Tech Regulation, Algorithms and the AI Buzz in Beverage Alcohol

Adobe Stock Images

Editor's note:

The previous six AI and Alcohol articles have incrementally explored how alcohol suppliers are integrating this technology into their businesses operations to increase productivity, marketing and warehouse initiatives. NABCA continues to explore this untamed world of artificial intelligence, this time looking at regulation and how it impacts the overall beverage alcohol operating sphere. NABCA's Margaret Barchine interviewed Amit Parulekar of Brown-Forman (B-F), and Shreyas Shukla of Info-Tech Research Group's (ITRG), a global IT firm and NABCA member.

Understanding that there is not a single comprehensive federal law regulating artificial intelligence, what and how companies use this technology is critical. If used unwisely, it may negatively impact a company's business operations, reputation and finances. TTB mandates that AI-generated imagery and content follow all existing federal labeling and advertising laws. It is also noteworthy that state governments actively regulate AI, making it similar to beverage alcohol in that each state has nuances that need review and understanding before any company administers programs or initiatives using AI, especially in the beverage alcohol space. State regulations look at consumer protections, data privacy, biases and other targets.

NABCA: What are the critical components of AI regulations you can identify that are specific to the beverage alcohol industry? Once identified, please explain the importance of the influence of the component.

ITRG: There is no single AI law that governs beverage alcohol. Instead, AI sits underneath several overlapping regulatory lenses that already apply to the category such as, alcohol advertising and labeling rules, privacy law, consumer protection law, age-gating expectations, and responsible-marketing standards.

Within that environment, the components that matter most are very specific: who the AI targets, what claims it generates, what data it uses, whether its outputs can be explained, and whether a human remains accountable for the decision it influenced.

For example, the Alcohol and Tobacco Tax and Trade Bureau tells us that:

- AI-generated images should not misrepresent the appearance, color, or characteristics of product in a way that would mislead a consumer about what is in the bottle.
- AI-generated "lifestyle" imagery may not contain any health-related statement that is untrue or misleading as to the health effects of alcohol consumption.
- Any AI-generated depiction of a bottle or label should be a reproduction of an approved label.

These components matter because AI scales mistakes. A flawed human campaign creates a contained compliance issue. A flawed AI-driven campaign can generate thousands of messages, images, and audience segments before anyone reviews the first one. The regulatory exposure might be the same, but the speed and volume are not.

B-F: In my view, the critical components of AI regulation are not necessarily unique to the beverage alcohol industry; we are concerned with the same foundational pillars as any other sector: transparency, data privacy, and bias mitigation. Whether a company is a bank or a brewery, the National Institute of Standards and Technology, AI Risk Management Framework (NIST AI RMF) and AIUC1, the world's first independent certification standard specifically designed for autonomous AI agents, provide a necessary focus on the intersection of data and privacy. Where our industry finds its nuance is in the application of these rules—specifically regarding social responsibility and age-verification.
As a side note, on the regulator side of the advertising industry, we have seen a shift toward regulators using AI for proactive, continuous monitoring of advertisements, representing a significant evolution from traditional reactive oversight.

NABCA: As previously noted there are broad AI regulations for all industries. While this question may be repetitive, what are the nuances you see for the beverage alcohol space or do the same regulations apply across all types of businesses?

ITRG: The broad issues of privacy, bias, transparency, explainability, cybersecurity, consumer protection applies everywhere. They are not industry specific. What changes in beverage alcohol is the risk context, and that context makes governance more demanding.

Three nuances stand out:

- **First,** the audience cannot include minors. For example, industry standards from the Distilled Spirits Council of the United States and Wine Institute set explicit thresholds for the share of underage audience exposure that any marketing placement may carry. AI systems that optimize toward engagement may not honor those thresholds on their own.
- **Second,** claims and representations are tightly regulated. AI-generated product descriptions, labels, social posts, and images cannot misrepresent the product, its packaging, its origin, or its approved label.
- **Third,** the regulatory map is fragmented. Alcohol is regulated federally, by state, in control states, and sometimes locally. A national consumer goods brand can optimize one campaign across the country. A beverage alcohol brand cannot. AI tools that assume a single national rule will produce outputs that are not deployable in practice.

So, the same regulations do apply, they just carry more weight here, with less room for error.

NABCA: As AI continues to emerge, along with its capability to reason, what impact do you see this having in the beverage alcohol industry and the marketplace?

ITRG: The impact will be significant, but it is worth separating what is practical from what is hype. Today, most AI use in beverage alcohol is decision support: explaining why a forecast changed, summarizing campaign performance, drafting content, comparing claims or labels against approved rules.

As AI becomes better at reasoning, the next major change will be that AI will begin to connect information across functions. AI will be able to link a demand spike, a production constraint, a distributor issue, and a marketing campaign into a single explanation of what is happening and what choices the business has. That is real value, particularly in a category where those signals usually sit in different systems and different teams.

The marketplace impact will be positive. Suppliers can plan more accurately, distributors can improve service levels, and marketers can better understand which campaigns are working and why. Decisions get faster and better-informed.

However, this also creates a new risk. AI can sound confident even when the underlying information is incomplete, outdated, or not appropriate for the decision at hand. In a regulated category, a confident wrong answer is more dangerous than an obviously uncertain one. This is why retrieval-augmented generation, data quality, and human oversight are not optional features, they are what make reasoning AI safe to use here.

In the near term, I expect AI to raise both the quality and speed of decisions. The organizations that benefit most will be the ones that deploy it for controlled decision support.

Adobe Stock Images

NABCA: In an earlier article on the subject, AI, Marketing and the Beverage Alcohol Brand Experience, we addressed generative and agentic AI in beverage alcohol. What are some cautions you would say those in beverage alcohol need to be mindful of within these two areas? What may have changed from what was previously shared?

ITRG: Generative and agentic AI carry different risk profiles and need to be governed differently.

Generative AI creates or summarizes content such as campaign drafts, product descriptions, performance summaries, internal analysis. The risk is that the output can sound polished while being inaccurate, non-compliant, or inconsistent with approved brand and labeling standards.

Agentic AI can plan steps, trigger actions, and interact with other systems. In the beverage alcohol sector, an agent should not be allowed to independently launch campaigns, change targeting logic, approve claims, alter allocation rules, or publish content without review. The autonomy that makes agents useful is the same property that makes them risky in a regulated category.

What has changed from earlier discussions is that the market has moved from "AI can create content" to "AI can act" and the fact that AI enforcement is accelerating even without a single comprehensive federal AI law.

So the caution is straightforward: do not overstate what the AI does, do not let it bypass responsible marketing review, do not allow agents to act independently in high-risk areas, and document how the system works. The companies that get this right will be the ones with the clearest accountability when something goes wrong.

B-F: The emergence of 'agentic' AI—tools that can reason and act on behalf of a user—presents both a frontier and a challenge. Recent 2026 data from KPMG shows that 42% of companies have now integrated agents, a massive leap from just 11% in 2025. However, this speed brings a new caution: "Agentic Paralysis," where leaders struggle to navigate the complex spectrum of deployment options. Leaders must recognize that buying agents introduces thorny questions around data ownership, potential vendor lock-in, and the complexity of ensuring data sovereignty in the nation or region where it is physically stored or processed. Evaluating these options appears to be a critical step for any organization at this juncture, and this assessment is rapidly driving a fundamental change from previous years as 57% of organizations now favor a blend of building and buying to meet unique business needs. This 'blended' future means constructing internal agents while augmenting them with specialized third-party modules for contextual intelligence, requiring a federated mix of agents anchored by a unified control system to ensure both trust and scale.

NABCA: As it relates to marketing in the beverage alcohol space, what advice would you offer so that AI-driven behavioral targeting avoids individuals below the legal drinking age?

ITRG: Two principles matter here:

- **The first** principle is that AI-driven targeting cannot be a black box. If a brand cannot describe why an audience was selected, what signals were used, and what exclusions were applied, the model is not mature enough for beverage alcohol marketing. "The algorithm decided" is not a defensible answer.
- **The second** point is that legal drinking age protection must be built into the design of the campaign, not checked at the end. AI tools are very good at optimizing toward engagement. This can create risk if the model begins favoring younger audiences, content, platforms, or behaviors.

This is where existing industry standards still play a role. For example, the Distilled Spirits Council of the United States says digital marketing communications should be placed only where at least 73.8 % of the audience is reasonably expected to be of legal purchase age. That threshold must live inside the optimization itself, not inside a post-launch audit.

My advice is to not ask AI to "find the best audience" without defining what a responsible audience means. AI should optimize only within boundaries the company can explain, monitor, and defend.

NABCA: In another marketing related question, what would you say ensures transparency in how AI would select and target audiences for an alcohol product campaign?

ITRG: Transparency starts with being able to answer a simple question: why did this audience receive this message? If answering it requires guesswork, the campaign is not transparent enough to defend.

The practical test is whether the company can reconstruct the decision after the fact. That means knowing what data was used, what signals informed the audience selection, what signals were deliberately excluded, whether age-gating was applied, whether the audience composition was validated before launch, and who reviewed the campaign before it went live. This is the kind of audit trail that any regulated activity already requires.

Transparency also requires vendor discipline. Many advertising platforms and AI tools rely on proprietary targeting logic that brands cannot inspect directly. That is a commercial

reality, but it does not transfer the compliance burden to the vendor. If the platform cannot demonstrate that the delivered audience meets legal drinking age and responsible marketing expectations, the brand needs another way to verify it; independent audience composition analysis, third-party measurement, contractual reporting commitments, or all three.

Without that evidence, AI-driven targeting becomes difficult to defend, even when the campaign appears to perform well. Performance does not establish compliance.

NABCA: What would you suggest as the process for monitoring AI performance to prevent it from drifting towards unsafe or non-compliant marketing strategies?

ITRG: Monitoring is about making sure the AI continues to behave appropriately after the campaign is launched.

This matters because AI-enabled marketing systems optimize continuously. If the objective is to get clicks, engagement, conversion, or reach, the system will evolve toward whatever audiences, placements, and creative variations that perform better but are not appropriate for beverage alcohol. AI is not malfunctioning when it drifts; it is following the goal it was given. The company's job is to make sure that goal is bound by compliance rules.

A working monitoring process has four parts:

- **Define** the boundaries before launch. Approved audience criteria, prohibited signals, age-gating requirements, blocked placements, creative rules, and escalation triggers should exist as constraints inside the system, not as guidance documents alongside it.
- **Monitor** while the campaign is live. Audience composition, placement reports, creative variations, engagement patterns, and unusual signals (such as sudden engagement spikes, comments suggesting underage interest, unexpected platform shifts) should be reviewed during the campaign cycle, not at the close-out meeting.
- **Build** stop rules. If the campaign begins drifting toward questionable placements, youth-skewing engagement, unapproved creative, or unexplained targeting changes, it should pause automatically and route to human review.
- **Audit** after every campaign. Document what the AI changed, why it changed, and whether the campaign stayed inside approved boundaries.

The point that often gets missed is that the job of governance is not to prevent the model from optimizing. It is to constrain what it is allowed to optimize toward.

NABCA: AI governance manages rules, policies, and ethical standards to ensure these systems are safe, lawful, and responsible. As it relates to data privacy, could you identify a company's liability if an AI tool is used to analyze consumer habits and breaches privacy regulations?

ITRG: Using a third-party AI tool does not transfer accountability from the company that deploys it. The brand still owns the data, the consent, and the outcome.

Liability shows up in three forms:

- **Regulatory liability** - if the company violates privacy laws or consumer protection rules.
- **Civil litigation** - if consumers claim their data was used improperly, particularly around profiling, targeted advertising, or biometric data.
- **Contractual liability** - if partner, retailer, distributor, or platform data is used in ways that violate the underlying agreements.

All three are active enforcement and litigation areas right now.

The sensitivity is heightened for beverage alcohol because consumer data describes the audience and shapes who receives alcohol marketing, what messages they see, and how campaigns are optimized. If that data was collected without proper consent, used beyond the purpose consumers expected, shared with vendors without the right safeguards, or used to target inappropriate audiences, the issue is a privacy problem and a responsible-marketing problem at the same time.

Companies need to treat consumer data used by AI as governed data; they should know the source of the data, the legal basis for using it, the permissions attached to it, the vendor's rights, the retention period, and whether consumers can opt out or request deletion where applicable. They also need to verify that the AI vendor is not reusing the data for their own model training or other purposes unless that has been reviewed and approved. That is increasingly where exposure sits.

NABCA: How do General Data Protection Regulation (GDPR) and the enforcement component of the California Consumer Privacy Act (CCPA) fit into AI regulations? What are the minefields that industry needs to be cautious about?

ITRG: GDPR and CCPA were not written for AI specifically, but they apply to a large share of AI use cases. Most AI in marketing depends on personal data, profiling, behavioral

targeting, automated decisions, and data sharing across vendors and platforms. AI inherits the obligations of the data layer underneath it.

GDPR sets clear rules on how personal data is collected, used, retained, explained, and protected. Article 22 says, individuals have the right not to be subject to solely automated decisions, including profiling, when those decisions produce legal or similarly significant effects and they have the right to human intervention and to contest the outcome. CCPA goes further on the operational side, requiring risk assessments, cybersecurity audits, and consumer rights to access and opt out of automated decision-making technology.[5]

What this means for the beverage alcohol industry, is:

- If the company cannot explain where the audience data came from, what consent or notice was provided, and how consumers can opt out, the use case is indefensible.
- A model that profiles consumers without enough age-related safeguards becomes both a privacy issue and a marketing issue.
- If an agency, data broker, ad platform, or AI vendor is processing the data, the brand needs to know exactly how the data is being used.
- If AI selects an audience, changes campaign delivery, or recommends a marketing action, the company must be able to describe the data used, the logic applied, and the controls that were in place.

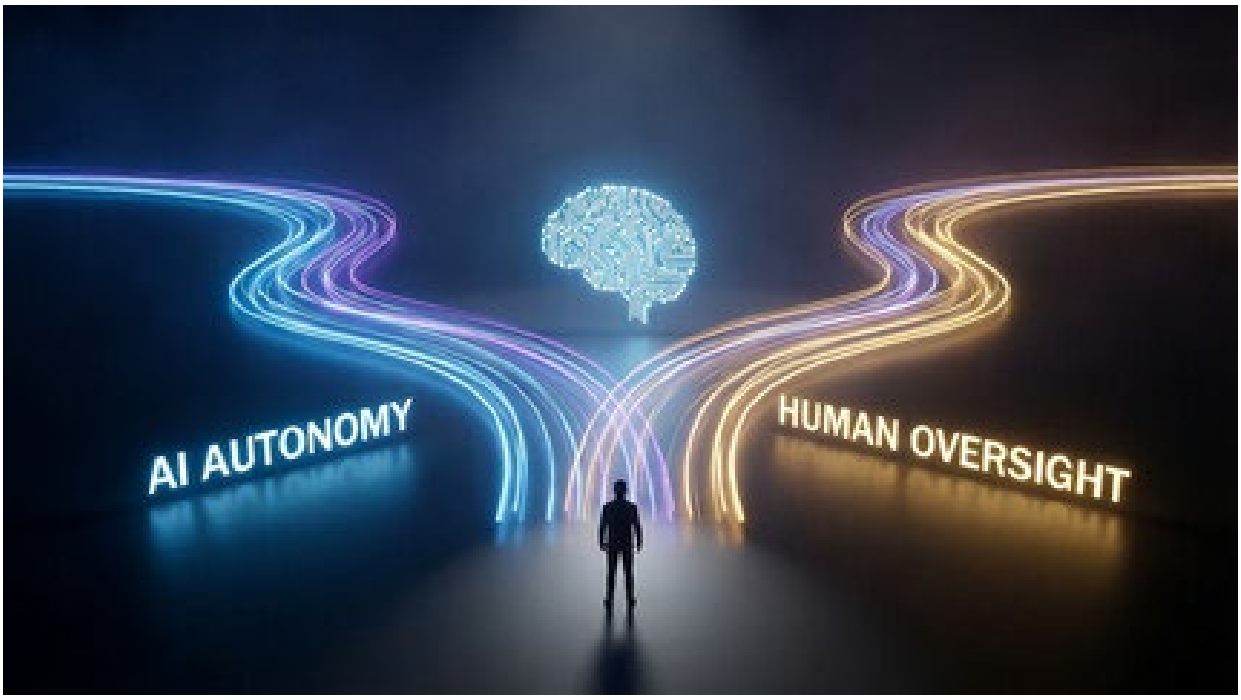
The broader point is that federal agencies, state attorneys general, and private plaintiffs are already using existing consumer protection, privacy, antitrust, and disclosure laws to pursue AI-related conduct. Companies waiting for a comprehensive federal AI statute before tightening their data practices are already exposed under the laws that exist today.

B-F: Regulations like GDPR and the CCPA fit into AI oversight by providing the "highest common denominator" for data protection, but they also carry significant risk; the potential fines for non-compliance under GDPR can be up to 7% of global turnover. The use of AI is critically reliant on huge datasets, which brings data privacy regulations and issues around copyrights and intellectual property immediately into play. GDPR and the CCPA's enforcement mechanisms establish a foundational legal framework for AI governance.

The key minefields industry must navigate are relevant in any industry:

- **Consent:** Ensuring a lawful basis, particularly securing explicit consumer consent for data processing, as required for AI-driven decisions or when data is collected for a specific purpose.

- **Purpose Creep:** The risk that data collected for one specific purpose is repurposed to train or improve AI models, which can violate the GDPR principle of purpose limitation if not consented to.
- **Data Sovereignty and IP Risk:** This refers to the dual challenge of complying with varying global data residency requirements and protecting proprietary and copyrighted materials in the training of AI models.
- **Model Drift:** The tendency for models to evolve towards non-compliant or biased outcomes over time.



Adobe Stock Images

NABCA: What could a company's strategy be if an AI tool violates industry compliance standards?

ITRG: Treat it like a compliance incident, not just a technology defect.

- **Pause** the campaign, workflow, model output, or automated action that created the issue to stop additional exposure.
- **Retain** the AI output, prompts, source data, audience criteria, approval records, vendor logs, and any system actions taken. AI failures can be hard to reconstruct after the fact. If the company cannot explain what the tool did, what data it used, and who approved the result, the compliance issue becomes harder to defend.

- **Determine** whether the issue involved misleading content, improper audience targeting, a privacy concern, an unapproved label or claim, an allocation or pricing concern, or another regulated activity.
- **Correct** by pulling content, adjusting targeting rules, disabling a model feature, changing the workflow, retraining users, or adding a human review gate. This is the final move.

The proof that a company is taking a compliance issue seriously is whether the next campaign reflects what was learned from the last one.

NABCA: Rephrasing the previous question to look at continuous/proactive compliance, what should an organization's strategy look like for an AI tool to ensure vendor accountability, governance, and ongoing compliance with industry standards?

B-F: An organization's AI strategy should emphasize strong vendor accountability and governance from an AI tool provider or solution provider. This includes conducting an initial AI risk assessment of procured tools and requiring vendors to disclose their responsible AI frameworks, along with contractual commitments to recognized standards. Robust IT vendor management practices should be enforced from procurement through ongoing operations, with clear ownership assigned to monitor compliance and embed responsible AI metrics into performance management. Regular reviews of vendor behavior, model updates, and adherence to standards may also help ensure continuous alignment and reduce the risk of violations.

NABCA: Would you recommend companies document AI development processes to demonstrate compliance to regulators if they are audited? Please explain the rationale for your response.

ITRG: Yes, absolutely. Documentation is one of the most practical forms of AI governance a company can put in place.

Regulators, auditors, legal teams, and business leaders will want to understand what the tool was intended to do, what data it used, what controls were in place, who reviewed the output, and why the final decision was accepted.

This matters because AI may touch areas that already have strong compliance expectations, such as marketing, labeling, pricing, promotion, consumer data, forecasting, allocation, and supplier or distributor interactions. In any of those areas, the

documentation should show the business purpose, the data sources, the model or vendor selected, the known risks, the review process, and the monitoring approach.

The level of documentation should match the level of risk. A low-risk internal productivity use case needs a light record. A consumer-facing marketing, targeting, pricing, or compliance-sensitive use case needs a much stronger audit trail; one designed to survive an external review.

B-F: In 2026, documenting AI development processes is no longer merely a best-practice recommendation; for systems classified as "High-Risk" under the EU AI Act, detailed technical documentation is a mandatory legal survival prerequisite for market access. Comprehensive documentation, including "AI system cards," provides the essential evidence required for "Compliance by Design," allowing organizations to reconstruct targeting logic during audits and mitigate the risk of eye-watering fines for non-compliance.

Adobe Stock Images

NABCA: What would you recommend as a plan to update AI governance as new, stricter regulations arise?

ITRG: Companies should treat governance as a living operating model, not a one-time policy document. The pace of AI change is too fast for a "write it once and forget it" approach.

A workable plan has five components:

- **The first** component is an inventory of use cases. Companies need to know where AI is being used, by whom, with what data, and for what purpose. Most organizations underestimate this. Shadow AI is one of the fastest-growing exposures in regulated industries. If an organization's IT or security departments are unaware of employees using AI, it can cause sensitive intellectual information leaks and compliance issues.
- **The second** component is classification of AI use cases by risk. The use cases that need the strictest oversight are the ones that touch consumers, legal drinking age safeguards, regulated claims, personal data, pricing, and market access.
- **The third** component is clear ownership. AI governance needs participation from IT, legal, compliance, marketing, data, cybersecurity, and the business function using the tool.
- **The fourth** component is monitoring of regulatory change. This is especially important in the US, where the absence of a single federal AI statute has not reduced risk. Federal agencies are using existing laws, and states are creating targeted AI rules and expanding enforcement through consumer protection, antitrust, privacy, and disclosure requirements. A quarterly review is typically the minimum.
- **The fifth** component is to build update mechanisms into the governance model. When a new rule, enforcement action, or industry standard emerges, the company should be able to quickly update approved use cases, vendor requirements, data access rules, disclosure practices, human review gates, and monitoring requirements. If a regulatory change requires a six-month internal process to implement, the governance model is too rigid.

The companies handling this well are treating AI governance the way they treat product compliance; a continuous discipline with named owners, regular reviews, and a clear escalation path. The ones treating it as a finished document are the ones that will need to rewrite it under pressure.

B-F: Traditional governance models have historically been static, with policies, standards, and controls designed as fixed artifacts rather than adaptive, living frameworks. Organizations typically revisited these assets on an annual basis, making incremental updates and validating compliance, treating governance as a periodic obligation instead of a continuous capability.

While this approach was sufficient in more stable technology environments, it is fundamentally incompatible with the speed, scale, and dynamism of today's AI-driven landscape, where systems evolve continuously and risks emerge in real time.

As highlighted by the World Economic Forum, the center of gravity in governance is now shifting toward always-on observability. This requires a transition from point-in-time oversight to continuous monitoring, with capabilities for on-demand risk detection, real-time performance tracking, and ongoing measurement of trust, safety, and reliability across AI systems.

In this new paradigm, governance must evolve from static and retrospective processes to dynamic, real-time, and intelligence-driven systems, enabling continuous visibility, proactive risk mitigation, and rapid, data-driven intervention as AI systems operate and adapt.

NABCA: Beverage alcohol companies are global. Is there a way to simplify the regulatory compliance process globally? What would that be?

ITRG: The global beverage alcohol industry operates across different alcohol laws, advertising standards, privacy rules, labeling requirements, age-gating expectations, and market structures. Those differences are not going away.

What can be simplified is the operating model. Companies should establish one global AI governance baseline and localize only where required. That baseline should cover common expectations such as responsible marketing, legal drinking age safeguards, privacy, data use, explainability, vendor oversight, human review, audit trails, and documentation. Local legal and compliance teams can then add market-specific requirements for labeling, promotions, consumer data, or channel rules.

AI can scale activity across markets very quickly. A generative AI tool can produce campaign content for a dozen countries in an afternoon. A targeting model can optimize audience selection across platforms simultaneously. An AI agent can recommend actions

across regions before any local team has reviewed them. Without a global baseline, each market interprets AI risk differently, and the company ends up with inconsistent practices that are difficult to oversee and harder still to defend.

The model that works is global principles, regional controls, and local legal review. Global principles create consistency, regional controls address broader regulatory zones, and local review ensures that market-specific alcohol rules are not missed.

B-F: AI regulatory complexity is not unique to beverage alcohol companies; it is a broader enterprise challenge across industries. Global AI regulations vary widely, reflecting each country's alignment of AI leadership, innovation, and agility with risk mitigation priorities, leading to inconsistent and often incoherent compliance obligations. For global organizations, the most effective way to simplify compliance is to adopt a unified, enterprise-level AI governance framework that standardizes control across markets, with targeted localization only where specifically required.

NABCA: Can you share what you look for when evaluating AI tools that a beverage alcohol company may incorporate into their business operations?

ITRG: I start with one question: what decision is this tool going to influence? The answer determines how much scrutiny it deserves.

A tool used to summarize internal meeting notes is very different from one that recommends audience targeting, pricing, product allocation, label language, supplier risk scores, or inventory actions. The more the tool touches consumers, regulated claims, personal data, pricing, market access, or compliance-sensitive decisions, the higher the bar should be.

From there, the evaluation runs through five lenses:

- **Fit:** Beverage alcohol companies operate inside legal drinking age requirements, responsible marketing standards, federal and state rules, control-state/jurisdiction requirements, distributor relationships, labeling obligations, and brand reputation concerns. If a tool cannot respect those boundaries, it will create more risk than value, regardless of how capable it is in other industries.
- **Data:** What data does the tool use? Where does it come from? Is it first-party, third-party, or vendor-provided? Can the company control whether its data is used for model training? Can the tool separate approved data from informal sources? The data layer is where most AI risk in this category sits.

- **Explainability:** If the AI recommends a forecast change, a supplier action, an audience segment, or a marketing adjustment, the business user must be able to understand why.
- **Control**: Can the company set up guardrails? Block certain outputs? Require human approval before content is published or actions are triggered? Maintain an audit trail of who used the tool, what was generated, what was approved, and what changed over time? These controls matter more as AI becomes agentic.
- **Vendor:** Evaluate the company behind the tool, not just the tool. Does the vendor understand regulated industries? Can they explain their model governance? Do they provide documentation, security controls, privacy commitments, and support for compliance review?

For beverage alcohol companies, the best AI tools are not the most advanced. They are the ones that are useful, explainable, governable, and aligned with the regulatory and commercial realities of the category.

B-F: When evaluating AI tools for a beverage alcohol or any organization, the starting point is confirming that the solution aligns with a clearly defined business need and delivers acceptable performance and accuracy for the intended use case. From there, it is critical to assess how well the solution integrates with the organization's data strategy and existing technology stack, including considerations around data sensitivity, scalability, and readiness.

Financial viability is also key, as AI solutions often introduce different cost structures compared to traditional software. Finally, equal emphasis must be placed on governance, risk, legal, and ethical considerations ensuring the solution effectively manages bias, complies with regulatory expectations, and aligns with organizations responsible AI principles.

Adobe Stock Images

NABCA: Beverage alcohol companies need to operate within a framework of federal and state guidelines for labeling, marketing and other necessary processes. How does your company manage these guidelines? Do they conflict or complement each other?

ITRG: The honest answer is that federal, state, and industry frameworks generally complement each other at the principle level, but they can conflict at the operational level. The shared intent is usually consistent: protect consumers, ensure truthful product representation, support responsible marketing, and maintain regulatory oversight. The difficulty emerges when a single piece of content, a single audience-targeting decision, or a single AI-generated asset is deployed across multiple states at the same time.

Some states may restrict claims, imagery, promotions, or channel practices that are otherwise acceptable under federal rules. Control states add another layer through allocation, listing, merchandising, and promotional requirements that may not exist in license states. Local jurisdictions can introduce further restrictions around placement, retail signage, events, or proximity-based advertising. As a result, a campaign that is

compliant in one state may need to be modified for another, and those modifications are rarely identical.

At the federal level, the framework is relatively stable. The Alcohol and Tobacco Tax and Trade Bureau (TTB) set the baseline for labeling approval, advertising standards, health claims, and product representation. Industry standards from the Distilled Spirits Council of the United States (DISCUS), Wine Institute, and Beer Institute add responsible-marketing expectations on top of that baseline. Most beverage alcohol companies already have internal review processes built around these requirements.

That is why I recommend treating AI-generated content the same way companies already treat labels, claims, marketing copy, and market-specific promotional material. AI should not create a shortcut around legal, regulatory, or brand review. The goal is to make sure people remain responsible for anything AI helps produce.

Acknowledgements:

A. Data & Privacy: AIUC-1. AIUC. (n.d.). https://www.aiuc-1.com/data-and-privacy

Ai Risk Management Framework. NIST. (2026, June 10). https://www.nist.gov/itl/ai-risk-management-framework

Art. 22 GDPR – automated individual decision-making, including profiling. General Data Protection Regulation (GDPR). (2018, July 26). https://gdpr-info.eu/art-22-gdpr/

Banifatemi, A., & Amezaga, K. Y. (2026, January 13). *How can agile AI governance keep pace with technology?*. World Economic Forum. https://www.weforum.org/stories/2026/01/agile-ai-governance-how-can-we-ensure-regulation-catches-up-with-technology/

California, S. of. (2023, March 29). *California Privacy Protection Agency (CPPA)*. California Consumer Privacy Act Regulations - California Privacy Protection Agency (CPPA). https://cppa.ca.gov/regulations/consumer_privacy_act.html

Chandrasekaran, S. (n.d.). *Agentic AI untangled: Navigating the build, buy, or borrow decision*. KPMG. https://kpmg.com/us/en/articles/2026/agentic-ai-untangled.html

Herrington, E. B., Egan, H., Satia, R. P., & Church, E. D. (2026, April 2). *AI enforcement accelerates as federal policy stalls and states step in*. Morgan Lewis - Global Law Firm & Lawyers. https://www.morganlewis.com/pubs/2026/04/ai-enforcement-accelerates-as-federal-policy-stalls-and-states-step-in

Tips for AI-generated imagery in alcohol beverage advertising. TTB. (2026, March 2). https://www.ttb.gov/public-information/featured-stories/tips-ai-generated-imagery-alcohol-beverage-advertising

What is the 73.8% discus rule for social media advertising? | malkin law P.A. (2024, October 4). https://www.malkinlawfirm.com/blog/2024/10/what-is-the-73-8-discus-rule-for-social-media-advertising/

About the writers:

- **Margaret "Maggie" Barchine**, APR, Director, Communications, National Alcohol Beverage Control Association
- **Amit Parulekar**, VP Director - Data and AI Strategy, Brown-Forman
- **Shreyas Shukla** – Principal Research Director, Manufacturing, Info-Tech Research Group