IBA/IFA 40th

ANNUAL JOINT CONFERENCE

* * * * *

40 Years of Franchise Excellence: Legal Insights, Global Trends, and Practical Compliance

* * * * *

PLENARY 2:
DIGITAL MARKETING AND LOYALTY PROGRAMS

—

May 7, 2025

Washington, D.C. U.S.A.

Alan Greenfield
Greenberg Traurig
U.S.A.

Peter Snell
Cassels Brock & Blackwell LLP
Canada

Jill Murphey
The Wendy's Company
U.S.A.

Elise Troll
Kennedy Van der Laan
The Netherlands

Benedikt Rohrssen
Company Taylor Wessing
Germany

I. Introduction

In today's digital age, marketing and customer engagement has dramatically evolved. This paper delves into the intricacies of digital marketing and the burgeoning field of digital loyalty programs. It provides insights into the latest trends, strategies, and legal considerations that are shaping the future of digital marketing across different jurisdictions worldwide, with the goal of equipping franchise law practitioners with the knowledge and tools necessary to navigate the complexities of the digital marketing landscape.

Authors:

Alan Greenfield, Greenberg Traurig, USA: Alan.Greenfield@gtlaw.com;

Peter Snell, Cassels, Canada: psnell@cassels.com;

Jill Murphey, The Wendy's Company, USA: Jill.Murphey@wendys.com;

Elise Troll, Kennedy Van der Laan, The Netherlands: Elise.Troll@kvdl.com; and

Dr. Benedikt Rohrßen, Taylor Wessing, Germany: B.Rohrssen@taylorwessing.com.

II. Digital Marketing

A. What is Digital Marketing?

Digital marketing uses traditional marketing strategies to boost sales of products and services, but on digital channels. Promoting a brand and connecting the brand to potential customers via online channels can take various forms such as search engines, website and web-based advertising, social media, email, mobile apps, text messaging and more. Using the right types and combination of digital marketing create curated experiences and engagement for customers. Franchises across various industries effectively leverage digital marketing strategies to enhance brand visibility, engage customers, and drive sales. The following are examples of digital marketing strategies:

1. Search Engine- Digital Marketing

Search engine marketing (SEM) is a digital marketing strategy aimed at increasing a website's visibility on search engine results pages (SERPs), like Google, through paid advertising. It involves purchasing ads that appear when users search for specific keywords related to a business's products or services. Amazon is a clear example of successful SEM by becoming the most visible online shopping platform.[1] According to Brightedge Research, SEM works because 68% of online experiences start with

[1] *See generally* Jungle Scout, *Consumer Trends Report Q1 2024*, Mar. 26, 2024, https://tinyurl.com/2jurnw9c.

organic and paid searches.[2] By promoting a brand at the source of most online experiences, you can attract more interested leads to your site.[3]

2. Email- Digital Marketing

Email marketing is a cost-effective marketing strategy for franchise businesses. For example, Ulta Beauty, a beauty and skincare franchise, uses email marketing to promote its loyalty program and increase customer engagement through a series of engaging emails offering exclusive discounts and rewards to its loyal customers.[4]

3. Social Media- Digital Marketing

Social media is, and continues to be, a leading marketing strategy for franchises. Advertisers spent nearly $76.4 billion on social media advertising in 2024 — a 5.6% increase from 2023.[5] As an example, Orangetheory, a fitness franchise, uses social media platforms to engage with its target audience and showcase its fitness classes and programs. Providing helpful information and encouraging members to post their own content are strategies that both increase engagement of existing customers and attract new customers.[6] Orangetheory also uses social media to run transformation challenges and offer discounts to its followers, helping increase customer engagement and loyalty.[7]

4. Content- Digital Marketing

Content digital marketing aims to educate and share value to readers instead of just promoting a product or service. It is not outwardly promotional but establishes a business as a thought leader and a trustworthy source of information. Businesses use content marketing to attract leads and convert them into loyal customers. Most marketers believe their content marketing strategies to be successful, which is not surprising when the content marketing industry is projected to be worth $107 billion by 2026.[8]

As an example, at the 2024 Sundance Festival, Hyatt kicked off a partnership with the MasterClass

---

[2] Erik Newton, *Organic Share of Traffic Increases to 53%*, BRIGHTEDGE RESEARCH, 2020, ttps://tinyurl.com/4un8tys2.
[3] *See generally Id*.
[4] *See generally* Nina Sheridan, *Ulta Beauty Marketing Strategy 2025: A Case Study*, LATTERLY.ORG, Jul. 3, 2024, https://tinyurl.com/yr2xmpdb.
[5] Oberlo, *Social Media Ad Spend in the US (2017–2028)*, https://tinyurl.com/yckmcsfp.
[6] *See, e.g.,* Orangetheory, *OTF class breakdown for all our newbies: Pick your vibe. We've got you*, INSTAGRAM, Jan. 18, 2025, https://tinyurl.com/5cdhrbcs
[7] *See, e.g.,* Orangetheory, *The Transformation Challenge is back, and this time, it's all about YOU and your reason for change! 8 weeks, 18 classes, and real results—just ask the 83% who nailed their fat loss goals or the 63% who gained muscle last year. Ready to make it happen? January 13 - March 9. Register now!*, INSTAGRAM, Dec. 29 2024, https://tinyurl.com/3jcb28er.
[8] Statista Research Department, *Content marketing revenue worldwide 2018 to 2026*, STATISTA, Dec. 10, 2024, https://tinyurl.com/4t4f8a5x.

program, focused on driving membership in the Hyatt Hotels Loyalty Program, and delivering a collection of experiences rooted in the concept of well-being and showcasing the unique attributes of hundreds of different Hyatt properties.[9] As a result, the brand experienced a 22% increase in loyalty membership year-over-year, to 51 million members.[10]

B. Use of Artificial Intelligence in Digital Marketing

Franchises are increasingly integrating Artificial Intelligence (AI) into their marketing strategies to enhance personalization, optimize advertising efforts, and improve customer engagement. Use of developed or deployed AI requires proper handling of a great deal of data and the need for foundational knowledge and technical know-how. Key applications include:

1. Personalized Customer Experiences

AI enables businesses to analyze vast amounts of customer data to deliver tailored content and recommendations. For example, Starbucks utilizes AI to provide personalized offers to customers based on their purchase history and preferences, enhancing customer loyalty and satisfaction. [11]

2. Predictive Analytics

By identifying patterns in historical data, AI can assist marketers in forecasting future trends and consumer behaviors. This capability allows companies to optimize pricing strategies, improve lead scoring, and anticipate customer needs, leading to more effective marketing campaigns.[12]

3. Content Creation and Optimization

AI-powered tools aid in generating and refining marketing content. Certain platforms use AI to assist in copywriting, enabling marketers to produce high-quality content efficiently. Additionally, other AI tools help optimize content for search engines, improving visibility and engagement. [13]

4. Chatbots and Virtual Assistants

---

[9] Pica9, *4 Franchise Marketing Campaigns That Had Viral Impact in 2024*, PICA 9 BLOG (Dec. 23, 2024), https://tinyurl.com/bd928cjr.
[10] *Id.*
[11] *How Does Starbucks Use AI?* ROBOLIZARD BLOG (Nov. 21, 2024), https://tinyurl.com/3kptn54b. *See also* Noah Barsky, *Why Boards Need to Clone Starbucks Digital Leadership*, FORBES, Mar. 18, 2024, https://tinyurl.com/3kjajeeu
[12] Paul Glenn, *AI and Digital Marketing: Insights into the Future of Data- Drive Strategies,* Sept. 13, 2024, https://tinyurl.com/2876mmue
[13] *See* Marketer Milk Team, *25 best AI marketing tools I'm using to get ahead in 2025,* MARKETERMILK BLOG, Nov. 15, 2024, https://tinyurl.com/yrjh3mef.

A common use of AI by franchises and many operations is the use of AI-driven chatbots and virtual assistants enhance customer service by providing instant, 24/7 support. These tools can handle inquiries, resolve issues, and guide customers through the purchasing process, thereby improving the overall customer experience with minimal labor resources.

5. Programmatic Advertising

AI automates the buying and placement of ads, ensuring that marketing messages reach the right audience at the optimal time, a key strategic component in digital marketing. This approach increases efficiency and effectiveness in digital advertising campaigns.[14]

6. Visual and Voice Search Optimization

With the rise of visual and voice searches, companies are leveraging AI to optimize their content for these mediums. This strategy enhances accessibility and aligns with evolving consumer search behaviors. By incorporating AI into these aspects of marketing, companies can deliver more personalized, efficient, and effective campaigns, ultimately driving better customer engagement and business outcomes. AI can analyze data and recognize patterns on a scale that is humanly impossible. While it is important to adopt innovation, franchisors must ensure that their use of this technology complies with United States (US) and European Union (EU) regulations, such as California's AI Training Data Transparency Law (CA AI Law) and AI Transparency Act (CA AI Act), California Business and Professions Code Section 17941,[15] Colorado's AI Act,[16] Utah's AI usage laws,[17] the EU's General Data Protection Regulation (GDPR),[18] the EU's Artificial Intelligence Act (AI Act)[19] and Canada's Digital Charter Implementation Act.[20] In Section IV.G. of this paper, we offer some practical guidance for using this technology in a compliant way.

III. Loyalty and Rewards Programs

A. What is a Loyalty or Rewards Program?

A loyalty program is a strategy that companies use to encourage continued customer loyalty and long-term repeated business and can include coupons, discounts, free merchandise, or advanced access to

[14] *See generally* Jeffrey F. Rayport, *Is Programmatic Advertising the Future of Marketing?*, HARVARD BUSINESS REVIEW, Jun. 22, 2015, https://tinyurl.com/2wvuttmj.
[15] Cal. Bus. & Professions Code § 17941 (2024).
[16] Colo. Rev. Stat. § 6-1-1703 (2024).
[17] Reena Bajowala and Arda Goker, *Utah Enacts First AI-Focused Consumer Protection Legislation in US*, GREENBERG TRAURIG, Apr. 2024, https://tinyurl.com/2p8r4byk.
[18] General Data Protection Regulation (Regulation (EU) 2016/679), https://tinyurl.com/htj4tnwz (GDPR).
[19] Artificial Intelligence Act (Regulation (EU) 2024/1689), https://tinyurl.com/bdd36ccf.
[20] Bill C-27, *Digital Charter Implementation Act*, 2022, 1st Sess, 44th Parl, 2021, (second reading 24 April 2023).

new products before their official release.[21] Loyalty programs "can increase customer stickiness and boost spending" where such loyal customers tend to spend more with the brand. These programs extend brands the ability to introduce new revenue streams, try new offerings, and acquire new customers.[22] A BCG survey found that programs receiving the highest rating for engagement and loyalty can have up to three times the percentage of customers who feel highly engaged with the business vis-à-vis less-successful programs—and as much as five times the percentage who feel loyal to the company. These programs also see an average 35 percentage points greater share of their customers' wallets.[23] There are several types of loyalty programs that offer various levels of incentives, personalization and customer engagement. The following are examples of loyalty programs used by many franchises:

1. Points Based System

A standard and common type of free loyalty program is a points based system. An example of a free points based system is BPme Rewards. Members earn 1 point per liter of regular fuel and 2 points per liter of Ultimate fuel and 1 point per £1 spent in BP convenience stores on eligible items.[24] Points can be redeemed for fuel, in-store purchases and even gift cards.[25]

BPme Rewards enhances customer engagement by offering real savings on essential purchases like fuel, while also providing digital convenience through its mobile app.[26] The ability to earn points beyond just fuel purchases makes it a comprehensive rewards program.[27]

2. Tiered Rewards System

A tiered rewards system allows an additional level of personalization for customers compared to a points based system. This type of reward system offers different tiers of benefits based on a customer's engagement or spending. As customers increase their purchases or interactions with a brand, the customer progresses through tiers that provide increasingly valuable rewards. This structure incentivizes higher spending and fosters deeper brand loyalty.

---

[21] WixEncyclopedia, *Loyalty Program*, last visited Apr. 17, 2025, https://tinyurl.com/448eyju4.
[22] Comarch Loyalty Platforms, *A Comprehensive Guide to Paid Loyalty Programs*, COMARCH, Oct. 29, 2024. *See also* Vignesh Wadarajan, *Loyalty Programs: What Works And What Doesn't*, FORBES, Nov. 18, 2022, https://tinyurl.com/musztkdf.
[23] Elizabeth Hearne, Ed Crouch, Ben Eppler, Carolyn Nelson, and Harsha Chandra Shekar, *Loyalty Programs Need Next-Generation Design*, BCG BLOG, May 30, 2023, https://tinyurl.com/bdv6kevp.
[24] BP United Kingdom, *BPme Rewards*, BP, last visited Apr. 15, 2025, https://tinyurl.com/48v2dte4.
[25] *Id.*
[26] *Id.*
[27] *Id.*

At Sephora, the tiered loyalty program incorporates a tiered and paid approached with different levels of membership and benefits based on the dollar amount spent with the company.[28] Points can be redeemed for beauty products, exclusive experiences, and discounts. Sephora's program has three tiers: (1) Insider (free to join) – basic membership with birthday gifts and seasonal promotions, (2) VIB (Very Important Beauty Insider) with a spend of $350/year earns more rewards and early access to sales, and (3) Rouge (spend $1,000/year) – highest tier with exclusive events, free shipping, and first access to new products.[29] Sephora's program is successful because it keeps customers engaged with personalized recommendations, early product access, and high-value rewards.

3. Paid Loyalty- VIP/Premium/Subscription

A paid loyalty program requires an upfront investment for membership such as a regular fee (usually on a monthly or annual basis) to join for exclusive benefits such as discounts, free miles, early access or certain exclusive products or services.[30] The types of paid loyalty programs differ slightly but all target high-value customers. "In the aftermath of the lockdown, paid programs have emerged as a way to show clients you're ready to take that relationship to the next level and offer exclusivity and a personal touch that free programs simply can't."[31] Setting a brand apart from the plethora of loyalty programs is increasingly difficult. Paid loyalty programs and those incorporating Artificial Intelligence (AI) can forge specialized relationships with customers through sophisticated levels of personalization and tailored experiences. Such paid programs also represent a strategic venue to attract new customers.

According to a BCG survey, over 60% of digitally savvy consumers under the age of 35 anticipate joining at least one new paid program within the next years, with a notable 17% expecting to enroll in three or more.[32]

While many refer to paid/VIP/Premium/Subscription loyalty programs interchangeably, there are slight differences as reflected in the chart below.[33]

Type	Definition	Features	Examples
Paid Loyalty Programs	Customers pay a fee to join the program.	Typically offers enhanced rewards, exclusive discounts,	Amazon Prime, which provides free shipping, access to streaming

[28] *Beauty Insider Benefits*, SEPHORA, last visited Apr. 15, 2025, https://tinyurl.com/yfecm6um.
[29] *Id.*
[30] Comarch Loyalty Platforms, *A Comprehensive Guide to Paid Loyalty Programs*, COMARCH, Oct. 29, 2024, https://tinyurl.com/ey6vmypr.
[31] *Id.*
[32] Hearne, Crouch, Eppler, Nelson & Shekar, *supra* at n. 23.
[33] Comarch Loyalty Platforms, *supra* at n. 30.

Type	Definition	Features	Examples
		or special services not available to non-members.	services, and more for an annual fee.
Premium Loyalty Programs	A subset of paid loyalty programs, often with a focus on providing high-end or luxury benefits.	Provides top-tier perks such as access to exclusive events, premium customer service, and higher earning rates for points.	Airline programs offering first-class lounge access and elite hotel memberships with guaranteed room upgrades.
Subscription Loyalty Programs	Customers subscribe to regular deliveries or services, which may include additional loyalty benefits.	Regular, ongoing payment (monthly, quarterly, or annually) for a set of services or products, often bundled with loyalty rewards.	Subscription boxes (e.g., Birchbox), streaming services with loyalty points, or perks (e.g., Netflix offering discounts on merchandise).
VIP Loyalty Programs	Programs targeting a company's most valuable customers, often based on spending thresholds or frequency of purchase.	Exclusive access to special events, personal concierge services, higher reward points, and other luxury perks. Often invitation-only or based on achieving a certain status.	High-end retailer programs (e.g., Nordstrom's "The Nordy Club" at higher tiers), credit card VIP

While loyalty programs effectively enhance customer engagement and retention, they also present opportunities for fraudulent activities. To maintain the integrity and success of these programs, implementing robust fraud prevention strategies are a must to safeguard both customers and company resources.

B. Preventing Fraud in Loyalty Programs with AI

Preventing customer fraud in loyalty programs, especially concerning the exploitation of free items, requires a multifaceted approach that combines technological safeguards, strategic program design, and customer education. AI can play a pivotal role in safeguarding loyalty programs against fraudulent activities by enhancing detection capabilities, automating processes, and adapting to emerging threats. Such contributions can include automated detection of fraud, continuous monitoring and adaptation, proactive anomaly detection, and real time decision making.

1. Automated Detection of Fraudulent Activities

AI systems can process vast amounts of transaction data in real-time, identifying patterns and anomalies that may indicate fraudulent behavior. This automation reduces the need for manual monitoring, allowing for swift responses to potential threats.[34] According to a Statista survey, in 2024, refund/policy abuse was the most common type of fraud experienced by just under half of online merchants worldwide.[35]

2. Continuous Monitoring and Adaptation

Machine learning algorithms enable AI to continuously learn from new data, adapting to evolving fraud tactics. This dynamic approach ensures that the system remains effective against sophisticated schemes, providing ongoing protection for loyalty programs.[36]

3. Enhanced Accuracy and Reduced False Positives

By analyzing complex data sets and recognizing subtle indicators of fraud, AI improves the accuracy of detection systems. This precision minimizes false positives, ensuring legitimate customers are not inconvenienced while effectively targeting fraudulent activities.[37]

4. Proactive Anomaly Detection

AI's ability to identify unusual patterns in user behavior allows for proactive measures against fraud. By detecting anomalies that deviate from established norms, AI can flag suspicious activities before they result in significant losses.[38]

5. Real-Time Decision Making

The speed of AI processing enables real-time analysis of transactions, allowing businesses to make immediate decisions regarding the legitimacy of activities within their loyalty programs. This rapid response is crucial in preventing fraudulent actions before they escalate.[39]

By incorporating AI into fraud prevention strategies, businesses can effectively protect their loyalty programs, maintain customer trust, and safeguard revenue.

C. Data Collection

[34] *See* Dhruv Verma, *Using AI to combat fraud in loyalty programs*, FINANCIAL EXPRESS, Sep. 22, 2024, https://tinyurl.com/3byfde5k.
[35] Lynn Beyrouthy, *Main types of e-commerce fraud experienced by merchants worldwide 2024*, STATISTA, Dec. 10, 2024, https://tinyurl.com/mv3vzbh4.
[36] *Id.*
[37] Verma, *supra* at n. 34.
[38] *Id.*
[39] *Id.*

From a marketing perspective, data is still gold. Collecting personal data from customers, such as name, address details, purchasing behavior, customer communication, social media interactions, third-party data, and information provided by the customer themselves through surveys, are all extremely valuable for a personalized digital marketing campaign.

In practice, however, collecting personal data is not always easy. An appealing loyalty program can sometimes convince a (potential) customer to create an account and fill in a list of personal details. The customer then becomes a member. The feeling of belonging to an exclusive "club" often resonates, as does the prospect of earning discounts and certain perks such as invites to events.

There are various tools available in the market that can segment customers (e.g., "new customers," "best customers," and "intermittent customers"—often even more specific categories). AI is then applied to these segments to predict customer behavior per segment. Based on this, hyper-personalized offers are generated. Next, AI-driven chatbots guide customers through the purchasing process, thereby improving the overall customer experience. It is imperative to align such marketing methods with relevant US and EU legislation, such as Utah's AI usage laws,[40] California's Business and Professions Code Section 17941,[41] California's AI Law and AI Act, the GDPR,[42] the AI Act[43] and Canada's Digital Charter Implementation Act.[44] In the following section of this paper we will discuss the applicable US, EU and Canadian laws, and some key compliance considerations.

IV. Legislation Applicable to Digital Marketing and Loyalty and Reward Programs

A. Utah's AI Usage Laws

In April 2024, Utah became the first state in the U.S. to enact a statute specifically governing private-sector AI usage.[45] The new statute was incorporated into Utah's consumer protection statutes. Under the new law, if a business or natural person uses generative AI to interact with an individual in connection with commercial activities regulated by Utah's Division of Consumer Protection, it must clearly and conspicuously disclose to the individual that he or she is interacting with generative AI and not a human. This requirement applies only if the individual interacting with the generative AI prompts or asks the generative AI to disclose whether the individual is interacting with a human. The Utah law also sets forth more restrictive disclosure obligations on persons providing the services of "regulated occupations" such

[40] Bajowala & Goker, *supra* at n. 17.
[41] Cal. Bus. & Professions Code, *supra* at n. 15 at § 17941.
[42] Regulation (EU) 2016/679, *supra* at n. 18.
[43] Regulation (EU) 2024/1689, *supra* at n. 19.
[44] Bill C-27, *supra* n. 20.
[45] Bajowala & Goker, *supra* at n. 17.

as clinical mental health, dentistry, and medicine. Further, the Utah law establishes liability for inadequate/improper disclosure of generative AI use and creates the Office of Artificial Intelligence Policy to administer Utah's AI program.[46] Since the enactment of the Utah law, at least five other states (California, Colorado, Illinois, New York and Maryland) have enacted some form of legislation governing the use of AI.

B. California's Chatbot Related AI Laws, AI Training Data Transparency Law and AI Transparency Act

California's Business and Professions Code makes it unlawful for any person or business to use a bot to communicate or interact with a person in California online, with the intent to mislead the other person about its artificial identity for the purpose of knowingly deceiving the person about the content of the communication in order to incentivize a purchase or sale of goods or services in a commercial transaction. The code requires the person or company using the bot to display a clear, conspicuous, and reasonable disclosure informing persons with whom the bot communicates or interacts that it is a bot.[47] A business or person or business using a bot will not be liable if it makes such disclosure.

In September 2024, California enacted two AI-specific laws, the CA AI Law and the CA AI Act,[48] both of which take effect January 01, 2026. The CA AI Law requires developers to post, on their websites, information regarding the data used to train their AI systems. The law is said to adopt a definition for AI that is also seen under other laws, such as the EU AI Act and Colorado's Artificial Intelligence Act (Colorado AI Act).[49] The CA AI Law regulates generative AI, which can "generate derived synthetic content, such as text, images, video, and audio, that emulates the structure and characteristics of the artificial intelligence's training data." Developers are required to document information related to sources and owners of datasets, the intended purpose of the GenAI system, a description of the types of data used, intellectual property considerations, and privacy considerations, among others.

Further, the CA AI Act, defines a "covered provider" as a person that creates, codes, or otherwise produces a GenAI system that has over 1,000,000 monthly visitors or users and is publicly accessible within the geographic boundaries of the state. The CA AI Act, among other things, requires a covered provider to make available to a user "the option to include a manifest disclosure in image, video, or audio content […]

---

[46] Harris Chernow, Alan Greenfield & Tony Marks, *Practical Advice for In-House Counsel*, INTERNATIONAL FRANCHISE ASSOCIATION 56TH ANNUAL LEGAL SYMPOSIUM, 25-26 (2024).
[47] Cal. Bus. & Professions Code, *supra* at n. 15, at § 17941.
[48] *California passes legislative instruments governing GenAI*, MOODY'S, Oct. 28, 2024 https://tinyurl.com/2suy3tvn8s.
[49] Colo. Rev. Stat., *supra* at n. 16, at § 6-1-1703.

created or altered by the covered provider's GenAI system." This disclosure would identify that the output is AI-generated content, be permanent (or "extraordinarily difficult to remove"), and be "clear, conspicuous, appropriate for the medium of the content, and understandable to a reasonable person." Additionally, a Covered Provider must "include a latent disclosure in AI-generated image, video, or audio content, or content that is any combination thereof, created by the covered provider's GenAI system." The disclosure must, to the extent technically feasible and reasonable, provide pertinent information (name of the Covered Provider, data on the system that generated the content, time and date of creation, and a unique identifier), be consistent with industry standards, and also be "permanent or extraordinarily difficult to remove." The CA AI Act also requires Covered Providers to make available an AI detection tool to identify content created by their system "at no cost to the user" and the disclosure must be "detectable by the covered provider's AI detection tool."

If a covered provider knows a third-party licensee modified a licensed GenAI system in a way that it is no longer capable of including the required disclosures in the content the system creates or alters, the provider must revoke the license within 96 hours of discovering the licensee's action. The CA AI Act also requires a third-party licensee to cease using a licensed GenAI system after the license for the system has been revoked by the covered provider. As per the CA AI Act, a Covered Provider that violates the CA AI Act "shall be liable for a civil penalty in the amount of $5,000 per violation to be collected in a civil action filed by the Attorney General, a city attorney, or a county counsel." Additionally, each day a Covered Provider is in violation is "deemed a discrete violation." The Act also stipulates penalties for third-party licensees. The Act states that "for a violation by a third-party licensee […] the Attorney General, a county counsel, or a city attorney may bring a civil action for" injunctive relief and reasonable attorney's fees and costs.

C. Colorado's Artificial Intelligence Act

Colorado became the first state in the U.S. to enact a comprehensive law relating to the development and deployment of certain AI systems. The Colorado AI Act will go into effect on February 1, 2026, adopts a risk-based approach to AI regulation that shares many similarities with the EU AI Act.

Among other obligations, the Colorado AI Act creates duties for developers and deployers to use reasonable care to protect consumers from any known or reasonably foreseeable risks of "algorithmic discrimination" arising from the intended and contracted uses of "high-risk AI systems." "Algorithmic discrimination" includes any use of a high-risk artificial intelligence system that:

> results in unlawful differential treatment or impact that disfavors an individual or group of individuals on the basis of their actual or perceived age, color, disability, ethnicity,

> genetic information, limited proficiency in the English language, national origin, race, religion, reproductive health, sex, veteran status, or other classification protected under the laws of [Colorado] or federal law.[50]

A "high-risk AI system" is a system that makes or is a substantial factor in making a "consequential decision," which is a decision that has a material legal or similarly significant effect on the provision or denial to any consumer of, or the cost or terms of: (i) education enrollment or an education opportunity; (ii) employment or an employment opportunity; (iii) a financial or lending service; (iv) an essential government service; (v) health-care services; (vi) housing; (vii) insurance; or (viii) a legal service.[51] Developers are also required to clearly display on their website, or in a public use case, inventory an up-to-date disclosure of any high-risk AI systems they have developed and make available how they manage known or reasonably foreseeable risks of algorithmic discrimination. However, deployers that make available any AI system that interacts with consumers (even if not high-risk) must disclose to the consumer that they are interacting with an AI system, unless it would be obvious to a reasonable person.

Developers must disclose any known or reasonably foreseeable risks of algorithmic discrimination arising from the intended uses of a high-risk AI system to the Colorado Attorney General and to all known deployers or other developers of the system within 90 days. Like with developers, deployers of high-risk AI systems must notify the Colorado Attorney General of any algorithmic discrimination caused by a high-risk AI system they have deployed within 90 days after making such a discovery. The Colorado Attorney General has exclusive enforcement authority to address violations of the Colorado AI Act.[52]

D. European Union's General Data Protection Regulation

The EU's GDPR has been in effect since May 25, 2018. The GDPR offers a framework for the protection of personal data of individuals. It applies to organizations that are established in the EU and to organizations not established in the EU that intentionally offer goods or services to individuals residing in the EU, or that monitor the behavior of individuals within the EU.

An organization that decides to process personal data, i.e. that determines the purposes and the means of the processing of personal data is the 'controller' under the GDPR.[53] The controller bears all responsibility under GDPR and must comply with all its obligations. "Personal data" is any information

[50] Colo. Rev. Stat., *supra* at n. 16, at § 6-1-1701.
[51] *Id.*
[52] *Id.* at § 6-1-1706.
[53] Regulation (EU) 2016/679, *supra* at n. 18 at Art. 4(7).

relating to an identified or identifiable natural person (such as a name, an email address, an online identifier etc.)

1. Legal Basis

A controller is only allowed to process personal data if it has a legal basis to do so.[54] The most commonly used legal grounds are *consent* of the individual or *the legitimate interest* of the controller or a third party. If the controller wishes to rely on consent as a legal ground for processing, certain conditions apply. The consent needs to be freely given (no pre-ticked boxes), specific, informed and unambiguous.

If an organization offers customers to join its loyalty program, customers usually sign up via an account, thereby providing their personal data. Such collection of personal data requires a legal basis. If participation in a loyalty program is based on consent, it is important to keep in mind that there are often different processing activities for different purposes. Separate consent must be requested for each purpose. A common concern of marketers is that the more consent checkboxes a customer must click, the more likely they are to lose interest and 'drop off'. For each purpose, it should be considered whether another legal basis might be appropriate, such as legitimate interest. However, sometimes consent is the only option. Sending out personalized marketing messages must always be based on consent. This consent checkbox should not be a "mandatory field" – it cannot be a condition for joining the loyalty program.

2. Transparency

According to article 13 of the GDPR, controllers are required to inform individuals such as customers about their data processing activities. This is usually done via an easy to find (online) privacy statement. This privacy statement must provide a clear explanation of the loyalty program, including the different processing activities, purposes, and legal bases.

3. Data Minimization

According to the principle of data minimization, personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.[55] It is therefore important to only process personal data from loyalty members that align with their expectations (such as purchase history). Processing activities like web scraping to draw up more detailed customer profiles should be avoided.

[54] Regulation (EU) 2016/679, *supra* at n. 18 at Art. 6.
[55] Regulation (EU) 2016/679, *supra* at n. 18 at Art. 5(1)(c).

4. Automated Decision-Making

The GDPR recognizes that automated decision-making, including profiling can have serious consequences for individuals. According to article 22 (1) of the GDPR, individuals shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

In many typical cases the decision to present advertising based on profiling will not have a 'similarly significant effect' on individuals, for example an advertisement for a mainstream online fashion outlet based on a simple demographic profile: 'women in the Brussels region aged between 25 and 35 who are likely to be interested in fashion and certain clothing items'.[56] However, in certain cases, such decisions *may* significantly affect individuals, depending on specific factors, including:

- The intrusive nature of the profiling process;
- The expectations and wishes of the individuals concerned;
- The use of knowledge about vulnerabilities of the targeted individuals.

Automated decision-making that results in differential pricing based on personal data or personal characteristics could have a significant effect if, for example, prohibitively high prices effectively bar someone from certain goods or services.[57] Controllers should therefore always avoid *intrusive* profiling, be mindful of customer expectations, and avoid using special categories of personal data or insights into their vulnerabilities.

E. European Union's Artificial Intelligence Act

The EU's AI Act is a highly impactful European Regulation, the first law to regulate Artificial Intelligence in general.[58] The AI Act follows a risk-based approach, in which AI systems providing higher risks are met with more compliance obligations and mitigation measures than those with low to no risks.[59] As a regulation, the AI Act provides directly enforceable obligations on its subject matter: AI systems. 'AI system' means a machine-based system that is designed to operate with varying levels of autonomy, and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the

[56] EDPB Guidelines on Automated Individual Decision-Making and Profiling for the purposes of Regulation (EU) 2016/679, Feb. 6, 2018, p. 22, available at https://tinyurl.com/bdzehd8n.
[57] *Id.*
[58] Arnoud Engelfriet, *The Annotated AI Act: Article-by-article analysis of European AI legislation* (2024).
[59] *Id.*

input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.[60]

The AI Act applies to providers that place in the EU market or put into service AI systems, irrespective of whether the provider is established within or outside the EU.[61] It also applies to deployers of AI systems established in the EU.[62] Furthermore, the AI Act applies to providers and deployers in countries outside the EU, when the AI systems they provide or deploy produces output that is used in the EU.[63]

In its risk-based approach, the AI Act creates three categories: Article 5 of the AI Act lists certain prohibited AI practices because they are particularly harmful and abusive;[64] Article 6 discusses AI systems that are 'high-risk;' and for AI systems related to products that are not high-risk, Regulation (EU) 2023/988 on general product safety applies as a safety net.[65]

1. Content creation

If ad content is generated by AI and qualifies as generative AI, the provider of the AI system must indicate such.[66] According to art. 50 (2) of the AI Act, providers of AI systems, generating synthetic text content, shall ensure that the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated.

2. Chatbot

AI-driven chatbots enhance customer service and may guide customers through the purchasing process. According to art. 50 (1) of the AI Act, providers shall ensure that AI systems intended to interact directly with natural persons are designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system, unless this is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect, taking into account the circumstances and the context of use. This applies to all AI systems, regardless of their risk level.[67]

F. How does the EU AI Act work with regard to digital marketing using AI?

[60] AI Act at Art. 3(1).
[61] AI Act at Art. 2(1)(a).
[62] AI Act at Art. 2(1)(b).
[63] AI Act at Art. 2(1)(c).
[64] AI Act at Recital 28.
[65] AI Act at Recital 166.
[66] AI Act at Art. 50(2).
[67] Engelfriet, *supra* at n. 58.

The rapid rise of artificial intelligence (AI) in digital marketing is fundamentally reshaping how franchise networks engage with consumers, personalize offerings, and manage sales processes. From algorithmic targeting to automated pricing and behavioral analytics, franchisors and franchisees are increasingly integrating AI technologies to gain a competitive edge. However, these innovations also raise complex regulatory questions – particularly in the European Union, where the new **AI Act** (EU) 2024/1689 introduces a comprehensive compliance framework that applies directly across all Member States. The AI Act entered into force on August 1, 2024. Some provisions, in particular on prohibited AI practices and AI literacy obligations went into effect on February 2, 2025. The AI Act will be fully applicable on August 2, 2026 (*cf.* Article 113). Though the AI Act brings forward quite some requirements, it focuses on high risk AI – which in practice only concerns a small number of AI systems as per the European Commission's interpretation: "The vast majority of AI systems currently used in the EU fall into this category [of minimal risk] where the new rules do not intervene as these systems represent only minimal or no risk for citizen's rights or safety."[68]

1. The Risk-Based Approach of the AI Act

The AI Act follows a risk-based regulatory structure, imposing obligations based on the potential harm AI systems may pose to safety and fundamental rights. Its relevance for franchising lies not only in the use of AI in products (e.g., smart appliances) but especially in the deployment of AI tools in digital marketing and sales strategies. The regulation basically[69] distinguishes[70] between:

- **Prohibited AI practices**, which include emotionally manipulative techniques, social scoring, and certain forms of profiling for price discrimination (Art. 5 AI Act). These are categorically banned.
- **High-risk AI systems**, which may include tools used for credit scoring or AI-based personal pricing that significantly affect consumers' access to goods or services (Art. 6(1)(b) and Annex III of the AI Act).
- **Low or minimal risk AI**, where only transparency obligations apply – this covers the majority of AI applications used in EU digital marketing today.

2. Implications for Franchisors and Franchisees

[68] European Commission, *Excellence and trust in artificial intelligence: Trustworthy artificial intelligence (AI),* https://tinyurl.com/bderwxpc
[69] The European Commission distinguishes four levels of risk, from minimal risk, over limited risk (AI systems with specific transparency obligations) over high risk to unacceptable risk, *cf.* https://tinyurl.com/yc8kf4kd.
[70] *Cf.* for an overview of AI compliance requirements: Rohrßen, ZfPC 2024, 111, 115 *et seq.*

The AI Act's obligations apply not only to AI developers but also to so-called "deployers" – i.e., businesses that integrate and use AI in their operations. This makes franchisors and franchisees alike responsible for compliance when adopting AI-based systems within their networks.

Key applications in franchising include:

- **Dynamic pricing and personalization tools**: If these tools materially affect consumer decision-making or access to products, they will generally qualify as low or minimal risk AI, especially if they do not work with:
    - manipulative or deceptive techniques or exploit vulnerabilities due to a person's age, disability or specific social or economic situation (*cf.* Article 5(1)(a) and (b) AI Act), in which case they could constitute prohibited practices), or
    - tools which evaluate the creditworthiness of customers and thus restrict access to essential private services[71] (unless meant for detecting financial fraud, *cf.* Article 6(2) in conjunction with Annex III No. 5(b));
- **Marketing algorithms and behavioral analytics**: While often classified as low-risk, the line is crossed when such systems exert undue psychological pressure or exploit consumer vulnerabilities, which may constitute a prohibited practice under Article 5(1)(a).
- **Scoring systems for consumer profiling**: Often used in loyalty programs or targeted promotions, these can fall into the high-risk category if they influence access to essential or significant services (Annex III No. 5(b) AI Act).

3. AI Compliance as a Strategic Governance Issue

Franchisors should view AI compliance not merely as a legal necessity but as a governance imperative. Especially in systems where AI tools are centralized and deployed across multiple franchisees, the franchisor may assume the role of AI "provider" or "deployer" under the AI Act, with corresponding liability. The need for contractual clarity, training, and auditing mechanisms within the franchise system becomes paramount.

4. Double Regulation in Product Distribution

Where AI functionalities are embedded into products (e.g., smart vending systems, autonomous vehicles, or robotic devices used in franchised services), obligations under both the AI Act and other EU

[71] Whereby "essential private services" lack a clear definition; they are broadly described as "necessary for people to fully participate in society or to improve one's standard of living", *cf.* AI Act at Recital 58.

product regulations – such as the new Batteries Regulation (EU) 2024/1542,[72] the new Machinery Regulation (EU) 2023/1230,[73] the General Product Safety Regulation (EU) 2023/988[74] or the Cyber Resilience Act (EU) 2024/2847[75] – apply cumulatively. This dual compliance requirement should be considered early in product development and market launch strategy.

5. Practical Next Steps

Franchise systems operating in or targeting the EU should:

- Conduct AI risk assessments for marketing and sales applications;
- Map the AI value chain to clarify roles and responsibilities (provider, deployer, importer, etc.);
- Implement transparency and human oversight measures, especially where AI affects pricing or targeting;
- Review franchise agreements and digital tools licenses for compliance clauses and liability allocation.

AI offers tremendous opportunities in franchising – but the legal framework in the EU, and particularly the AI Act, imposes strict boundaries. For global franchisors, navigating these limits will be key to sustaining consumer trust and regulatory certainty. In this context, compliance becomes a competitive advantage.

[72] The Battery Regulation follows – new – a lifecycle approach, *i.e.* sets rules for the safety, sustainability, and environmental impact of batteries in the European Union, from development over production to recycling and waste batteries.
[73] The Machinery Regulation sets safety standards for machinery and aims to protect users and consumers by regulating the design, manufacture, and use of machinery. On the combined requirements for robots, *i.e.*, machinery with AI embedded, *cf.* Rohrßen, ZfPC 2025, 6 *et seq*.
[74] The General Product Safety Regulation ("GPSR") is the new fundamental regulation on safety for all non-food consumer products.
[75] The Cyber Resilience Act ("CRA") aims to enhance the cybersecurity of products with digital elements / connected products, making them more secure and resilient to cyberattacks.

G. Case studies to illustrate how the EU AI Act impacts AI-driven marketing and sales practices in the franchising sector

1. Case Study 1: Personal Pricing in a Fast-Casual Food Franchise

Scenario:

A global fast-casual restaurant brand uses an AI-powered app in Europe that tailors real-time pricing of meal combos based on customer behavior, time of day, and purchase history. Franchisees across the EU rely on the centralized pricing engine controlled by the franchisor.

Legal Risk under the AI Act:

Apart from competition law risks – retail price maintenance works under EU competition law only in very limited scenarios, e.g. introduction of new products on the market for a short marketing campaign,[76] this model will generally qualify as a low or minimal risk AI system. Dynamic pricing AI could, however, qualify as high-risk AI depending on purpose, context, and impact – especially if used for evaluating the creditworthiness of individuals or for assessing access to essential services, including financial services or benefits (cf. Annex III No. 5). If classified as high-risk, the AI system must meet strict obligations on data governance, transparency, human oversight, and risk management (Arts. 9–15 AI Act),[77] , the threshold being whether the system "poses a significant risk to the health, safety or fundamental rights of natural persons" (Art. 6(2))..

Practical Implication:

The franchisor (as AI provider) and EU-based franchisees (as deployers) may both bear responsibility. Compliance requires a clear justification for the pricing logic, and—only where an AI system qualifies as high risk—transparency towards users, and human oversight mechanisms. Franchise agreements must allocate these responsibilities and ensure franchisees understand the compliance requirements.

[76] *Cf.* Benedikt Rohrßen, *VBER 2022: EU Competition Law for Vertical Agreements*, Chapter 4.1.3 (2023).
[77] The full obligations under Articles 9–15 are: risk management (Art. 9), data governance (Art. 10), documentation and record keeping (Art. 11, 12), transparency (Art. 13), human oversight (Art. 14) and cybersecurity (Article 15).

2. Case Study 2: Targeted Advertising in a Fitness Franchise

Scenario:

A fitness franchise with outlets in several EU countries uses AI to analyze online browsing behavior, fitness goals, and social media activity to target consumers with personalized ads. The system is designed to appeal to insecurities and aspirations – for example, by pushing promotions after users post late-night food photos.

Legal Risk under the AI Act:

If the AI system exerts psychological pressure or emotionally manipulates consumers into joining programs, this may qualify as a prohibited AI practice under Article 5(1)(a). Even if it does not cross that line, it may still require disclosure and opt-in mechanisms under transparency obligations.

Practical Implication:

The franchisor must audit the marketing algorithms for legal risks and may need to adjust or geo-block certain features in the EU. Failure to do so exposes both franchisor and EU franchisees to enforcement action. Proper documentation and a review of marketing workflows become essential.

3. Case Study 3: AI Chatbots in Franchisee Customer Service

Scenario:

A home services franchisor (e.g., cleaning, repairs) deploys AI chatbots for first-line customer interaction across its European network. The bots provide quotes, schedule services, and upsell additional packages based on perceived urgency.

Legal Risk under the AI Act:

While most chatbots fall into the low-risk category, the AI Act requires clear labelling whenever users interact with AI systems (Article 50(1); *cf. also* Article 50(7)). If the chatbot nudges vulnerable consumers (e.g., elderly individuals) toward unnecessary purchases, it may again raise red flags.

Practical Implication:

All customer-facing bots must clearly disclose their non-human nature. Scripts and upselling strategies need legal review to avoid unfair commercial practices. The franchisor should provide franchisees with a compliance toolkit to ensure uniformity and avoid reputational damage.

H. Canada's Artificial Intelligence and Data Act and Related Legislative Developments

1. Overview of Canada's Federal AI Framework

Canada is among the first countries to propose comprehensive federal legislation to regulate AI. At the center of these efforts is Bill C-27, the Digital Charter Implementation Act.[78] This Bill aims to modernize Canada's digital and privacy landscape by enhancing transparency, individual control over personal data and responsible governance of emerging technologies. Upon enactment, it would establish three new statutes: the Consumer Privacy Protection Act (CPPA), the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act (AIDA).[79]

In parallel, several provinces, most notably Québec, Ontario and Alberta, have begun introducing legislation addressing AI transparency, automated decision-making and data governance in the public and private sectors.

2. The Artificial Intelligence and Data Act

The AIDA introduces a principles-based approach aimed at regulating high-impact AI systems. Its central objective is to prevent harm to individuals, property and the broader economy, while enabling innovation through clarity and oversight.[80] The AIDA imposes transparency and accountability obligations on developers, providers and managers of AI systems, and proposes new criminal law provisions for reckless or malicious AI use. The Act would also establish an office led by a new AI and Data Commissioner, serving as a center of expertise in regulation, development and administration of AI use.[81]

3. Legal Authority and Data Protection

While the AIDA governs AI system deployment, Bill C-27 also proposes the CPPA, which will significantly reform Canada's privacy regime.[82] The CPPA enhances individual control over personal data by codifying rights such as data portability, the right to deletion and robust consent requirements. It expands the powers of the Privacy Commissioner of Canada, granting them the authority to issue binding orders and impose fines of up to $25 million or 5% of global revenue, whichever is greater.[83]

---

[78] Bill C-27, *supra* n. 20.
[79] Innovation, Science and Economic Development Canada, *Artificial Intelligence and Data Act*, Sep. 27, 2023, https://tinyurl.com/5avh3vmk
[80] Bill C-27, *supra* n. 20.
[81] *Id.*
[82] *Id.*
[83] Innovation, Science and Economic Development Canada, *supra* n. 79; Bill C-27, *supra* n. 20.

4. Transparency and Automated Decision-Making

Although the AIDA is still pending, Canada's evolving framework emphasizes clear communication when AI is used in decision-making. The AIDA would require organizations deploying high-impact AI systems to disclose their use, ensure human oversight and prevent deception or harm.[84]

Similarly, Québec's Law 25 already mandates disclosure when decisions are made solely based on automated processing and supports an individual's right to know and challenge automated decisions.[85] In Ontario, the proposed Strengthening Cyber Security and Building Trust in the Public Sector Act, would require disclosure of AI use in public sector hiring and expands the jurisdiction of its Information and Privacy Commissioner.[86] Alberta's Protection of Privacy Act, enacted in December 2024, compels public institutions to ensure the accuracy and retention of personal information used by AI systems for at least one year when making consequential decisions.[87]

5. Guidance on Generative AI and Sectoral Developments

To supplement legislative reform, the Government of Canada has recently published a proposed Code of Practice for Generative AI Systems.[88] The Code encompasses principles such as safety, fairness and equality, transparency and human oversight, validity and robustness and accountability. It aims to help developers, deployers and operators of generative AI systems to avoid harmful impacts, build trust in their systems and transition smoothly to compliance with Canada's forthcoming regulatory regime.

Additionally, various sectors across Canada have begun introducing specific guidance on AI use. The Office of the Privacy Commissioner of Canada, in coordination with provincial and territorial privacy regulators, released guidance in December 2024 addressing the responsible use of generative AI.[89] This guidance sets out key principles including transparency, human oversight, accountability, legal authority and data minimization. The Competition Bureau of Canada has also examined how AI affects market behavior and competition.[90] In March 2024, the Bureau published a report recommending inter-agency coordination and balanced regulation to address emerging risks posed by AI-driven business models.

---

[84] Bill C-27, *supra* n. 20.
[85] Act Respecting the Protection of Personal Information in the Private Sector, CQLR, c P-39.1.
[86] Strengthening Cyber Security and Building Trust in the Public Sector Act, SO 2024, c 24.
[87] Bill 33, Protection of Privacy Act, 1st Session, 31st Leg, Alberta, 2024, s 6.
[88] Innovation, Science and Economic Development Canada, *Canadian Guardrails for Generative AI – Code of Practice*, Aug. 16, 2023
[89] Office of the Privacy Commissioner of Canada, P*rinciples for Responsible, Trustworthy and Privacy-Protective Generative AI Technologies*, Dec. 7, 2023, https://tinyurl.com/3jkffvm8
[90] The Competition Bureau of Canada, *Consultation on Artificial Intelligence and Competition: What We Heard*, Jan. 27, 2025), https://tinyurl.com/y9zeyva9

6. Implications for Businesses and Franchise Systems

Taken together, these federal and provincial efforts reflect Canada's move toward a comprehensive, multilevel regulatory regime for AI. While the AIDA and related legislation have yet to be passed, their expected impact on sectors such as digital marketing, loyalty programs and franchising is significant. Businesses operating in Canada should begin preparing for compliance by:

- Identifying and assessing AI systems that could be classified as "high impact" under AIDA;
- Ensuring transparency in how AI is used in customer and franchisee interactions, particularly in decision-making and personalization tools;
- Implementing risk mitigation frameworks to prevent discriminatory outcomes or data misuse;
- Reviewing contracts and franchise agreements to clarify data ownership, oversight responsibilities and compliance obligations across the system; and
- Aligning with national guidance such as the Code of Practice for Generative AI, which emphasizes fairness, privacy and human oversight.

Franchise systems should ensure that AI tools used for customer engagement, franchisee support or operational automation are deployed responsibly, with appropriate human oversight and disclosure. By adopting privacy-preserving and explainable AI practices now, franchisors can reduce legal risk, strengthen trust within their systems and position themselves for long-term compliance under Canada's forthcoming regulatory regime.

V. Conclusion

Franchise brands thrive on consistency, trust, and innovation. As digital marketing becomes ever more data-driven and AI-enabled, the legal guardrails around these technologies are tightening – particularly in the European Union and North America. The good news? Regulatory compliance does not have to stifle creativity. Done right, it enhances credibility and consumer confidence.

Franchisors and their counsel must now treat AI and data governance as integral parts of brand strategy, not back-office issues. That means rethinking loyalty program structures, embedding transparency into digital campaigns, and ensuring franchise agreements allocate roles and responsibilities under laws like the EU AI Act or the Colorado AI Act. Those who invest early in AI literacy, cross-border compliance frameworks, and ethical marketing design will be best positioned to lead in creativity and customer engagement in the next decade of franchising.