (AI) in the creation and development of brand campaigns.

Retail companies are increasingly using generative AI (GenAI) tools to reduce the cost of brand campaigns. For example, a company may decide to use an AI-generated model as the "face" of its campaign rather than spend a significant portion of its creative budget on hiring a real-life model or celebrity for its advertisement or commercial. Another company may decide to save costs by taking campaign photos in an inexpensive, nearby location and using GenAI to replace the background with a more scenic, exotic view. Yet another company may input a prompt into the GenAI tool of its choice, such as "Explain the benefits of using a cruelty-free makeup formulation, using a catchy slogan" and use the output in its ad copy. While these are all innovative ways to use GenAI, they could potentially leave companies without an avenue to protect these creative works which are generated by the GenAI tool under copyright law, hampering their ability to stop others from imitating them.

U.S. copyright law - the human authorship requirement

Under U.S. copyright law, copyright protection is only extended to "original works of authorship."[2] Although the Copyright Act does not explicitly define who (or what) can be considered an "author," U.S. courts to date have interpreted this statute to require human authorship, refusing to extend copyright protection to nonhuman authors (like a monkey taking selfie photographs, infamously).

In March 2025, the U.S. Court of Appeals for the D.C. Circuit upheld a federal district court ruling that an AI system could not be considered the "author" of a work for copyright purposes. [3]There, although a (human) computer scientist created the AI system which ultimately generated the subject artwork ("A Recent Entrance to Paradise"), the U.S. Copyright Office (USCO) rejected his copyright application on grounds that the work was ultimately created by the AI system, and not the scientist himself. This follows the USCO's January 2025 report, Copyright and Artificial Intelligence, *Part 2: Copyrightability,* which issued guidance regarding the

1 United States Copyright Office, *Copyright and Artificial Intelligence, Part 2: Copyrightability* (January 2025), available here.
2 17 U.S.C. § 102(a).

copyrightability of works incorporating AI elements. This guidance is helpful for companies seeking to balance the cost savings and efficiency of using GenAI in brand campaigns, with the desire to obtain legal protection over the creative fruits of labor.

First, the USCO clarified that "AI-assisted works" are eligible for copyright protection. These are works that use AI to assist or enhance human expression, rather than to substitute for the expression itself. Examples of AI assistance include using GenAI to brainstorm campaign ideas, create written outlines to assist with building a script, or even synthesize voice for digital music to be incorporated into the ad.

On the other hand, the USCO clarified that guiding AI output using prompts does not meet the threshold creativity requirement for copyright protection. The USCO determined that these prompts function as "instructions" that convey unprotectable ideas. Because AI models operate unpredictably, even detailed prompts do not give the prompter sufficient control over the resulting output to claim authorship.

Impact (or lack thereof) on preexisting copyrights

Importantly, AI does not destroy preexisting copyrights and may confer even further protection. When a human's own copyrightable work is input into a GenAI tool, and that work is perceptible in output (such as the earlier example of replacing the background in a campaign photo, where the other elements of the photo – the actor, props, theme – all remain), the human is entitled to copyright protection, including in the GenAI output, of "at least" the original creative expression encompassed by the input. The USCO may also consider the protectability of compilations of human-authored and AI-generated material, if sufficient creativity is exercised in the selection, coordination, and arrangement of elements of the work.

Finally, if a company makes meaningful modifications to GenAI output, those modifications may themselves be eligible for copyright protection, depending on the nature and extent of the modifications. For example, certain GenAI tools give users control over "the selection and placement of individual creative elements," such as the Midjourney tool allowing users to select and regenerate regions of an AI-generated image with a modified prompt. There is some ambiguity as to how this differs from prompt engineering, which the USCO does not consider protectable copyright material.

Given these positions taken by the USCO in its report, companies are well advised to consider the following best practices for developing marketing and advertising materials with the use of GenAI:

- Where possible, AI should be used as an assistive rather than creative tool, i.e., for purposes of brainstorming or outlining what will ultimately be a human-created work.
- For works that are themselves created using AI, material and creative modifications to those works should be maximized and documented.
- When available, the company's own human-authored work should be used as an input into the GenAI tool, potentially allowing the user to claim compilation rights in the resulting AI-generated output.

Ultimately, whether a work developed with the use of GenAI has sufficient human authorship to be protected under copyright law is a case-by-case determination, depending on the specific purpose and use of the AI tool at hand, but companies can maximize the likelihood – and extent – of available protection by making strategic use of this exciting technology.


Lauren Cury
Partner, Washington, D.C.


Brendan Quinn
Senior Associate, Washington, D.C.


Hadley Dreibelbis
Associate, Washington, D.C.

3 *Thaler v. Perlmutter,* 2025 WL 839178, No. 23-5233 (D.C. Cir. Mar. 18, 2025).

Unwrapping Ownership: Copyright in AI-Generated Fashion

Over the past few years, generative AI has advanced at breakneck speed, and retailers—especially in the fashion industry—are increasingly exploring generative AI for product design and marketing. From rough concept and illustrations to choosing a garment that fits the visualisation that the designer has in mind, fashion designers make numerous creative choices in the process of creating works of fashion. With the holiday season upon us, being armed with AI is no doubt important for productivity. But who owns the copyright in the outputs of generative AI in works of fashion?

UK & APAC

In the UK and Hong Kong, the requirement of originality for copyright subsistence can pose a challenge when AI is used in the creation of a work of fashion, or indeed in any work. It is arguably satisfied where a human contributes sufficiently to a work generated by a computer such that it is a result of their free and creative choices, choices which cannot be made with AI alone. However, in the context of generative AI models, there is a risk that the user will only contribute a general and non-specific idea of what is expected as the AI output, and consequently not contribute sufficiently to the expression of the work to be considered its author. The threshold might, however, be satisfied specifically instructs AI through detailed prompts, reflective of the designers own creativity and knowledge, such that the AI model becomes more similar to an assistive tool in the creative process of the prompt-giver, akin to having a pen for an illustration.

In cases of works where the prompts are general and there is no identifiable human author, these are arguably considered computer-generated works under UK and Hong Kong copyright legislation, and the author is *"taken to be the person by whom the arrangements necessary for the creation of the work are undertaken* Is this person the user giving the prompts or the AI programmer? In 2006, a UK court applied the computer-generated work provision to determine that the copyright in a screenshot taken of a computer game was owned by the computer programmer, rather than the user who took the screenshot of the game. However, this decision is not easily applicable to generative AI.

Practical implications

Pending legislative amendments, official guidance or case law which provide certainty regarding the copyright ownership of AI-generated works, good governance of AI use in retail and fashion requires a multifaceted approach as suggested below:

1. Identify, evaluate and regularly audit the terms of AI tools regarding copyright ownership to the generated output.
2. Keep records of inputs made to AI tools in creative processes to show human contribution.
3. Establish guidelines or a business policy on the use of AI.
4. Regularly communicate AI guidelines and policies to employees and train employees on best practices to achieve copyright protection.
5. Establish a steering committee responsible for AI tool implementation to allow your retail business to oversee AI use and respond to developments quickly.

PJ Kaur
Counsel, Hong Kong

Grace Gladdle
Senior Associate, London

A Bright (and Compliant) Holiday Ahead: Navigating AI and Privacy Updates

As retailers and brands gear up for the holiday rush, many are leaning more heavily on AI-powered tools to personalize marketing, streamline operations, and support customer engagement during the busiest shopping season of the year. But while AI is adding sparkle to everything from festive ad campaigns to automated customer service, the regulatory landscape governing these technologies has been evolving just as quickly. What once felt like a race to keep up with innovation has shifted, with governments and industry bodies now rapidly advancing standards and rules that companies must navigate.

U.S. & EU

This season, businesses using AI should ensure their practices align with the latest legal and industry expectations across the markets in which they operate. The holidays may be a time of celebration, but they also present heightened scrutiny and heightened risks, making it more important than ever for retailers and consumer brands to understand how AI and data privacy obligations are changing and what steps they need to take now to stay compliant.

Ongoing engagement by regulatory bodies

In 2025, the European Union's AI Act entered its phased implementation, which includes a tiered risk-based framework that establishes different categories of regulatory requirements for AI systems depending on their risk profile. For example, as of February 2025, certain AI systems are classified as "Prohibited" due to unacceptable risk levels—such as AI systems for social scoring. Aside from these outright bans on unacceptably risky AI systems, the tiered risk structure permits the use of AI in certain "high risk" areas like infrastructure (such as supplying electricity or other utilities), but sets out strict obligations for AI use, with full compliance expected by 2027. Other lower risk categories of AI systems, such as chatbots, will be subject to transparency requirements—for example, systems that interact directly with individuals will need to be designed and developed so users understand they are interacting with an AI system, if that is not obvious based on the circumstances and context of use. Companies doing business in the EU should take note of these existing and upcoming compliance obligations and ensure they are on target for timely compliance.

Industries are also self-regulating and establishing best practices for the use of AI. For example, in January 2025 the Institute of Electrical and Electronics Engineers (IEEE) published its "Standard for Algorithmic Bias Considerations" (IEE 7003-2024) with the goal of mitigating the risk of unintended bias in algorithmic systems and promoting transparent documentation and communications to stakeholders regarding the purpose, use, and limitations of AI systems. These industry standards are likely to continue evolving across all categories—and if past practices hold true, government regulators will likely take guidance from industry standards in setting and revising their own regulatory requirements.

Privacy statements and transparency

Against the backdrop of this changing regulatory environment, organizations are increasingly expected to provide clear disclosures about not only data collection and usage, but also how they use AI systems. This shift toward transparency into AI-driven processes and applicable guardrails, as emphasized in the World Economic Forum's September 2025 Insight Report, may prompt companies to consider updating their privacy policies to include sections describing the logic and potential impacts of automated decision-making.

Third-party risk and vendor accountability

Likewise, the proliferation of generative AI tools has introduced new complexities in third-party risk management. Vendors that offer AI-as-a-service—or employ AI on an ancillary basis while performing their core services—may use customer data to train models, raising concerns about data ownership and confidentiality. This has significant potential privacy implications, particularly if vendors have access to sensitive data. Accordingly, companies should carefully review the policies and practices of potential new vendors and should periodically review existing vendor relationships to assess these risks. Business can also take advantage of key opportunities during routine audits and contract renewal periods to assess vendor compliance and update written contracts with provisions to proactively mitigate these risks.

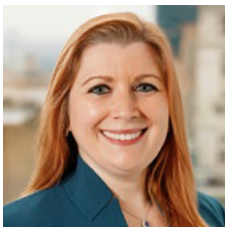
Careful oversight is key

Finally, it bears repeating in every discussion of generative AI: human oversight is crucial to using AI effectively and minimizing risk. Indeed, some attorneys have learned this lesson the hard way—numerous courts have imposed sanctions this year on counsel who submitted court documents with "hallucinated" quotations and citations that were originally generated by AI and not verified by counsel. In some cases, the attorneys even repeated similar errors in their "corrected" filings, indicating systemic deficiencies in their approach to using AI tools. These egregious, headline-grabbing errors are easily avoidable with careful oversight and verification of AI-generated content, and lack of oversight by an opponent should not be overlooked as a potential strategic advantage. Given the salience of this issue in the legal community right now, companies involved in litigation should carefully review all opposing counsel's work for potential AI-generated errors and promptly raise them to the court, if found.

Looking ahead

As AI capabilities continue to advance, so too must the frameworks that govern their use. As regulatory frameworks and industry standards continue to evolve, organizations should anticipate further updates to compliance obligations and best practices in 2026 and beyond. Proactive engagement with legal, compliance, and technical stakeholders is essential to navigating the complex intersection of AI and data privacy, adapting to changes, and maintaining responsible AI governance. Most importantly, continuous human oversight, including advice from industry and legal experts, can help organizations to continue harnessing the benefits of AI while protecting the interests of their clients, employees, and stakeholders.

Jasmeet Ahuja
Partner, New York, Philadelphia



Kate Mancuso
Senior Associate, Philadelphia

Cookie Consent: The Ghost of Christmas Past (and Present)

Cookie consent might feel like a tale as old as time, but regulators across Europe and the UK are still keeping a close eye, proving that this ghost isn't going away anytime soon.

EU & UK

In the EU, the Dutch Data Protection Authority (DPA) has been particularly active, scrutinising non-compliant cookie banners and inadequate consent mechanisms. Since April 2025, the Dutch DPA has issued over 200 warnings, with roughly 25% of non-compliant companies facing enforcement if they continue to fail to update their practices. The DPA will continue its monitoring activities in 2026. The message is clear: intrusive cookies cannot be placed before consent is given, and users must have a genuine choice. "Accept" and "reject" options must be equally accessible, and consent cannot be bundled or implied. This aligns with broader EU trends, where authorities are increasingly intolerant of dark patterns and pre-ticked boxes.

Across the Channel, the UK Information Commissioner's Office (ICO) has also ramped up scrutiny. Following its call to action for the UK's top 100 websites, the ICO contacted 1,000 sites to assess whether they are giving users meaningful choices about advertising cookies. The new Data (Use and Access) Act raises the stakes further, aligning cookie fines with UK GDPR levels (up to £17.5 million or 4% of global turnover). Helpfully, the Act will ease the compliance burden in the UK somewhat by classifying a broader range of cookies as outside of the requirements to obtain consent, including those used for fraud, security, and certain analytics purposes.

Our festive tip? While cookie consent compliance may feel like yesterday's news, this issue is far from resolved. Brands that prioritise user trust and clear and simple consent will stay off regulators' naughty lists and make the most of the holiday season.

Katie McMullan
Counsel, London

Chantal van Dam
Counsel, Amsterdam


fn
control
option
command

Sensitive Data, High Stakes: New U.S. Rule Impacts Global Retail Transactions

Global retailers face substantial challenges this holiday season given sweeping new U.S. restrictions on cross-border data flows.

U.S.

In April of 2025, the U.S. Department of Justice (DOJ) final rule—Preventing Access to *U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons*—took effect. The rule imposes substantial restrictions on U.S. entities that provide certain foreign individuals or legal entities with access (including the ability to access) American government-related data or bulk sensitive personal data related to U.S. individuals. The rule reflects the increasing recognition by the U.S. government that foreign access to data may create national security concerns, particularly where recipients of data have ties to China (including Hong Kong and Macau), Cuba, Russia, North Korea, Iran, or Venezuela.

The rule prohibits or substantially restricts certain data transactions involving entities with certain ties to those countries, including transactions that involve providing access to demographic data, device identifiers, government identifiers, financial account information, advertising IDs, account credentials, IP addresses, biometrics, and precise geolocation data, along with certain other sensitive data. And some transactions—such as employment agreements, vendor agreements, and investment arrangements—may be restricted, requiring the implementation of security requirements.

The net effect of the rule is that U.S. organizations engaging in transactions where foreign persons may access bulk U.S. sensitive personal data must assess whether they are subject to robust due diligence, auditing, and reporting obligations.

As retailers seek to comply with the rule, they will need to assess:

- global data flows to determine whether their data transfers may be prohibited or restricted;
- existing compliance programs to identify how to update or supplement existing documentation to comply with new requirements;
- security controls to confirm the right security controls are in place; and
- existing processes for managing the complex contractual and reporting obligations set forth under the DOJ's new regime.

W. James Denvil
Partner, Washington, D.C.

Alyssa Golay
Senior Associate, Washington, D.C.

Deepfakes in Fashion and Retail: Navigating the New Legal Landscape

As the holiday season approaches and brands launch their most imaginative festive campaigns, deepfakes – AI-generated or AI-manipulated images or audio-visual content – are drawing increasing attention. While AI-driven models and immersive virtual try-ons unlock bold creative possibilities, they also introduce new legal considerations for fashion and retail.

EU, Italy

Deepfakes touch on personality rights, copyright, data protection, and—in some jurisdictions, such as Italy— (even) criminal law. Using a person's likeness or voice without consent may infringe personality rights, and AI-generated content based on real individuals requires careful handling of personal data. Copyright issues may also arise when deepfake tools rely on or alter existing creative works, making licensing essential. A newly introduced criminal offence in Italy further strengthens protection by penalizing the non-consensual dissemination of deepfakes capable of causing unjust harm. At the regulatory level, the EU AI Act imposes transparency obligations: professionals must clearly disclose when content has been generated or manipulated by AI, helping ensure that consumers are not misled.

Despite the challenges, deepfakes also offer remarkable opportunities. In this evolving landscape, fashion and retail leaders must balance creativity with responsibility. By prioritizing ethical practices and clear communication, industry can harness deepfake technology to inspire and engage, while safeguarding rights and building lasting consumer confidence.

Used ethically and transparently, AI-generated imagery offers brands an opportunity to innovate while reinforcing consumer trust—an especially valuable combination during the festive season.

Maria Luigia Franceschelli
Counsel, Milan

Dreaming of a Green(?) Christmas: The EU's Push for Sustainable Fashion

It's time to get out the Christmas jumpers again, but how long do we really wear them – a few weeks of the year before buying a new one? The EU is launching legislation aimed at reducing the environmental impacts associated with our beloved Christmas jumpers (and other fast-fashion).

EU

The Eco-design for Sustainable Products Regulation ("ESPR"), in force since July 2024, aims to make sustainable products the new EU norm. It establishes several requirements to improve the circularity, energy performance, recyclability, and durability of almost any physical product placed on the EU market. For textiles, the key measure include:

- **Digital Product Passports (DPPs):** A mandatory digital ID tracking a product's composition, repairability, origin, and environmental impact throughout its lifecycle. For textile products, DPPs will likely be mandatory by mid-2028.
- **A ban on the destruction of unsold textiles and footwear:** The ESPR restricts premature obsolescence. For textiles like clothing and footwear, this effectively acts as a ban on the destruction of any unsold consumer goods.
- **Potential product design changes:** In-scope products will need to meet eco-design criteria (e.g., durability, reparability, recyclability, energy-resource efficiency).

In addition, the EU is also introducing Extended Producer Responsibility ("EPR") under the revised Waste Framework Directive ("rWFD"). EPR will mean companies that first place textiles on the EU market will be responsible for their end-of-life management: collection, sorting, recycling, and consumer awareness campaigns. To meet these obligations, they will have to register in each Member State where they sell textiles and appoint Producer Responsibility Organizations ("PROs"). Fees to be paid to PROs will be linked to eco-design quality - meaning meeting these obligations for a simple wool jumper would likely incur lower costs than one decorated with bells and flashing lights!

Compliance will not be easy:

- **Significant investment** will be required to develop and maintain DPP systems, redesign products, adapt production lines, and prevent the destruction of unsold consumer goods.
- DPP-related data may expose unsustainable practices, **requiring remedial measures.**
- In-house legal and compliance teams will need to **continuously track** operation of the ESPR in practice.

Compliance will however be worth it, not least to avoid regulatory penalties, but also to increase consumer trust and competitive advantage, with sustainability becoming a major purchasing driver for consumers everywhere.

So don't be a Scrooge and give the gift of sustainable products this holiday season!

Valerie Kenyon
Partner, London

Christiane Alpers
Partner, Hamburg, Berlin

Vicki Kooner
Senior Associate, London

Eshana Subherwal
Senior Associate, London

Magdalena Bakowska
Senior Associate, London

Hanns-Thilo von Spankeren
Associate, Hamburg

The Price of Failure to Prevent Fraud: Why Retail and Fashion Businesses Need to Act Now

The new corporate Failure to Prevent Fraud (FtPF) offense, in force from September 2025, marks a significant tightening of the UK's corporate crime framework. For retail and fashion businesses—defined by rapid product cycles, extensive third-party networks and intense seasonal trading—the exposure is immediate. The law applies to all large organizations irrespective of where in the world they are incorporated. For a prosecution before the UK courts, all that is required is the commission of a fraud offense with a UK nexus, meaning global brands selling into the UK remain firmly in scope. No retailer can hang its stocking elsewhere and assume liability stops at an overseas head office.

UK

Liability arises where an associated person (i.e. an employee, agent, subsidiary, or any other person performing services for or on behalf of an organisation) commits fraud intending to benefit that organization. In this sector, that group extends well beyond employees. Marketing agencies preparing ESG claims, franchisees driving local sales, freight forwarders handling customs paperwork, and distributors promoting products can all be caught. Seasonal pressure can increase the risk of corners being cut as quickly as a customer dashing through the stores on Christmas Eve.

Examples relevant to retail and fashion include:

- Sustainability and marketing claims: A creative agency "adds extra sparkle" to environmental claims to boost festive sales.
- Sales incentives and reporting: A store manager inflates holiday-period figures to secure bonuses.
- Supply chain and logistics: A freight partner falsifies customs declarations to keep Christmas stock moving.
- Procurement and sourcing: A buying agent conceals quality failures or misrepresents test results to keep seasonal lines on shelves.

So how do those in the sector avoid the *naughty* list and demonstrate that they have in place reasonable procedures to prevent misconduct? Practical actions for brands include:

- Map associated persons across franchise, distribution, logistics, and marketing chains.
- Stress-test product claims, influencer activity, and promotional campaigns.
- Reinforce targeted training for buying, logistics, marketing, and store teams.
- Strengthen governance around sustainability messaging
  and seasonal sales so fraud risks do not snowball.

UK law enforcement authorities have promised to "go hunting" using these new powers. So, you'd better watch out, you'd better not cry... preparation and the implementation of reasonable prevention measures are essential.

4 Meeting at least two of the following three criteria in the financial year preceding the year of the fraud offence: (i) Turnover of more than £36 million; (ii) Balance sheet total of more than £18 million; and/or (iii) More than 250 employees.

Olga Tocewicz
Counsel, London

Reuben Vandercruyssen
Senior Associate, London

The EU's Sustainability and Green Claims Wish List: Preparing for EU's New Rules Empowering Consumers for the Green Transition

It's that time of year again—Christmas lights sparkle, holiday shopping is in full swing, and sustainable product offers from "eco-friendly" toys to "sustainable" parfums promise presents with environmental and social benefits. Next year, the EU Empowering Consumers for the Green Transition Directive (ECGT) will notably restrict sustainability marketing and require green claims to be reliable, comparable, and verifiable.

EU

Starting September 27, 2026, the ECGT Directive introduces strict rules for all consumer-facing marketing practices—advertising, product labelling, and online communication. The new rules aim to combat greenwashing, prevent early obsolescence, and empower consumers to make informed sustainable choices. Green claims shall be more than just shiny wrapping.

Key takeaways for consumers businesses:

Substantiation is a must-have: Vague claims such as "green" or "sustainable" must be substantiated on the same medium (e.g., on the product packaging).

- **No more self-certification:** Self-certified sustainability labels are banned. Only sustainability labels based on third-party verified certification schemes or established by a public authority are permitted.
- **Offsetting is out:** CO_2 and climate claims based on offsetting emissions are prohibited.
- **Future promises:** Forward-looking claims (like "climate-neutral by 2050") must be supported by clear, objective, and publicly available commitments. Such claims require a detailed and realistic implementation plan with measurable, time-bound targets, verified by an independent third-party expert.
- **Product features:** Environmental benefits must go beyond legal requirements. Compliance with mandatory rules (like recyclable packaging) cannot be marketed as a unique selling point.
- **Comparisons:** Sustainability comparisons must disclose methodology, products, suppliers, and update measures.
- **Mandatory information:** Consumers must be provided with information on statutory warranty rights and voluntary commercial durability guarantees in harmonized formats.
- **Don'ts:** Misleading claims about durability, repairability, or irrelevant benefits are banned. Early obsolescence tactics (such as features designed to shorten a product's lifespan) are also prohibited.

Companies should review and update product descriptions, labels, packaging, and advertising in due course. The clock is ticking – the new rules will be in full force by the next Christmas holiday season.

Christiane Alpers
Partner, Hamburg, Berlin

Cynthia Staiger
Associate, Berlin, Hamburg

Copyright Protection for Fashion Goods: How the Latest Birkenstock Case Showcases the Solid Copyright Protection Doctrine for Functional Goods in the Netherlands (Even When Foreign Courts Rule Otherwise)

The Netherlands is known for its generous approach to copyright, and the recent Birkenstock case proves it once again. On 12 November 2025, the District Court of Midden-Nederland (located in Utrecht, the Netherlands) ruled in favour of Birkenstock in a copyright dispute against retail chain Scapino. In this case, Birkenstock claimed copyright protection for its "Madrid," "Arizona," "Florida," "Boston," and "Gizeh" models. For three of these ('Madrid', 'Arizona' and 'Florida'), the Court granted copyright protection.

Illustration from District Court of Midden-Nederland 12 November 2025, ECLI:NL:RBMNE:2025:5837

Netherlands, Germany, EU

In the Netherlands, a decision like this one in a copyright matter isn't unusual. The Netherlands has an advantageous copyright protection doctrine for functional goods. So why is it worthwhile to highlight this decision? Because earlier this year, the German Federal Court of Justice reached the opposite conclusion in at least three cases (20/2/2025 – I ZR 16/24; 20/2/2025 – I ZR 17/24; 20/2/2025 – I ZR 18/24). This showcases that essentially the same copyright infringement case is handled differently in the different EU member states, and so it pays off to carefully consider the jurisdiction in which you enforce these rights in copyright cases. Interestingly, the German courts in these cases seemingly applied the same criterion – copyright protection requires a "personal intellectual creation" – yet interpreted it differently. The German court demanded that these objects of daily use were "artistically designed *beyond* their form," resulting in a higher threshold.

The Dutch court took a more lenient view: as long as the design reflects the creator's free choices, it deserves copyright protection.

In conclusion, the (comparatively) low threshold for copyright protection in the Netherlands means that even products with a functional purpose – for example, sandals – can enjoy copyright protection (that is, if their appearance reflects creative choices). Keeping this in mind can provide a strategic advantage for retail and fashion brands seeking to prevent copycats. Dutch law does not treat functionality as eliminating a product's creative character and copyright protectability making the Netherlands a good choice for enforcing against lookalikes.

Hot off the press: The Dutch approach is in line with a recent judgment by the CJEU, dated 4 December 2025 (in joined cases C-580/23 and C-795/23). This provides reassurance that the Dutch methodology will hold strong even in the highest EU court.

Samantha Brinkhuis
Partner, Amsterdam

Iris Toepoel
Junior Associate, Amsterdam

Clarity for Online Retailers: New Guidance from the CMA on Displaying Delivery Fees

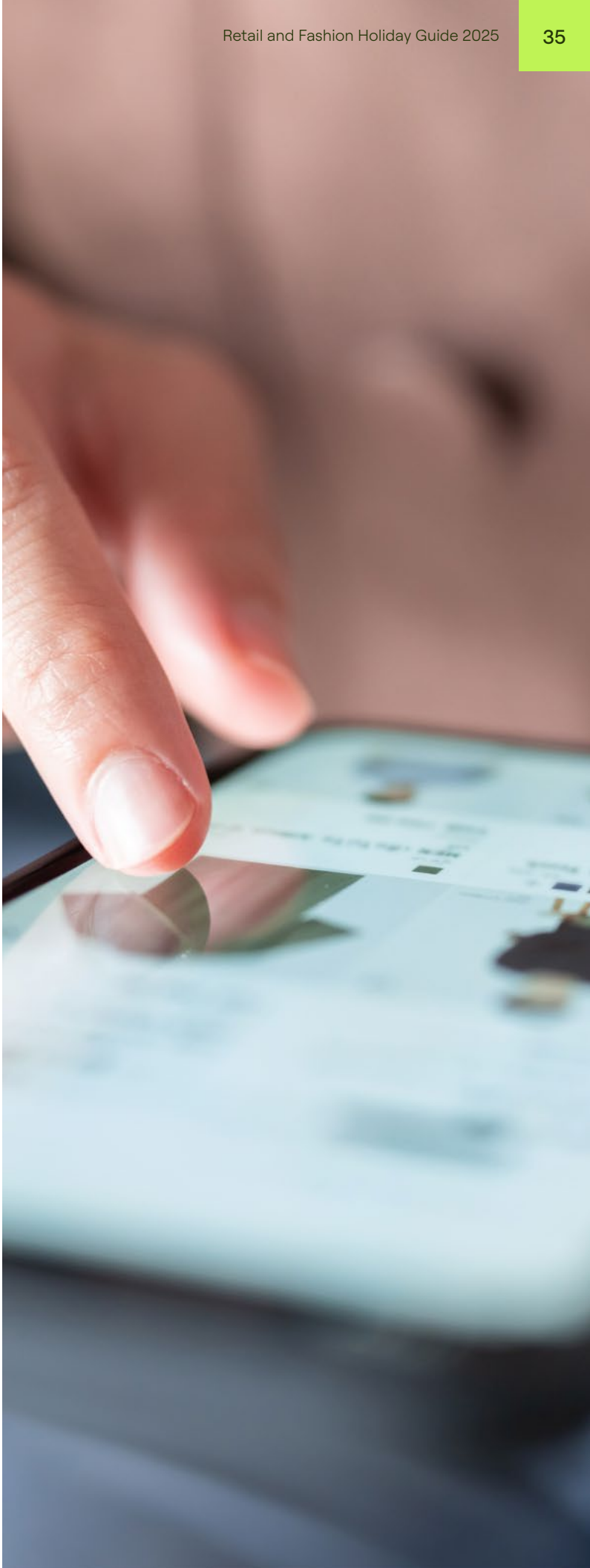
As shoppers fill their virtual baskets with holiday gifts and year-end deals, clear and upfront pricing becomes especially crucial to maintaining consumer trust. In April 2025, new consumer protection rules were introduced in the UK by the Digital Markets, Competition and Consumers Act 2024, including an express obligation on businesses to ensure that pricing displayed to consumers is inclusive of any unavoidable charges. The aim of this was to prohibit "drip pricing," which is the practice of showing a lower initial price and then disclosing additional mandatory charges later in the purchasing process.

UK

While the principle behind the new obligation seems clear—to make sure consumers know what they are paying up front—the practical application has proven challenging. A key issue for many online retailers has been how to display delivery fees, which are often applied on a per transaction, rather than per item basis. Applying the strict letter of the law, and in the absence of any guidance to the contrary, it appeared that businesses were required to add the delivery fee to the price of each item, even though this would result in the headline prices being higher than what a consumer would actually be charged if the consumer purchased more than one item.

Thankfully, in November the Competition and Markets Authority (CMA) published its finalized price transparency guidance, which recognizes that it may not be realistic or meaningful to include the delivery fee in the headline prices on e-commerce websites and apps when multiple items can be ordered and this fee is only applied once. Rather, the guidance presents three options for complying with the drip pricing prohibition in these circumstances:

- Removing the delivery fee and incorporating the delivery cost into the base cost of the product.
- Presenting the base cost exclusive of delivery as the headline price with the total price inclusive of delivery presented below or alongside the headline price.
- Providing the product's base price and information about the delivery fee, as well as a clear and prominent rolling total which updates as consumers add products to their basket. The guidance gives the following examples:
  - A prominent "floating basket" or "sticky banner" which stays on the screen with the total price visible at all times.
  - Displaying the basket with the total price as a prominent pop-up after each product is added.
  - A dynamic "add to basket" button on the product page, confirming what the cost of adding an item to the basket will be, including any additional fees.



While this guidance provides welcome clarity for online retailers, it is likely that many businesses who want to continue charging delivery fees will need to make significant changes to the interfaces of their online stores. What's more, the publication of this guidance also means that the CMA will start enforcing against those who do not comply, having previously reassured businesses that it would not take enforcement action in relation to the more uncertain aspects of the drip pricing prohibition until the position had been clarified. As the guidance has been published shortly before the holiday season and transparent pricing appears to be a priority area for the CMA, it is likely that the CMA will begin monitoring for compliance with the guidance in the new year. Retailers with an online presence should therefore take action now to ensure their pricing practices are compliant.

Jennifer Crust
Senior Associate, London

Micaela Bostrom
Associate, London

Pricing Tools: The Hidden Risk

The retail and fashion sectors are once again in the crosshairs of European competition authorities: The European Commission recently fined three luxury fashion brands a combined €157 million for resale price maintenance (RPM).

EU

The European Commission states that these brands restricted independent retailers – both online and offline – by preventing them from deviating from recommended retail prices, capping discounts rates, and controlling and limiting sales periods. In essence, the brands strived to have their independent retailers mirror the prices and conditions of the brands' own direct sales channels.

Pricing software and AI pricing algorithms have become integral to modern retail. They deliver significant efficiency through dynamic discounts and real-time adjustments. But unchecked, they create massive compliance risks.

If you use software to enhance your pricing, or an AI agent to retaliate against retailers who are not in line with your pricing strategy, you may coordinate prices illegally. To keep your commercial strategy innovative without crossing antitrust boundaries as you gear up for the Christmas shopping season, take these four steps:

- **Demand Transparency:** Ensure your software uses lawful, transparent data sources and avoids sensitive, non-public information.
- **Strengthen Governance:** "The algorithm did it" is not a defense. Approve and monitor your pricing software and train IT and sales teams on antitrust compliance.
- **Review Contracts:** Check agreements with software providers for safeguards - such as data segregation, data-use restrictions, audit rights, and cooperation clauses for regulatory inquiries.
- **Watch Adoption Trends:** Be cautious when software is marketed as "industry standard" widely used by competitors; shared algorithms or AI can create hub-and-spoke cartels and lead to tacit collusion.

Intelligent compliance today means the only surprises are under the Christmas tree – and not in the form of an antitrust proceeding.

Dr. Elena Wiese
Partner, Dusseldorf

Dr. Julian Urban
Senior Associate, Dusseldorf

Unwrapping New Legal Firepower: China's AUCL's Expanded Arsenal for Online Business Activities

China's latest amendment to the Anti-Unfair Competition Law (AUCL), effective October 15, 2025, introduced new protections to brand owners and imposes additional obligations on online sellers and e-commerce platforms, aimed at fostering a fairer business environment on the internet.

China

For brand owners, the AUCL now explicitly protects new digital identifiers (which includes online usernames, social media handles, app names, and icons) as "distinctive signs." If these signs are reputable and their unauthorized use misleads consumers, such use is now prohibited as an act of confusion under the AUCL. This gives rights holders stronger grounds for online enforcement against infringing uses of such digital identifiers on social media and e-commerce platforms in China.

For online business sellers and business promoters, the amendment introduces a set of anti-unfair advertising measures, targeting practices such as keyword manipulation, predatory pricing (i.e. sales below cost), and fabricated reviews. The law now also bans platform manipulations by false transactions, fake reviews, or malicious returns, which are measures that can all be impactful during major shopping festivals.

For e-platforms, the amended AUCL also shifts the platforms' roles from passive hosts to more active gatekeepers by imposing proactive duties (fair-competition clauses in policies, dispute-resolution mechanisms, timely remedial actions, record-keeping, etc.) paired with increased liabilities.

Notably, the amended AUCL sets long-arm jurisdiction over the unfair competition activities that are conducted outside of China but disturb the domestic market competition order and jeopardise the legal interests of domestic business operators or consumers.


Helen Xia
Partner, Beijing


Stefaan Meuwissen
Knowledge Lawyer


Grace Guo
Counsel, Beijing

Alternative Christmas Menu: From Vegan Meat to Alcohol-free Drinks – Adapting to new EU Food Labelling Rules

The festive season is around the corner... it's time to get your Christmas menu sorted. From modern appetizers to traditional mains, sides, desserts, and drinks—plant-based and alcohol-free alternatives shake up what's served under the Christmas tree, but new rules for labeling these delicacies are knocking at the door.

EU

Recent legislative and judicial developments in the EU significantly tighten food labeling requirements, especially for plant-based meat analogues, alcohol-free drinks, and dairy alternatives. The European Parliament is moving forward to reserve terms like "steak," "burger," and "sausage" exclusively for meat products, meaning plant-based alternatives may soon need new names. At the same time, the European Court of Justice has ruled that traditional terms such as "gin" cannot be used for non-alcoholic drinks, and local courts, e.g. in Germany, take a strict approach enforcing existing restrictions against dairy alternatives like "soymilk."

Food businesses are well advised to take action to ensure that their products meet the evolving labeling rules so that they are good to go on the plate for future Christmas menus:

- Stay alert to ongoing legislative negotiations, as final rules may change before coming into force (likely not before 2028).
- Review product names and packaging for compliance with evolving EU rules – especially for plant-based or alcohol-free alternatives.
- Prepare for potential rebranding and adjustments of marketing campaigns.

Proactive compliance can help avoid legal risks and maintain consumer trust in a stricter regulatory environment so that no bitter taste remains.

Christiane Alpers
Partner, Hamburg, Berlin

How New U.S. Tariff Policies Are Increasing the Risk of Gray Market Goods

Many retailer and manufacturers are grappling with the challenges presented by recent increases in U.S. tariffs worldwide. In response, some companies have sought to diversify their supply chains and manufacturing sites. However, these decisions can introduce unintended risks including a rise in gray market goods entering the U.S. marketplace.

U.S.

Gray market goods are genuine, branded goods which are authorized by the trademark owner and first sold outside of the U.S. but are subsequently imported into and sold in the U.S. without authorization. Goods with material differences (physical and non-physical) can be enjoined from U.S. sale. Sales of gray market goods can lead to damaged customer trust, diminished goodwill, disruption of relationships with authorized U.S. distributors, and lost sales.

Here are a few proactive steps retailers can take to protect their brands and customers:

- Make sure your trademarks are registered with the U.S. Patent and Trademark Office and record your registered intellectual properties with U.S. Customs and Border Protection ("CBP").
- Provide authenticity trainings to CBP Import Specialists, which are used by CBP officers to identify and prevent infringing goods from entering the U.S. market. To learn more, click here.
- Monitor the marketplace and take appropriate enforcement action as needed.
- For retailers selling branded goods, make sure that your supply chain has adequate authorization to manufacture, import, ship and sell these goods in the U.S. market – request a brand authorization letter, license agreement, or other proof of authorized use.
- Protect your supply channels and limit your liability through contractual provisions.

Anna Kurian Shaw
Partner, Washington, D.C.

Hadley Dreibelbis
Associate, Washington, D.C.

How to Keep Dupes off Christmas Wish Lists: IP Tips

With Christmas just around the corner, consumers are on the hunt for the perfect gifts. Once seen as something quietly bought for personal use—and decidedly uncool—non-authentic copies of fashion products have rebranded themselves as "dupes" and entered the mainstream. On platforms like TikTok and Instagram, influencers openly promote where to find the best lookalikes for well-known retail and fashion clothing, bags, and shoes. For retail and fashion brands, the growing popularity of dupes brings new challenges, as the distinction between (permitted) inspiration and (infringing) imitation is often unclear.

EU & Netherlands

IP law provides various tools to combat dupes:

- **Trademarks:** Most dupes intentionally avoid using the original brand's name or logo, which complicates trademark enforcement. However, the original brand's branding likely extends into other elements that might not be registered trademarks. Registering less obvious, non-traditional brand elements may make the original brand less of a target for dupes, and also provide alternative avenues of enforcement if it is targeted.
- **Copyrights:** In some countries, the door has been opened to protecting some functional goods, such as fashion items, by copyright, if the design can be shown to be the result of free and creative choices by the designer (in other countries you would have to rely on design rights), No registration is needed, as copyright arises automatically by operation of law, providing an easy way to assert a proprietary right against a dupe in those plaintiff-friendly courts.
- **Design Rights:** When fashion goods are eligible for design protection, registering a design right provides a registered exclusive right on the appearance of its product, precisely the aspect that dupes try to imitate.
- **Platform Liability (DSA):** Under the European Digital Services Act (DSA), online platforms must act against reported dupes if the dupe infringes on IP rights. Reviewing which IP rights apply and using the reporting tools of platforms can be effective.

IP rights are essential, but creative brand strategies can also shift consumer attention back to "the real thing". Examples include influencer collabs that redirect shoppers from "dupe" searches to original products, or collabs between luxury and high-street fashion brands to make luxury fashion goods more accessible.

Curious about the best strategy to protect your brand from dupes? We're here to help!


Samantha Brinkhuis
Partner, Amsterdam


Babette Dol
Associate, Amsterdam

The Compliance Gift Guide: Navigating Festive Risks in Retail & Fashion

As the festive lights go up, so do compliance risks: the festive season is one of the busiest times of year for the retail and fashion industry and often overlaps with critical business milestones—year-end contract renewals, supplier negotiations, and performance reviews. In this context, even well-intentioned gifts can be misinterpreted as attempts to influence business decisions, increasing bribery, corruption, and reputational risks.

U.S. & UK

Across the U.S. and the UK, anti-bribery and corruption laws apply without seasonal exceptions.

- The U.S. Foreign Corrupt Practices Act (FCPA) prohibits offering anything of value to foreign officials with the intent to obtain or retain business. This means that for a gift to violate the FCPA, the giver must intend to improperly influence the government official. Items of nominal value, such as company promotional items, are not, without more, items that have resulted in enforcement action, but cases have involved single instances of large, extravagant gift-giving (such as sports cars, fur coats, and other luxury items) as well as widespread gifts of smaller items.
- The UK Bribery Act 2010 (UKBA) is often considered the strictest regime in terms of gifts and hospitality because there are no promotional expenses or de minimis exceptions and in so far as public officials are concerned, any gift could be considered a bribe even absent dishonesty. And what's more, a gift given (or received) by a senior manager of a UK company could in theory bring liability to the corporate entity under recent legal reforms concerning criminal attribution in the UK. That overlays the special offence which makes companies liable for "failing to prevent" associated persons from giving bribes (including gifts) subject to an adequate procedures defense. Bona fide gifts and hospitality are not per se illegal under English law but having good policies in place is key.

With the East and South East Asian Lunar New Year and Tet festivals following closely in early 2026, organizations must remain vigilant to ensure seasonal goodwill does not compromise integrity. The fact is that although gift giving may be customary during holiday periods, gifts are not immune to challenge.

Behind the festive cheer therefore lies a compliance challenge: how can organizations maintain strong relationships without crossing lines? To stay compliant, clear policies, transparency, and training are essential. Organizations should ensure gifts comply with the applicable corporate policy of the giver and receiver (where relevant) and local applicable law and are accurately recorded in accordance with company policy. Training should be reinforced by evaluating everyday compliance with policies and procedures, and compliance monitoring systems should specifically target gift registers, expense recovery systems and other relevant financial controls. Tone from the top in respect of integrity is also key.

Before giving or accepting a corporate gift this festive season, ask yourself:

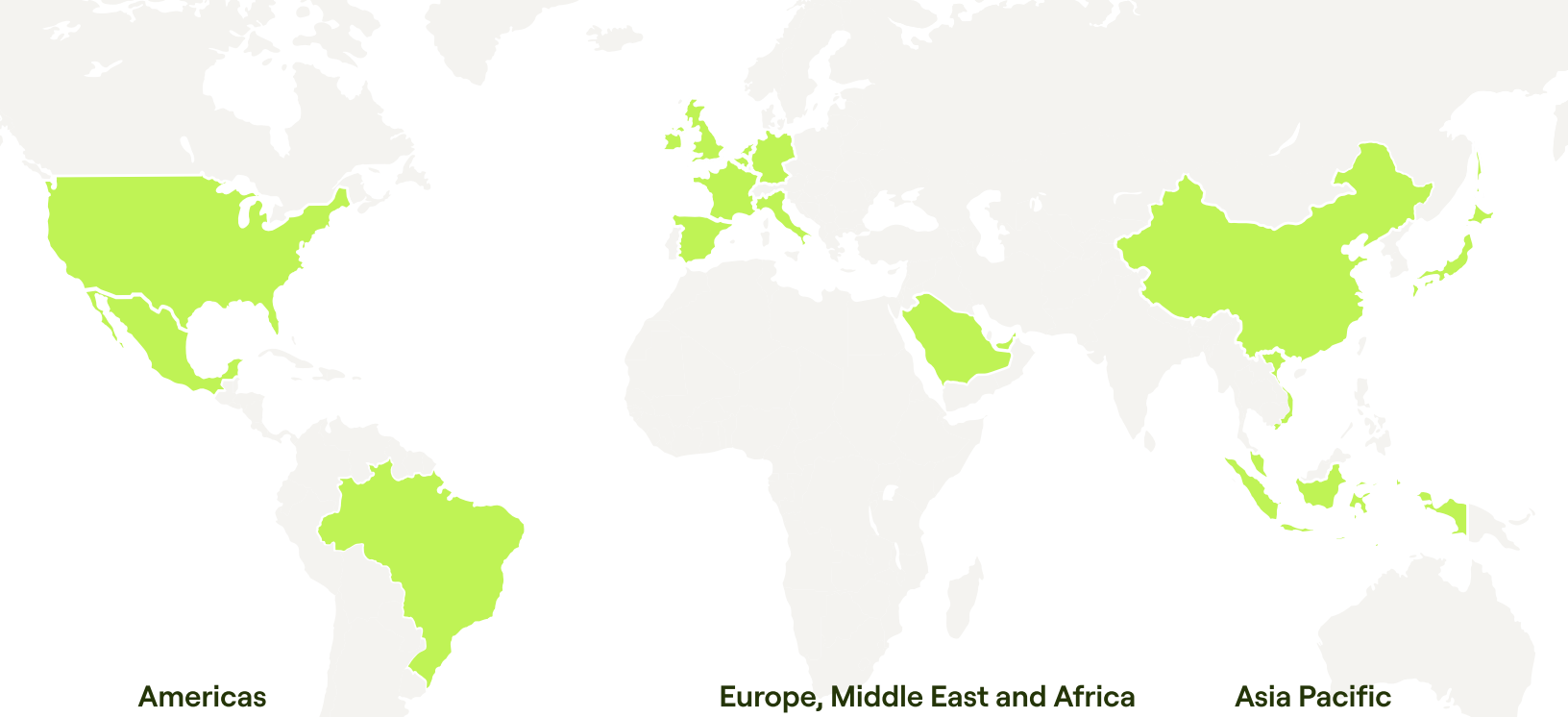
1. Is the gift permitted under the giver's corporate policy?
2. Is the gift permitted under the recipient's corporate policy?
3. Is the gift reasonable, proportionate, and transparent in the circumstances?
4. Is there any specific relevant local law that prohibits or limits the relevant gift?

Stephanie Yonekura
Partner, Los Angeles

Liam Naidoo
Partner, London

Khushaal Ved
Partner, Singapore

Catrin Norton
Associate, London



Americas

- **Boston**
- **Denver**
- **Greater Washington, D.C.**
  - Baltimore
  - Washington, D.C. and Northern Virginia
- **Houston**
- **Los Angeles**
- **Miami**
- **Minneapolis**
- **New York**
- **Philadelphia**
- **Northern California**
  - San Francisco
  - Silicon Valley
- **Latin America**
  - Brazil
  - Mexico

Europe, Middle East and Africa

- **Amsterdam**
- **Brussels**
- **Dublin**
- **Germany**
  - Berlin
  - Düsseldorf
  - Frankfurt
  - Hamburg
  - Munich
- **London**
- **Luxembourg**
- **Madrid**
- **Milan**
- **Rome**
- **Paris**
- **Middle East**
  - Dubai
  - Riyadh

Asia Pacific

- **Greater China**
  - Beijing
  - Hong Kong
  - Shanghai
- **South East Asia**
  - Ho Chi Minh City
  - Jakarta
  - Singapore
- **Tokyo**

www.hoganlovells.com