

AI and the Law: Are We Smarter Yet?

How Artificial Intelligence Is Influencing Advertising and Marketing Right Now, and What We Can Expect Next

November 12, 2024

Melissa Landau Steinman

Partner | +1 202.344.4972 | mlsteinman@Venable.com

Justin E. Pierce

Partner | +1 202.344.4442 | jpierce@Venable.com

Rob Hartwell

Partner | +1 202.344.4663 | rlhartwell@Venable.com

Meredith K. McCoy

Partner | +1 202.344.4571 | mkmccoy@Venable.com

VENABLE LLP

Introduction and Speakers



Melissa Landau Steinman

Partner

+1 202.344.4972

mlsteinman@Venable.com

Melissa Steinman focuses on advertising and marketing, promotions, consumer protection, antitrust, trade regulation, and consumer product safety. In addition to counseling and compliance, she also actively represents clients in government investigations and defends clients against class actions. Melissa represents a broad array of clients, including consumer products and hospitality brands, media and tech companies, retailers, gaming and software companies, start-ups, celebrities, producers, charities, and trade associations. She is particularly well known for her deep knowledge of promotions law, including sweepstakes, contests, gift cards, loyalty programs, and charitable promotions, and she speaks and writes frequently on the topic in the United States and internationally.



Justin E. Pierce

Partner

+1 202.344.4442

jpierce@Venable.com

Justin Pierce is a co-chair of Venable's Intellectual Property Division. Justin has significant experience advising companies and their executives on how best to acquire, develop, and apply their intellectual property to achieve their business objectives. He has guided clients through a wide range of matters involving patent litigation, trademark and brand protection, anti-counterfeiting initiatives, copyright, design rights, trade secrets, and licensing. Justin is also well versed in strategies for handling rights of publicity, domain name, and social media disputes. He routinely advises companies with respect to artificial intelligence and cutting-edge issues involving intellectual property.

Introduction and Speakers



Rob Hartwell

Partner

+1 202.344.4663

rlhartwell@Venable.com

Rob Hartwell draws on his deep understanding of the digital marketplace, from company practices to legislative and regulatory developments, as he holistically counsels clients on their product development, advertising and marketing, and policy advocacy. Rob offers practical and actionable advice to companies, complemented by his relationships with policymakers, ensuring that clients can anticipate the coming challenges and requirements.



Meredith K. McCoy

Partner

+1 202.344.4571

mkmccoy@Venable.com

Meredith McCoy provides experienced guidance to businesses, tax-exempt organizations, individuals, and political groups in their efforts to impact public policy and the political process. Meredith works with clients to understand their goals and make tailored recommendations for complying with the range of laws that may affect their plans, including tax, campaign finance, lobbying disclosure, gift and ethics, and pay-to-play laws. Her previous experience as an attorney for the Federal Election Commission helps her foresee compliance challenges and evaluate risks facing Venable's clients. She is skilled at providing practical, user-friendly guidance that helps clients make informed decisions and achieve their objectives.

How Do We Define Artificial Intelligence?

Working definition of AI: “a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.” Ex. Ord. No. 14110. (2024)

- Predictive Analytics
- Programmatic Ads
- Deepfakes
- Voice Cloning, etc.

What is Generative AI (“GenAI”)? A class of AI models that emulate input data to derived generate synthetic content, including images, video, audio, and text.

- Models can be multi-modal, but are generally not deterministic - so outputs can change even if data doesn't
- Models are dependent on training and input data quality

How Are Marketers Using AI?

- Generating imagery, video, animation for ads
- Generating business pitches and completing related tasks
- Customer service chatbots
- Integrating into sweepstakes, games, and UGC requests
- Generating AI avatars for brands, influencers, and customers
- AI search (e.g., Google)
- Product design
- BUT, there are still many challenges (even besides the legal ones)
 - Can't recreate brand logos, products
 - Can't follow brand guidelines faithfully
 - Difficulties in faithfully reproducing human characteristics (6 fingers, anyone)?



AI Executive Order (October 2023)

- Biden administration issued an AI Executive Order in October 2023:
 - “Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence”
- Outlined regulations for agency use of AI, standards and best practices for developing and using safe and secure AI, and support for continued American innovation
- Guiding Principles and Priorities
 - AI Must be Safe and Secure
 - Innovation, Competition, and Collaboration
 - Supporting American Workers
 - Equity and Civil Rights
 - Consumer Protection
 - Privacy
 - AI in Governance and Government



Federal Trade Commission

- FTC is lead U.S. agency in AI consumer protection regarding advertising and data use, as well as unfair and deceptive acts.
 - From early on, expressed concerns about potential use of AI, deepfakes, etc. to mislead or defraud consumers.
 - Chair Lina Khan: “There is no AI exemption from the laws on the books.” FTC has taken the position that AI is not a black box technology; firms must take ownership of what they say it can do and what it actually does.
 - FTC generally asserts authority over deceptive AI claims through Section 5 of FTC Act; has then applied or adopted new rules to address specific conduct as appropriate.
 - Expectation is that bots, etc. will be *designed* to avoid deception; designers and users should avoid emulating humans if it is not necessary, and make disclosure if it is.
 - FTC has begun bringing enforcement actions, provided guidance, and adopted rules in a number of areas related to AI.



FTC Truth in Advertising **and AI Products**

Four Guiding Questions for Truth in Advertising **AI Products**

1. Are you exaggerating what your **AI** product can do?
2. Are you promising your **AI** product does something better than a non-AI product (or non-AI version of a product)?
3. Are you aware of the risks?
4. Does the **AI** product actually use a certain **AI** technology at all?
 - Recent wave of cases involving “AI-washing”: promises the product has AI or can do more using AI than it actually can.



FTC Operation AI Comply

FTC is skeptical of deceptive claims about AI technology, including claims overstating the involvement or capability of the technology (“**AI-washing**”), claims that AI can fully replace human professionals, and business opportunity or earnings claims



“Operation AI Comply” (announced October 2024) includes several such claims:

- ***DoNotPay***: “World’s First Robot Lawyer,” a chatbot subscription that could allegedly be used to create “ironclad” documents (\$193,000 settlement).
- ***Automators AI et al. v. FTC***: FTC suit for unfair and deceptive advertising of a business opportunity scheme that lured consumers to invest in online e-commerce stores and earn passively or learn how to manage them using AI. \$21,765,902.65 settlement (with lifetime ban).
- ***Delphia and Global Predictions Settlements***: Defendants fined by the **SEC** for making deceptive claims about use of AI algorithm that gave their investors an “unfair advantage” over other investors when in fact defendants never used any AI technology. (Delphia fined \$225,000; Global Predictions fined \$175,000).

AI and Reviews

FTC has been pursuing a number of cases involving use of AI in generating and/or collecting reviews:

- ***New case announced 11/16/2024: FTC v. GGL Projects, Inc. d/b/a Sitejabber:*** FTC brought case against AI-enabled consumer review platform that deceived consumers by misrepresenting that ratings and reviews it published came from customers who actually experienced the reviewed product or service when many such reviews were collected at time of purchase, before the product was sent; average ratings and review counts were thus artificially inflated.
- ***Rytr:*** Rytr marketed and sold an AI “writing assistant” that violated Section 5, because it paid subscribers could use to generate an unlimited number of detailed consumer reviews based on limited/generic input, which, as a result, contained specific, material details that “almost certainly would be false for the users who copied them and published them online” and thus lead to potential consumer deception.
- ***Ascend Ecom; Ecommerce Empire Builders; and FBA Machine:*** Businesses used deceptive earnings claims to convince people to invest in AI business opportunities, then threatened consumers who tried to share honest reviews and/or withheld refunds from people unless they withdrew their complaints, in violation of the Business Opportunity Rule and the Consumer Review Fairness Act.

Impersonation, Deepfakes, Chatbots, and AI Influencers

- A significant concern with AI is its potential use to create or impersonate individuals or businesses and thus deceive consumers. AI systems can leverage anthropomorphic design to seem human-like and engage in convincingly spontaneous back-and-forth interactions with human users.
 - AI startup AI21’s experiment “**Human or Not**” paired players for two-minute conversations, after which they had to guess whether were speaking with a human or with an AI chatbot.
 - **68%** of participants guessed correctly when asked whether they talked to a human or an AI bot.
 - AI can be (and has been) used to generate fake reviews, fake influencers, and chatbots—albeit not always successfully.
 - For example, AirCanada’s chatbot invented a refund policy--and then the airline was forced to follow it.
 - Use of AI or CGI influencers has become extremely popular—so popular that the FTC’s recent update to its **Guide to the Use of Endorsements and Testimonials in Advertising specifically addressed it**, saying that their use must be specifically disclosed.
 - The FTC has also passed a new **Impersonation Rule** that will be critically important in addressing issues arising with **the use of AI to impersonate businesses** or **government agencies** to commit fraud
 - FTC is seeking to extend this rule to the use of AI in impersonation of individuals.
 - Rule allows the FTC to seek consumer redress and civil penalties
 - The Rule goes beyond deepfakes and other innovative technologies to bar conduct such as:
 - Deceptive use of government seals or logos
 - Spoofing government or business email or web addresses
 - Adopting lookalike email addresses or URLs

AI and Dark Patterns

FTC is concerned about potential for use of AI to achieve biased and discriminatory results, and other activity that may constitute “dark patterns”

- “Companies thinking about novel uses of generative AI, such as customizing ads to specific people or groups, should know that design elements that trick people into making harmful choices are a common element in FTC cases.”
- *E.g.*, Cases involving [financial offers](#) and [attempts to cancel services](#).
- Risk with AI: AI can analyze a large amount of data and tailor dark patterns to target user preferences and behaviors (and vulnerabilities).

- FTC and DOJ are currently looking at the use of AI/algorithms to manipulate pricing in a potentially discriminatory or anticompetitive way, and whether that may also trigger deceptive pricing and/or antitrust laws.
 - *E.g.*, Agencies are looking at “dynamic” or “surveillance” pricing and have requested information from middlemen; expressed concerns about consumers receiving different prices based on their location, “bait and switch.”
- Manipulation can be a deceptive or unfair practice when it causes people to take actions contrary to their intended goals.
- Disclosures can be particularly important in this context—it should always be clear that an ad is an ad. If generative AI is steering a person towards advertising, then that should be clear, too.

State Law Patchwork

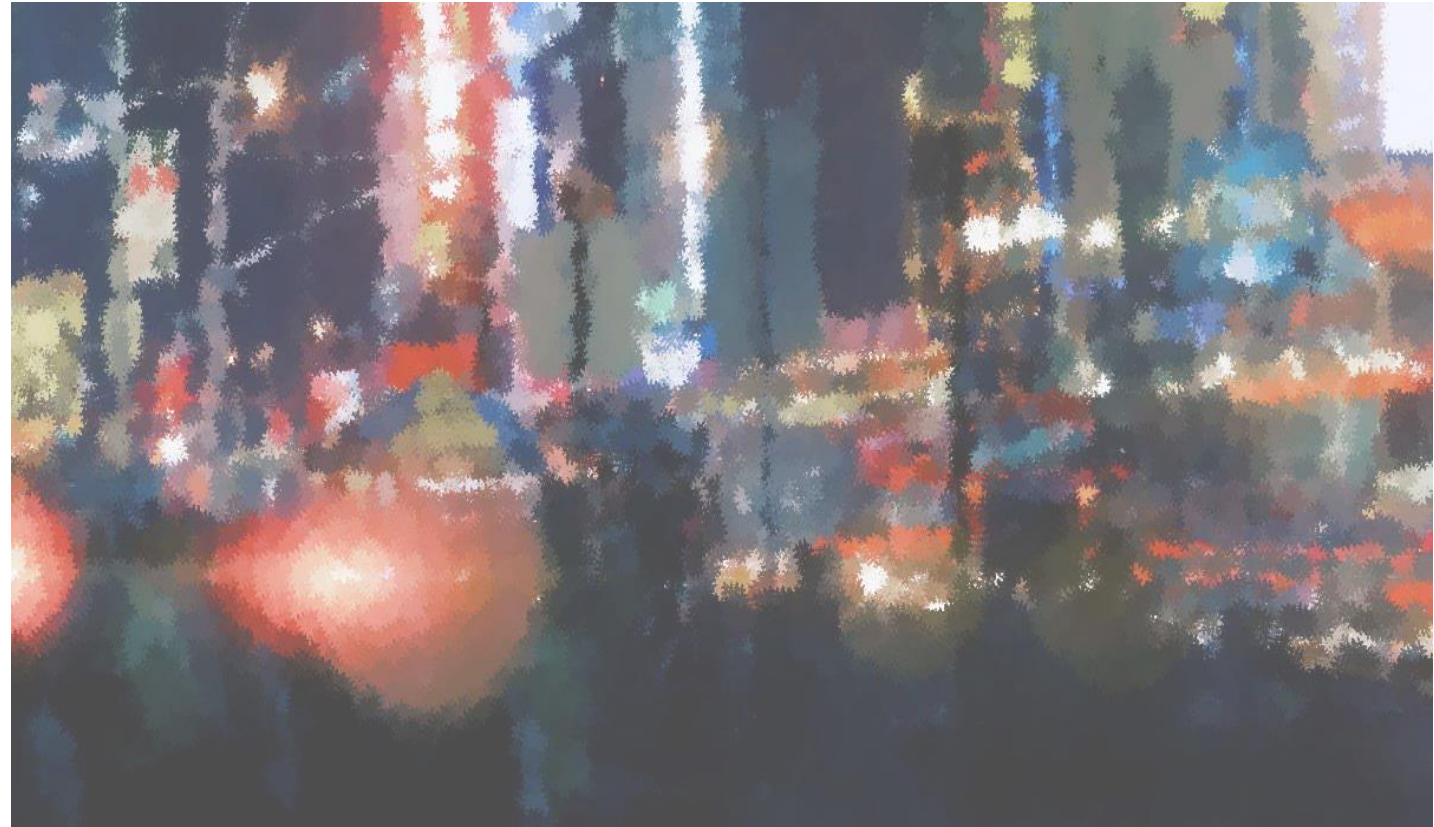
In September of 2024 alone, 30 bills were introduced with the goal of regulating AI.

- **California:** California AI Transparency Act (SB 942)(enacted) requires providers of generative AI systems to:
 - (1) make an AI detection tool available at no cost;
 - (2) include a latent disclosure in AI generated content;
 - (3) provide AI users with the options to include a manifest disclosure; and
 - (4) maintain capability to include disclosure in content.
- CA Artificial Intelligence Training Data Transparency (AB 2013)(enacted): Requires AI developers to disclose the sources of data that trains their models.
- CA Bot Law (2018): “Unlawful for any person to use a bot to communicate with a person online with the intent to mislead about its artificial identity.”
- **Tennessee *ELVIS Act***
 - Protects against any unauthorized commercial use of an individual's voice that is readily identifiable.
- Most state laws to date have been focused on politics/elections: 16 states have enacted laws creating a disclosure requirement or a prohibition on using AI in political advertising.

Artificial Intelligence, IP, and the Advertising Industry

Developing technology is making it easier to create content faster, including advertisements.

- Efficiency
- Speed
- Easy Information
- On-Trend





***(Almost)
Everything
comes from
something.***

Part I: “The Input”

- Data and privacy considerations
- Submission of content
- Applicable laws and regulations

Data Considerations



Scraping for AI Training



Submission of Data or
Confidential Information as Input

Data Considerations – Scraping for AI Training

“Scraping”: the act of pulling data from one website and placing it into another website in a new format; scraped information may include generated data (such as behavioral “cookie” type data, or information entered by the user (inputs))

- U.S. law does not clarify whether copying material for algorithm training purposes requires permission of the content owner, but it is possible that an AI platform or a user could be liable for infringement. Counterargument is “fair use”
- May present Computer Fraud and Abuse Act, copyright infringement, breach of contract, breach of privacy, or other legal concerns for the person responsible for the data scraping
- Entity responsible for data scraping should also consider domestic and international statutes, such as the California Consumer Privacy Act and the General Data Protection Regulation, as “scraping” could violate these statutes if the scraping involves certain personal information or is not stored or deleted accordingly

Data and IP Considerations – Submission of Data or Confidential Information as Input

Submitting certain information to an AI platform may present trade secret and confidentiality risks.

- Compromised trade secret status
- Potential license violations
- Breaches of contract
- Attorney-client privilege
- Violation of applicable privacy laws



Submission of Content

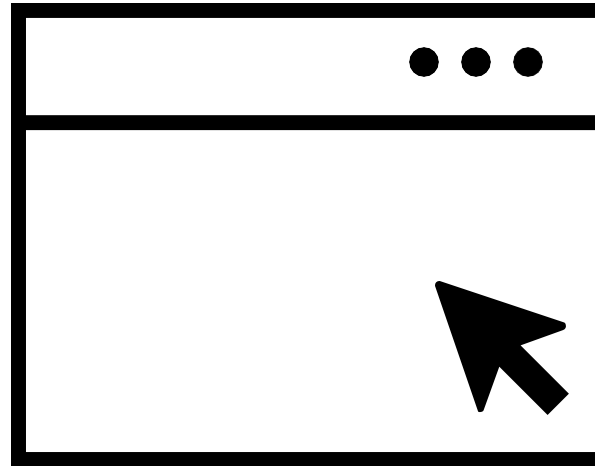


Inputs and IP



Right of publicity concerns

Submission of Content – Inputs and IP



- Submitted input may inform future output. So, submitting the company’s intellectual property to the AI platform opens the risk that the IP is used to inform output for a different user

Submission of Content – Inputs and IP (cont'd)



- Submitted input may infringe the copyright of the owner of the original content (e.g., submitting a poem, seeking to receive output “in the style of” the poem. Arguably, the output is a derivative work of the original poem.)

Submission of Content – Right of Publicity Concerns

- Potential right of publicity concerns
- AI has made it easier for users to mimic human appearances and voices in content
- Deepfakes (Article: [Overview of U.S. Copyright Office Report Regarding Artificial Intelligence and Digital Replicas](#))



Part II: “The Output”

- Flawed Output
- Copyright Ownership
- Lingering IP Loopholes

Flawed Output

Inaccuracies

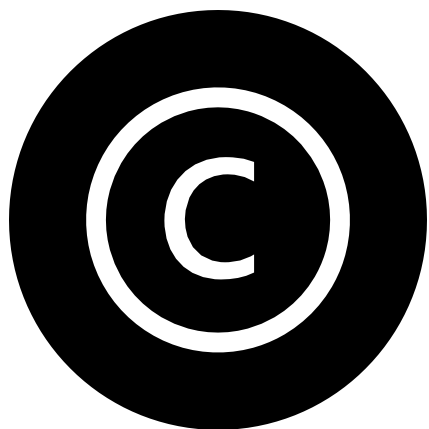
- Hallucination: when an AI platform generates false information
- Cannot assume that all information returned as output is accurate
- Output may also be based on outdated information

Deepfakes

- Simulations that purport to show actions that a person has not taken or create content that seeks to exploit someone's fame or reputation
- Digital replicas = deepfakes



Copyright Ownership



- Copyright Office has published guidance on copyrightability of AI- generated works
- Historically, copyrightable works must be the “product of human authorship” or “human creativity”
- If a work includes AI-generated content and human-generated content, the overall work may be copyrightable, whereas the AI- generated content, alone, is not
- Copyright Office is determining ownership of AI-generated works on a case-by-case basis

Copyright Ownership (cont'd)

- Copyrightability standards for AI-generated works vary by country
- Under the United Kingdom's Copyright Designs and Patents Act of 1988, works created solely by a computer are protectible under copyright for 50 years from the date the work is made. The author of the work is the “person by whom the arrangements necessary for the creation of the work are undertaken.”

Lingering IP Loopholes

- Causes of action for “stolen” AI-generated works?
- Can a user own output as a “work made for hire”?
- Are outputs derivative works of the works on which the AI model was trained?
- Can the terms of use of the AI platform override U.S. copyright principles?
- Will an AI machine, itself, ever be considered an “author” or “inventor” or receive human-like legal acknowledgment for creative works?





Part III: Best Practices

Best Practices – For Advertisers and Marketers



- Generally, establish policies for AI use by employees and contractors involved in advertising and marketing
- Stay abreast of data protection laws, and AI-specific legislation developments
- Review the terms of use/FAQs of the AI platform used by the company to understand the AI platform’s views on ownership and any use restrictions for output
- Review rights associated with any input submitted to an AI platform, and rights that may be associated with any output received, before publishing the output
- “Fact-check” any content generated by AI platforms before publication
- When using artificial intelligence to generate content for another party, disclose that AI has been used in the creation of the content

Best Practices – Licensing AI Tools

- Most company uses of AI platforms will be subject to a license agreement between the company and the provider of the AI platform
- Company may have negotiating power in dictating the terms of the arrangement



Best Practices – Licensing AI Tools (cont'd)

Before licensing an AI tool, consider...

- What is the company trying to achieve with the technology?
- What processes will the new technology enable, accelerate, or automate?
- What data sources will need to be integrated, and is that data integration a risk or violation of any confidentiality or contractual obligations?



Best Practices – Licensing AI Tools (cont'd)

- How will the licensor ensure privacy and confidentiality of data?
- How is data collected and stored, and what rights will each party have to the data?
- What will happen when the agreement is terminated?
- What will happen when the licensor breaches the agreement?
- What if the AI platform “goes down” unexpectedly?
- Is the licensor’s security adequate for the type of data that is being handled?
- Who is liable for third-party lawsuits?

What Is At Its Core?

- Artificial Intelligence (AI) is using computers to:
 - Make decisions and predictions, answer questions, and solve problems using data.
 - Complete tasks that require creativity or higher-order cognitive skills when done by humans.



U.S. Trends

- **Privacy and Data Protection:** A focus on data used in AI is driving state and national proposals around privacy laws.
- **Liability:** States and Congress are exploring how to attribute responsibility when AI systems cause harm, using both existing law and considering new liability frameworks and responsibilities.
- **Safety:** Establishing evaluations and best practices for AI that might impact individuals or society. State laws add additional obligations.
- **Security:** Establishing evaluations and best practices for securing AI systems and data. National agencies add additional obligations in certain sectors.

U.S. State AI Legislation and Actions

At least 45 states, Puerto Rico, the Virgin Islands and Washington, DC introduced AI bills, and 31 states, Puerto Rico, and the Virgin Islands adopted resolutions or enacted legislation. The following are examples:

- **Colorado** enacted comprehensive AI legislation requiring developers and deployers of high-risk AI systems to use reasonable care to avoid algorithmic discrimination and requiring disclosures to consumers.
- **Utah** requires businesses and regulated occupations to disclose the use of AI to consumers.
- **California** requires developers of generative AI to post documentation online about the data used to train the model.
- **Maryland** adopted policies and procedures concerning the development, procurement, deployment, use, and assessment of systems that employ AI by units of state government.
- **New Hampshire** and **Tennessee** passed laws to protect individuals against the use of their persona in deepfakes.

... and others

U.S. AI Policy and Regulatory Developments

- **White House:** In 2023, the Biden administration issued Executive Order 14110 (AI EO) and has secured voluntary commitments from companies to promote the safe, secure, and transparent development and use of generative AI. These agreements include actions focused on AI security and synthetic content.
- **NIST:** NIST's U.S. Artificial Intelligence Safety Institute (USAISI) is advancing research and measurement science and is developing guidelines for safety evaluations and risk mitigations. NIST is also collaborating with international partners and industry stakeholders on AI standards. NIST is also taking the lead on guidance and best practices for AI, including generative AI.
- **Regulatory Agencies:** Federal agencies are enforcing existing rules that can apply to AI. However, this enforcement may be complicated by the Supreme Court's June 2024 decision in *Loper Bright Enterprises v. Raimondo*, which overturned the *Chevron* Deference precedent.
- **Other Federal Agencies:** Some federal agencies are trying to lead by example, deploying AI alongside comprehensive risk management strategies. Others are limiting the use of AI until the technology improves and guardrails are established.

U.S. AI Regulators

Federal Trade Commission (FTC): Consumer protection, competition, unfair or deceptive practices, data privacy and security

Food and Drug Administration (FDA): AI/ML-enabled medical devices, safety, and effectiveness

Securities and Exchange Commission (SEC): AI in trading, disclosures, and compliance

Federal Aviation Administration (FAA): AI in unmanned aircraft systems and drones

Equal Employment Opportunity Commission (EEOC): AI in hiring, discrimination prevention

Consumer Financial Protection Bureau (CFPB): AI in lending, consumer protection

Federal Communications Commission (FCC): AI in communication technologies, spectrum management

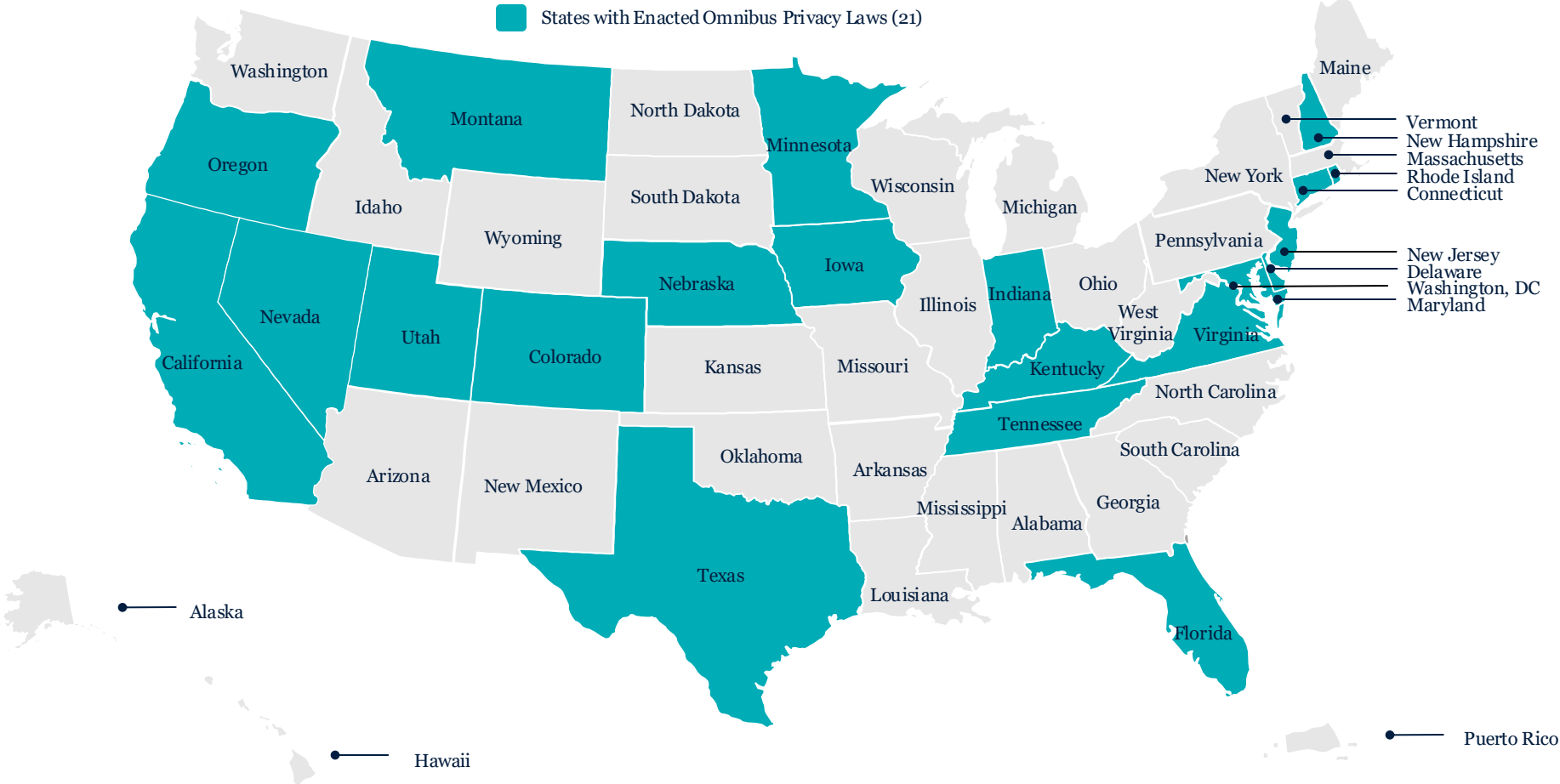
Department of Commerce (DOC): AI innovation, international trade and export requirements

Federal Energy Regulatory Commission (FERC): AI in energy grid management

Department of Health and Human Services (HHS): AI in health data management, public health surveillance

... and others

State Omnibus Privacy Laws as of November 1, 2024





AI (and other) Companies: Quietly Changing Your Terms of Service Could Be Unfair or Deceptive

By: Staff in the Office of Technology and The Division of Privacy and Identity Protection

Focus on California

- CCPA Update Jan. 2025:

(4) “Personal information” can exist in various formats, including, but not limited to, all of the following:

(A) Physical formats, including paper documents, printed images, vinyl records, or video tapes.

(B) Digital formats, including text, image, audio, or video files.

(C) Abstract digital formats, including compressed or encrypted files, metadata, or artificial intelligence systems that are capable of outputting personal information.

Focus on California



- Automated Decision-making Technology Rules
 - “Automated decisionmaking technology” or “ADMT” means any technology that processes personal information and uses computation to execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking.
 - “Profiling” means any form of automated processing of personal information to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person’s intelligence, ability, aptitude, performance at work, economic situation; health, including mental health; personal preferences, interests, reliability, predispositions, behavior, location, or movements.

Focus on California



- “Behavioral advertising” means the targeting of advertising to a consumer based on the consumer’s personal information obtained from the consumer’s activity—both across businesses, distinctly-branded websites, application, or services, and within the business’s own distinctly-branded websites, applications, or services.
 - Behavioral advertising includes cross-context behavioral advertising.
 - Behavioral advertising does not include nonpersonalized advertising, as defined by Civil Code section 1798.140, subdivision (t), provided that the consumer’s personal information is not used to build a profile about the consumer or otherwise alter the consumer’s experience outside the current interaction with the business, and is not disclosed to a third party.
 - The exceptions in the subsection do not apply to profiling for behavioral advertising as set forth in section 7200, subsection (a)(2)(C), or to training uses of automated decisionmaking technology as set forth in section 7200, subsection (a)(3). A business must provide the ability to opt-out of these uses of automated decisionmaking technology in all circumstances.

Data Privacy and AI: Practice Tips

1. Whose data is being used, who has the rights?
2. Is someone going to use your data to train an AI for others?
3. Is there “personal information” used in the system and what are my obligations?
4. Are the results what we expect?

What Is Political Advertising?

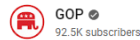
- Generally:
 - Paid advertisements
 - Relating to a clearly identified candidate or ballot measure and
 - Either:
 - A reasonable person would understand the ad to advocate for or against the identified candidate or ballot measure; or
 - The ad is paid for by a political committee (incl. candidate, party, PAC, super PAC, ballot measure committee, etc.)
- Not typically regulated by AI laws: unpaid advertising (e.g., organic social), lobbying campaigns (i.e., calling for official government action), general issue advertising
 - *But see* broadcast and platform-specific requirements

AI and Political Advertising

- **Tough to regulate deceptive uses of AI in political campaigns!**
- **Political speech is highly protected by the First Amendment; even *false* political speech may be protected**
 - Even if the government has a compelling interest in preventing misinformation in elections, laws must be narrowly tailored to achieve that end
 - “First Amendment protects the ‘civic duty’ to engage in public debate, with a preference for counteracting lies with more accurate information, rather than by restricting lies.”
 - **Compare: laws banning false political statements**
 - *U.S. v. Alvarez* (2012) – Invalidating federal Stolen Valor Act prohibiting one from claiming to win the Medal of Honor, rejecting the idea that false speech is never protected
 - *Susan B. Anthony List v. Driehaus* (6th Cir. 2016) – Striking down OH law prohibiting reckless false statements about candidates
 - **And: laws banning voter intimidation, voter fraud (false statements about when, where, how to vote that interfere with fundamental right to vote)**
 - *People v. Burkman* (Mich. 2024) (successful prosecution of individuals who financed robocall targeting Black voters asserting vote by mail would result in information becoming part of a public database that police would use to track down old warrants, credit card companies to collected debts, and CDC to track people for mandatory vaccines)
 - **With: laws requiring transparency (disclaimers, public disclosure)**

AI in Political Advertising

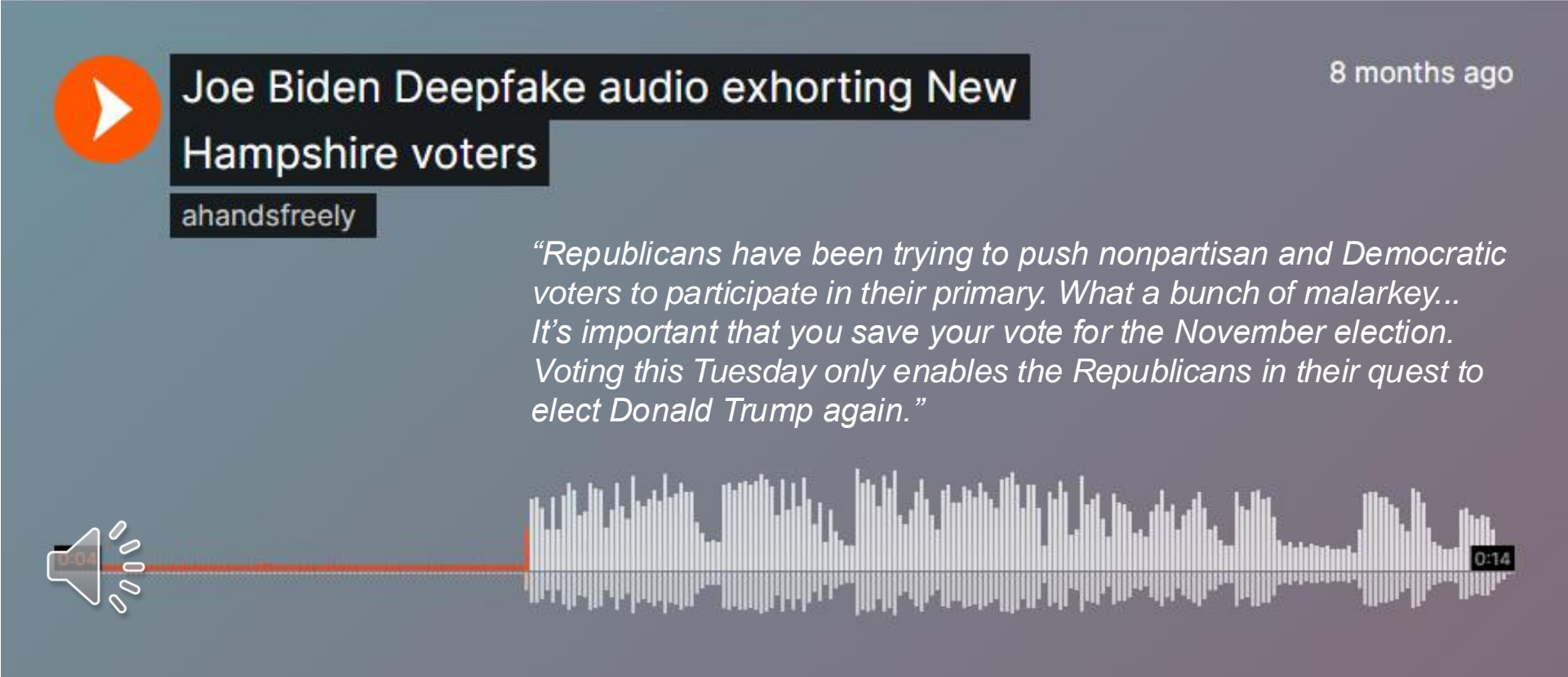
April 25, 2023



<https://www.youtube.com/watch?v=kLMMxgtxQ1Y>

AI and Political Advertising

January 22, 2024



The screenshot shows a video player interface. On the left, there is a red play button icon. The video title is "Joe Biden Deepfake audio exhorting New Hampshire voters" in white text on a dark background. Below the title is the channel name "ahandsfreely". In the top right corner of the player, it says "8 months ago". The main content area displays a quote in white italicized text: "Republicans have been trying to push nonpartisan and Democratic voters to participate in their primary. What a bunch of malarkey... It's important that you save your vote for the November election. Voting this Tuesday only enables the Republicans in their quest to elect Donald Trump again." Below the quote is a white audio waveform. On the left side of the waveform is a speaker icon with a red progress bar and a timestamp of "0:04". On the right side of the waveform is a timestamp of "0:14".

Joe Biden Deepfake audio exhorting New Hampshire voters

ahandsfreely

8 months ago

“Republicans have been trying to push nonpartisan and Democratic voters to participate in their primary. What a bunch of malarkey... It’s important that you save your vote for the November election. Voting this Tuesday only enables the Republicans in their quest to elect Donald Trump again.”

0:04 0:14



CNN Politics

SCOTUS

Congress

Facts First

2024 Elections

January 24, 2024

The deepfake era of US politics is upon us

AI and Political Advertising

New Hampshire Officials to Investigate A.I. Robocalls Mimicking Biden

The calls, in a voice most likely artificially generated, urged people not to vote in Tuesday's primary.

Political consultant behind AI-generated Biden robocalls faces \$6 million fine and criminal charges

Telecom company agrees to \$1M fine over Biden deepfake

Federal authorities hope the settlement will deter the deceptive use of AI-generated impersonations of political figures and others.

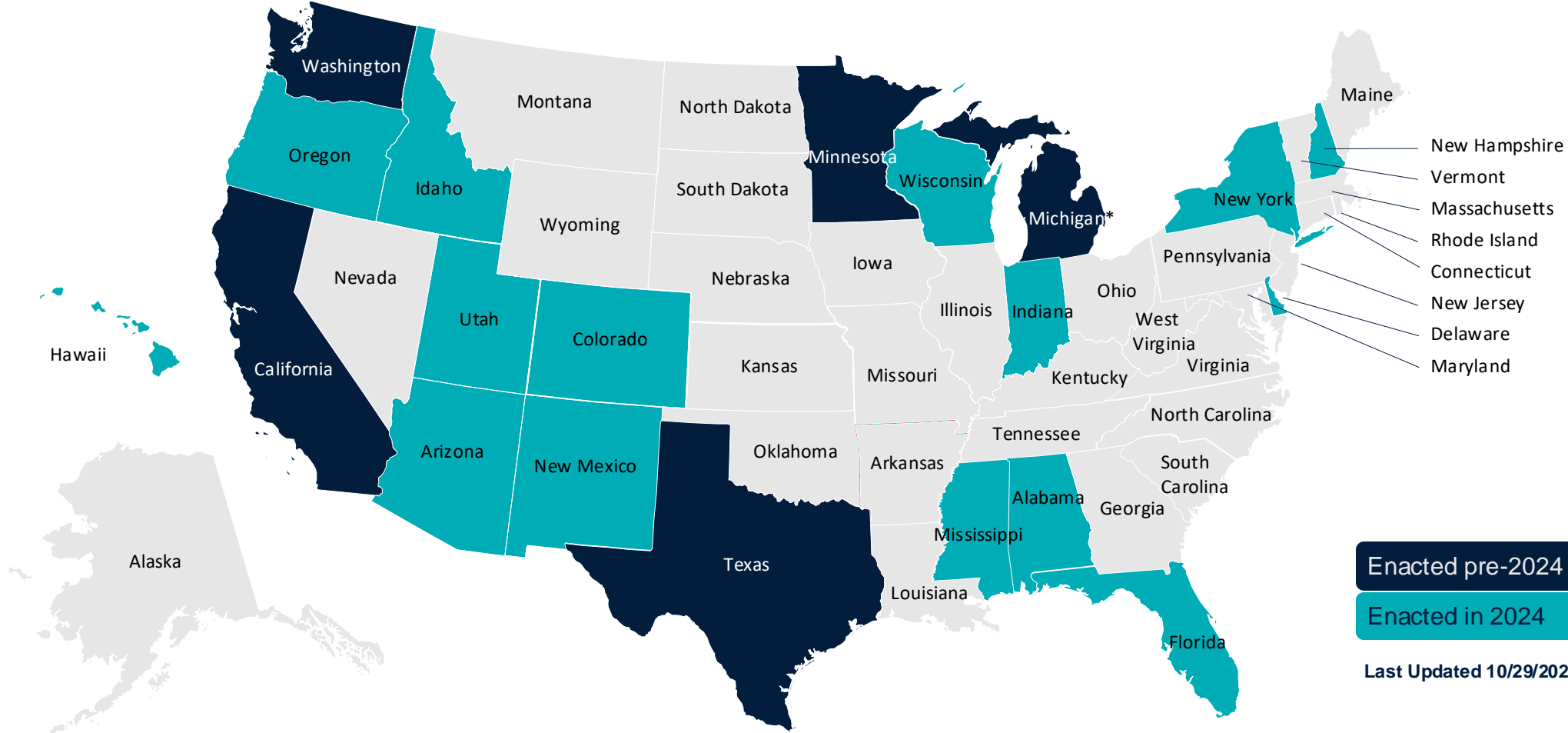
State Laws on AI in Political Advertising: 2023



Enacted pre-2024

Last Updated 10/29/2024

State Laws on AI in Political Advertising: Today



AI and Political Advertising

- **Approach 1:** Outright Bans on use of AI in political advertising
 - TX, MN, NH, CA
- **Approach 2:** Labeling/Disclaimers
 - Most common (more likely to survive strict scrutiny)
 - Generally require those responsible for “distributing” ads to include disclaimers that flag materially deceptive content to viewers
 - Content is often considered “materially deceptive” if it depicts a person doing or saying something that did not happen in reality in a way that a reasonable person would believe to be true
 - Some have intent requirement (e.g., ad made with “actual malice”)
- **Approach 3:** Existing laws cover new technologies

Outstanding Questions

- Who is liable? Payor vs. distribution platform?
- How does it interact with existing or future federal laws?
 - FCA – No censorship of candidate materials; Section 230 – no liability for censorship of third-party content





PAID FOR BY MIKE BRAUN FOR INDIANA. APPROVED BY MIKE BRAUN.
ELEMENTS OF THIS MEDIA HAVE BEEN DIGITALLY ALTERED OR ARTIFICIALLY GENERATED.

AI and Political Advertising



Where's the Federal Government on This?

- **FCC and FEC:** Existing laws cover new technologies
 - *Ex:* FCC says TCPA regulation of artificial voice recordings covers AI-generated voices
 - *Ex:* FEC says existing laws prohibiting impersonation prohibit AI-generated impersonation (“FECA is technology neutral”); can’t do more without congressional action
- **FCC:** Labeling/Disclaimers
 - *Ex:* Pending bills in Congress; pending NPRM at FCC (broadcast, radio, phone)
- **Congress:** Multiple proposals pending in current Congress to ban uses of AI or require labeling/disclaimers
 - Political will to pass now?

AI in Political Advertising: Practice Tips

1. Is the proposed ad “political”?
 - Who has obligation to assess? Advertiser, distribution platform?
2. To what election does it relate? (Fed, state, local)
3. Does that jurisdiction have limits on AI (or other political ad restrictions) and do they apply?
 - See also laws around “Paid for by...” disclaimers, recordkeeping, and reporting
4. Is this ad materially deceptive?
 - Consider substantiation processes for images, video, and audio
5. Reputational considerations

Questions?

VENABLE LLP



Melissa Landau Steinman

Partner

+1 202.344.4972

mlsteinman@Venable.com



Justin E. Pierce

Partner

+1 202.344.4442

jpierce@Venable.com



Rob Hartwell

Partner

+1 202.344.4663

rlhartwell@Venable.com



Meredith K. McCoy

Partner

+1 202.344.4571

mkmccoy@Venable.com



© 2024 Venable LLP.

This document is published by the law firm Venable LLP. It is not intended to provide legal advice or opinion. Such advice may only be given when related to specific fact situations that Venable has accepted an engagement as counsel to address.

VENABLE LLP