Agenda for AI and Data Regulation Panel

Panelist

Rob Bonta | California Attorney General

Moderator

Janet Kim, Partner (former White House Counsel attorney) Freshfields

Frank Partnoy, Professor of Law University of California, Berkeley

California Attorney General Issues Legal Advisories on AI Compliance with State Laws

- Consumer Protection and Civil Rights Obligations
  - Bias and Discrimination
  - Transparency
  - Privacy Compliance
- Healthcare Sector-Specific Guidance
  - Patient Transparency
  - Testing and Validation
  - Privacy Protections
- Legislative Developments
  - Disclosure Requirements
  - Unauthorized Use of Likeness
  - Election Integrity
  - Prohibitions on Harmful Practices
- Practical Steps for Businesses
  - Conduct of Comprehensive Audits

    - Implement Bias Mitigation Strategies
    - Enhance Transparency Practices
    - Train Employees

AG's Legal Advisory on the Application of Existing California Laws to Artificial Intelligence

- AI Holds Great Potential and Great Risks
- CA's Consumer Protection, Civil Rights and Competition Laws Provide Broad Protections
    - CA Unfair Labor Competition Law
    - CA False Advertising Law
    - CA Competition Laws
    - CA Civil Rights Laws
    - CA Election Misinformation Prevention Laws
- Data Protection Laws Provide Additional Broad Protections for Californians
- New CA AI Laws
    - Disclosure Requirements for Businesses
    - Unauthorized Use of Likeness in the entertainment Industry and Other Contexts
    - Use of AI in Election and Campaign Materials
    - Expanded Prohibitions and Reporting of Exploitative Uses of AI
    - Supervision of AI Tools in Healthcare Settings

More California Privacy Rules: California Agency Issues Proposed Regulations on Automated Decisionmaking, Cybersecurity Audits, and Risk Assessments

- New Proposed Rules for Automated Decisionmaking Technology
- Cybersecurity Audits
- Risk Assessments
- Next Steps

California's Legislative Push on AI: A Wave of New Obligations and Prohibitions

- Enacted AI Legislation
    - Election Integrity and Disinformation in the Age of AI
    - Transparency in AI Development and Use
    - Consumer Privacy and AI Transparency
    - Protections Against AI-Generated Harmful Sexual Content
    - Regulation of AI in Specific Sectors
        - Healthcare and Insurance
        - Education
        - Telemarketing
        - Government Agencies
- Vetoed Legislation: SB 1047
- Looking Forward: States Lead the Way in AI Regulation

The Rise of Audits as a Regulatory Tool for Tech

- Audits in Context
    - Internal Audits
    - External Audits
    - Regulator-Driven Information Gathering
- Why audits?
    - Accountability and Transparency
    - Cost Effectiveness
    - Standardization
- DSA and OSA Audits
- Auditing AI Systems
- Other Digital Regulation with Audit Requirements
- Practical Tips for Tech Businesses

- Advocate Thoughtfully
- Prepare for Audit Obligations
- Plan for Adverse Outcomes
- Leverage Audit Insights

FRESHFIELDS

January 24, 2025 | 3 minute read

California Attorney General Issues Legal Advisories on AI Compliance with State Laws


Beth George
Partner


Sean Quinn
Counsel


Madeline Cimino
Associate

On January 13, 2025, California Attorney General Rob Bonta released two legal advisories addressing how existing state laws apply to artificial intelligence (AI). "The fifth-largest economy in the world is not the wild west; existing California laws apply to both the development and use of AI," said Attorney General Bonta. These advisories provide guidance to businesses, healthcare entities, and other organizations utilizing AI, ensuring compliance with California's consumer protection, civil rights, and healthcare regulations. As AI becomes more prevalent in daily operations and decision-making processes, these legal advisories clarify how existing laws apply to AI systems, reinforcing the importance of ethical and transparent practices.

Consumer Protection and Civil Rights Obligations

The first advisory, titled "Application of Existing California Laws to Artificial Intelligence," emphasizes that AI systems must align with state laws designed to protect consumers and prevent discrimination. Key points include:

- **Bias and Discrimination:** Businesses must ensure that their AI systems do not perpetuate or exacerbate biases, particularly those that could negatively impact protected groups. California's anti-discrimination laws, including the Unruh Civil Rights Act, mandate that businesses provide equitable access and treatment regardless of race, gender, or other protected characteristics.
- **Transparency:** Companies must disclose when AI tools are used in decisions that affect consumers' rights or access to services. This ensures consumers are informed and able to exercise their legal rights effectively.
- **Privacy Compliance:** The advisory clarifies that AI applications must adhere to privacy laws such as the California Consumer Privacy Act (CCPA) and its expanded successor, the California Privacy Rights Act (CPRA). These laws require organizations to limit the collection and use of personal data, obtain consumer consent, and provide mechanisms for individuals to opt out of automated decision-making.

The advisory warns that non-compliance may result in penalties under the Unfair Competition Law (UCL), which prohibits unfair or deceptive business practices. Businesses should proactively assess their AI systems to avoid these risks.

Healthcare Sector-Specific Guidance

The second advisory, "Application of Existing California Laws to Artificial Intelligence in Healthcare," addresses the use of AI in medical settings and highlights:

- **Patient Transparency:** Healthcare providers are required to notify patients when AI technologies are used in diagnostic or

treatment decisions. This fosters trust and allows patients to make informed decisions about their care.

- **Testing and Validation:** Rigorous testing and validation of AI systems are essential to prevent errors and reduce the likelihood of harm. This includes ensuring that training data is free from biases that could compromise the accuracy or fairness of AI-driven medical tools.
- **Privacy Protections:** AI systems used in healthcare must comply with the Confidentiality of Medical Information Act (CMIA) and the Health Insurance Portability and Accountability Act (HIPAA). These laws impose stringent requirements for safeguarding patient data and ensuring its secure use.

The advisory also emphasizes ongoing monitoring of AI systems to address emerging risks affecting patient outcomes or legal compliance.

Legislative Developments

In addition to reiterating the applicability of existing laws, the advisories highlight new legislative measures that took effect on January 1, 2025, aimed at regulating the use of AI across industries. These measures include:

- **Disclosure Requirements:** Businesses are now required to clearly disclose when AI systems are employed, particularly in applications that influence consumer decisions or personal rights.
- **Unauthorized Use of Likeness:** California law prohibits the use of AI to create replicas of individuals' likenesses without their explicit consent. This protects against exploitation and unauthorized commercial use.
- **Election Integrity:** New laws restrict the use of AI in campaign and election-related materials to prevent misinformation and manipulation.
- **Prohibitions on Harmful Practices:** Regulations explicitly target exploitative or harmful uses of AI, such as systems

designed to mislead consumers or unfairly target vulnerable populations.

Practical Steps for Businesses

The advisories provide a roadmap for organizations seeking to align their AI practices with California's legal standards. Key recommendations from the Attorney General include:

1. **Conduct Comprehensive Audits:** Regularly review AI systems, and the process to develop them, to ensure they comply with applicable laws, including anti-discrimination, privacy, and transparency requirements.
2. **Implement Bias Mitigation Strategies:** Use diverse datasets and robust testing protocols to identify and address potential biases in AI algorithms.
3. **Enhance Transparency Practices:** Develop clear and accessible communication strategies to inform consumers and patients about the role of AI in decision-making processes.
4. **Train Employees:** Provide training for staff on the ethical and legal implications of AI use, ensuring they understand their obligations under California law.
5. **Engage Legal Counsel:** Work with legal experts to navigate the complexities of AI compliance and stay ahead of evolving regulatory requirements.

Conclusion

The Attorney General's advisories serve as an important reminder that compliance with state laws is an evolving challenge, and existing laws apply with equal force to new technologies. Companies that implement measures to align with these requirements will mitigate legal risks and support long-term stability in the evolving AI-driven economy.

CALIFORNIA ATTORNEY GENERAL'S LEGAL ADVISORY ON THE APPLICATION OF EXISTING CALIFORNIA LAWS TO ARTIFICIAL INTELLIGENCE

The California Attorney General's Office (AGO) issues this advisory to provide guidance to consumers and entities that develop, sell, and use artificial intelligence (AI)[1] about their rights and obligations under California law, including under the state's consumer protection, civil rights, competition, and data privacy laws.[2]

ARTIFICIAL INTELLIGENCE HOLDS GREAT POTENTIAL AND GREAT RISKS

AI systems are at the forefront of the technology industry, and hold great potential to achieve scientific breakthroughs, boost economic growth, and benefit consumers. As home to the world's leading technology companies and many of the most compelling recent developments in AI, California has a vested interest in the development and growth of AI tools. The AGO encourages the responsible use of AI in ways that are safe, ethical, and consistent with human dignity to help solve urgent challenges, increase efficiencies, and unlock access to information—consistent with state and federal law.

While AI tools present new opportunities, the use of AI can run the risk of exacerbating bias, discrimination, and the spread of disinformation, creating opportunities for fraud and causing harm to California's people, institutions, infrastructure, economy, and environment. For AI systems to achieve their positive potential without doing harm, they must be developed and used ethically and legally. Existing California law provides a host of protections that may be applicable to the development and use of AI tools.

Consumers must have visibility into when and how AI systems are used to impact their lives and whether and how their information is being used to develop and train systems. Developers and entities that use AI, including businesses, nonprofits, and government, must ensure that AI systems are tested and validated, and that they are audited as appropriate to ensure that their use is safe, ethical, and lawful, and reduces, rather than replicates or exaggerates, human error and biases. Developers and users must understand any risks involved in the use of AI, and ensure that AI is not used in a manner that causes harm to individuals, entities, infrastructure, competition, or the environment, or to the public at large.

AI systems are proliferating at an exponential rate and already affect nearly all aspects of everyday life. Businesses are using AI systems to evaluate consumers' credit risk and guide loan decisions, screen tenants for rentals, and target consumers with ads and offers. AI systems are also used in the workplace to guide employment decisions, in educational settings to provide new learning systems, and in healthcare settings to inform medical diagnoses. But many consumers are not aware of when and how AI systems are used in their lives or by institutions that they rely on. Moreover, AI systems are novel and complex, and their inner workings are often not understood by developers and entities that use AI, let alone consumers. The rapid deployment of such tools has resulted in situations where AI tools have generated false information or biased and discriminatory results, often while being represented as neutral and free from human bias.

Entities that develop or use AI systems must ensure that they and their systems comply with California law, including laws protecting consumers from unfair and fraudulent business practices, anticompetitive harm, discrimination

1 While the definition of AI may vary depending upon the context, for the purposes of this advisory, AI includes "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—(A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; and (C) use model inference to formulate options for information or action." (15 U.S.C. § 9401(3).) California has also recently passed a law defining the term in certain instances as "an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments." (See Gov. Code § 11546.45.5 et seq., added by AB 2885, Stats. 2024, ch. 843.)

2 This advisory provides the AGO's guidance on general application of California law to AI. This advisory does not address all potential violations or avenues of enforcement for the identified laws, nor does it identify all laws that may apply to AI.

and bias, and abuse of their data. Businesses must understand how the AI systems they utilize are trained, what information the systems consider, and how the systems generate output. They must also understand that they can be held accountable under tort, contract, or other laws if the employment of AI results in harm, particularly when AI systems are employed negligently or in use cases that could entail a level of risk. Developers and users of AI must also be transparent with consumers about whether consumer information is being used to train AI and how they are using AI to make decisions affecting consumers.

California's Consumer Protection, Civil Rights, and Competition Laws Provide Broad Protections

A. California's Unfair Competition Law

California's Unfair Competition Law protects the state's residents against unlawful, unfair, or fraudulent business acts or practices. (Bus. & Prof. Code, § 17200 et seq.) The law was intentionally written with broad, sweeping language to protect Californians from obvious and familiar forms of fraud and deception as well as new, creative, and cutting-edge forms of unlawful, unfair, and misleading behavior. (*People ex rel. Mosk v. Nat'l Research Co.* (1962) 201 Cal. App.2d 765, 772.) AI provides new tools for businesses and consumers alike, and also creates new opportunity to deceive Californians. Practices that deceive or harm consumers fall squarely within the purview of the Unfair Competition Law, and developers, entities that use AI, and end-users of AI systems should be aware that traditional consumer legal protections apply equally in the AI context.

In addition to prohibiting consumer deception, the Unfair Competition Law makes a violation of any other state, federal, or local law "independently actionable" under the Unfair Competition Law. (*Farmers Ins. Exchange v. Superior Court* (1994) 2 Cal.4th 377, 383.) Thus, the scope of the Unfair Competition Law is broad and incorporates numerous laws that may apply to AI in a variety of contexts.

For example, it may be unlawful under California's Unfair Competition Law to:[3]

- Falsely advertise the accuracy, quality, or utility of AI systems. This includes claiming that an AI system has a capability that it does not; representing that a system is completely powered by AI when humans are responsible for performing some of its functions; representing that humans are responsible for performing some of a system's functions when AI is responsible instead; or claiming without basis that a system is accurate, performs tasks better than a human would, has specified characteristics, meets industry or other standards, or is free from bias. (See, e.g., Bus. & Prof. Code, § 17500 et seq.; Civ. Code, § 1770 [The Consumer Legal Remedies Act].)

- Use AI to foster or advance deception. For example, the creation of deepfakes, chatbots, and voice clones that appear to represent people, events, and utterances that never existed or occurred would likely be deceptive.[4] Likewise, in many contexts it would likely be deceptive to fail to disclose that AI has been used to create a piece of media.

- Use AI to create and knowingly use another person's name, voice, signature, photograph, or likeness without that person's prior consent. (Civ. Code, §§ 3344, 3344.1; see also Civ. Code, § 1708.86 [prohibiting the creation and disclosure of sexually explicit material without the depicted person's consent]).[5]

- Use AI to impersonate a real person for purposes of harming, intimidating, threatening, or defrauding another person. (Pen. Code, § 528.5.)

- Use AI to impersonate a real person for purposes of receiving money or property. (Pen. Code, § 530; see also Pen. Code, § 529 [false personation of another in private or official capacity while doing specified acts].)

3 Many of the specific statutes listed in this advisory also provide for a private right of action.

4 See Michael Atleson, *Chatbots, deepfakes, and voice clones: AI deception for sale*, Federal Trade Commission Business Blog (Mar. 20, 2023), https://www.ftc.gov/business-guidance/blog/2023/03/chatbots-deepfakes-voice-clones-ai-deception-sale.

5 Additional requirements for the use of AI in this context will go into effect on January 1, 2025—AB 2602 (Kalra) and AB 1836 (Bauer-Kahan)—and are described at page 8 below.

- Use AI to impersonate a real person for any unlawful purpose. (Pen. Code, § 530.5 [identity theft]; Pen. Code, § 530.55 [personal identifying information includes unique biometric data including fingerprint, facial scan identifiers, voiceprint, retina or iris image, or other unique physical representation]; see also *People v. Bollaert* (2016) 248 Cal.App.4th 699, 711-12 [unlawful purpose for identity theft includes intentional civil torts including invasion of privacy].)

- Use AI to impersonate a government official in the execution of official duties. (See Pen. Code, § 538d [impersonating a peace officer]; Pen. Code, § 146a [impersonating a state officer while committing specified acts]; Pen. Code, § 538f [impersonating a public utility officer]; Pen. Code, § 538g [impersonating a state/county/city/special district/city or county officer or employee].)

- Use AI in a manner that is unfair, including using AI in a manner that results in negative impacts that outweigh its utility, or in a manner that offends public policy, is immoral, unethical, oppressive, or unscrupulous, or causes substantial injury.

- Create, market, or disseminate an AI system that does not comply with federal or state laws, including the false advertising, civil rights, and privacy laws described below, as well as laws governing specific industries and activities.

Businesses may also be liable for supplying AI products when they know, or should have known, that AI will be used to violate the law. (See, e.g., *People v. Toomey* (1984) 157 Cal.App.3d 1, 15 [liability under section 17200 can be imposed for aiding and abetting].)

B. California's False Advertising Law

California's False Advertising Law provides another layer of protection for California's citizens against deceptive advertising. (Bus. & Prof. Code, § 17500 et seq.) The False Advertising Law "broadly prohibit[s] false or misleading advertising, declaring that it is unlawful for any person or business to make or distribute any statement to induce the public to enter into a transaction 'which is untrue or misleading, and which is known, or which by exercise of reasonable care should be known, to be untrue or misleading.'" (*Nationwide Biweekly Administration, Inc. v. Superior Court* (2020) 9 Cal.5th 279, 306 [quoting Bus. & Prof. Code, § 17500].) The law would prohibit false advertising regarding the capabilities, availability, and utility of AI products, the use of AI in connection with a good or service, as well as false advertising regarding any topic, whether or not it is generated by AI.

C. California's Competition Laws

California's competition laws, including the Cartwright Act, which prohibits anticompetitive trusts (Bus. & Prof. Code, § 16720), and the Unfair Practices Act, which regulates practices such as below-cost sales and loss leaders, protect California's economy. (Bus. & Prof. Code, § 17000 et seq.) The Unfair Competition Law, discussed above, also prohibits acts and practices that violate antitrust laws, among other practices. This includes, but is not limited to, conduct that threatens an incipient violation of an antitrust law, that violates the policy or spirit of one of those laws because its effects are comparable to a violation of the law, or that otherwise significantly threatens or harms competition.

AI developers and users should be aware of any risks to fair competition created by AI systems, such as those that set pricing. Even inadvertent harm to competition resulting from AI systems may violate one or more of California's competition laws. Anticompetitive actions by dominant AI companies may also harm competition in AI markets and violate both state and federal competition laws.

D. California's Civil Rights Laws

California's Unruh Civil Rights Act protects the freedom and equality of all people within the state, "no matter what their sex, race, color, religion, ancestry, national origin, disability, medical condition, genetic information, marital status, sexual orientation, citizenship, primary language, or immigration status." (Civ. Code, § 51.) The California Fair Employment and Housing Act (FEHA) also protects Californians from harassment or discrimination in employment or housing based on a number of protected characteristics, including sex, race, disability, age, criminal history, and veteran or military status. (Gov. Code, § 12900 et seq.) Businesses may be liable for FEHA-prohibited discriminatory screening carried out by an agent, and further, the agents themselves may be directly liable to the individuals who

were discriminated against. (See *Raines v. U.S. Healthworks Medical Grp.* (2023) 15 Cal.5th 268, 291.) And Section 11135 prohibits denial of full and equal access to the benefits of, or discrimination under, any program or activity receiving state funds. (Gov. Code, § 11135.) This includes practices that, regardless of intent, have an adverse or disproportionate impact on members of a protected class, or create, reinforce, or perpetuate discrimination or segregation of members of a protected class. (Cal. Code of Regs., tit. 2, § 14027.)

We have seen AI systems incorporate societal and other biases into their decision-making.[6] Developers and users of AI should be wary of these potential biases that may be unlawfully impacting Californians.[7] Other laws also require that entities that take adverse action against citizens provide specific reasons for those adverse actions, including when AI was used to make the determination. As one example, the federal Fair Credit Reporting Act and Equal Credit Opportunity Act, as well as the California Consumer Credit Reporting Agencies Act, require such specific reasons be provided to Californians who receive adverse actions based on their credit scores. (See 15 U.S.C. § 1681 et seq.; 15 U.S.C. § 1691 et seq.; Civ. Code, § 1785.1 et seq.) The Consumer Financial Protection Bureau recently clarified that creditors who use AI or complex credit models must still provide individuals with specific reasons when they deny or take another adverse action against an individual.[8]

E. California's Election Misinformation Prevention Laws[9]

California law also provides guidance on a number of scenarios in which the use of AI may be illegal in the context of elections.[10] California law prohibits the use of undeclared chatbots with the intent to mislead a person about its artificial identity in order to incentivize a purchase or influence a vote in an election. (Bus. & Prof. Code, § 17941.) It is also impermissible to use AI to impersonate a candidate for elected office, or a candidate or initiative's website (Elec. Code, § 18320),[11] and to use AI to distribute, with actual malice, materially deceptive audio or visual media of a candidate for elective office within 60 days of that candidate's election with the intent to injure the candidate's reputation or deceive a voter into voting for or against the candidate. (Elec. Code, § 20010.)

6 See, e.g., Press Release, California Office of the Attorney General, Attorney General Bonta Launches Inquiry into Racial and Ethnic Bias in Healthcare Algorithms (Aug. 31, 2022), https://oag.ca.gov/news/press-releases/attorney-general-bonta-launches-inquiry-racial-and-ethnic-bias-healthcare; Press Release, California Office of the Attorney General, Attorney General Bonta Welcomes Biden Administration's Effort to Increase Transparency, Combat Bias in Healthcare Algorithms (June 20, 2023), https://oag.ca.gov/news/press-releases/attorney-general-bonta-launches-inquiry-racial-and-ethnic-bias-healthcare.

7 See, e.g., National Institute of Science and Technology, *There's More to AI Bias Than Biased Data, NIST Report Highlights* (Mar. 16, 2022), https://www.nist.gov/news-events/news/2022/03/theres-more-ai-bias-biased-data-nist-report-highlights.

8 Consumer Financial Protection Circular 2023-03 (Sept. 19, 2023), https://www.consumerfinance.gov/compliance/circulars/circular-2023-03-adverse-action-notification-requirements-and-the-proper-use-of-the-cfpbs-sample-forms-provided-in-regulation-b/.

9 For more on Californians' voting rights, see Press Release, Ahead of General Election, Attorney General Bonta and Secretary of State Weber Remind Californians of Voting Rights and Advise Law Enforcement of Laws to Protect Voters (Oct. 3, 2024), https://oag.ca.gov/news/press-releases/ahead-general-election-attorney-general-bonta-and-secretary-state-weber-remind; see also California Department of Justice Law Enforcement Bulletin, Protecting California Voters from Election Interference and Voter Intimidation and Deception (Oct. 4, 2024), https://oag.ca.gov/system/files/attachments/press-docs/2024-dle-11.pdf.

10 For a description of new AI-related election laws see the discussion of AB 2355 (Carrillo) and AB 2655 (Berman) at page 8.

11 See Press Release, California Office of the Attorney General, Attorney General Bonta: Using Robocalls to Spread Disinformation is Unacceptable (Feb. 5, 2024), https://oag.ca.gov/news/press-releases/attorney-general-bonta-using-robocalls-spread-disinformation-unacceptable.

Data Protection Laws Provide Additional Broad Protections for Californians

Data is the bedrock underlying the massive growth in AI, and Californians' broad privacy and data rights directly impact AI systems, whether through the data used to build and train AI, or through the information that may be exposed by AI outputs.

Californians possess a constitutional right to privacy that applies to both government and private entities. (*Hill v. National Collegiate Athletic Assn.* (1994) 7 Cal.4th 1, 20.) Informational privacy, i.e., the "interest in precluding the dissemination or misuse of sensitive and confidential information" is a core privacy interest protected by the California Constitution. (*Id.* at 35.) Developers and entities that use AI must carefully monitor AI systems' training data, inputs, and outputs to ensure that Californians' constitutional right to privacy is respected.

The California Consumer Privacy Act (CCPA) broadly regulates the collection, use, sale, and sharing of consumers' personal information, including heightened protections for sensitive personal information. Personal information may also include inferences about consumers made by AI systems. (See Civ. Code, § 1798.140(v).) CCPA grants consumers important rights:

- The right to know about the personal information a business collects about them, and how it is used and shared;
- The right to correct inaccurate personal information that a business has about them;
- The right to delete personal information collected about them (with some exceptions);
- The right to opt out of the sale or sharing of their personal information; and
- The right to limit the use and disclosure of their sensitive personal information. (*Id.* § 1798.100 et seq.)

AI developers and users that collect and use Californians' personal information must comply with CCPA's protections for consumers, including by ensuring that their collection, use, retention, and sharing of consumer personal information is reasonably necessary and proportionate to achieve the purposes for which the personal information was collected and processed. (*Id.* § 1798.100.) Businesses are prohibited from processing personal information for non-disclosed purposes, and even the collection, use, retention, and sharing of personal information for disclosed purposes must be compatible with the context in which the personal information was collected. (*Ibid.*) AI developers and users should also be aware that using personal information for research is also subject to several requirements and limitations. (*Id.* § 1798.140(ab).) A new bill signed into law in September 2024 confirms that the protections for personal information in the CCPA apply to personal information in AI systems that are capable of outputting personal information. (Civ. Code, § 1798.140, added by AB 1008, Stats. 2024, ch. 804.) A second bill expands the definition of sensitive personal information to include "neural data." (Civ. Code, § 1798.140, added by SB 1223, Stats. 2024, ch. 887.)

The California Invasion of Privacy Act (CIPA) may also impact AI training data, inputs, or outputs. CIPA restricts recording or listening to private electronic communication, including wiretapping, eavesdropping on or recording communications without the consent of all parties, and recording or intercepting cellular communications without the consent of all parties. (Pen. Code, § 630 et seq.) CIPA also prohibits use of systems that examine or record voice prints to determine the truth or falsity of statements without consent. (*Id.* § 637.3.) Developers and users should ensure that their AI systems, or any data used by the system, do not violate CIPA.

California law contains heightened protection for particular types of consumer data, including education and healthcare data that may be processed or used by AI systems. The Student Online Personal Information Protection Act (SOPIPA) broadly prohibits education technology service providers from selling student data, engaging in targeted advertising using student data, and amassing profiles about students, except for specified school purposes. (Bus. & Prof. Code, § 22584 et seq.) SOPIPA applies to services and apps used primarily for "K-12 school purposes." This includes services and apps for home or remote instruction, as well as those intended for use at a public or private school. Developers and users should ensure any educational AI systems comply with SOPIPA, even if they are marketed directly to consumers.

Finally, the Confidentiality of Medical Information Act (CMIA) governs the use and disclosure of Californians' medical information and applies to businesses that offer software or hardware to consumers for the purposes of managing

medical information, or for diagnosis treatment, or management of medical conditions, including mobile applications or other related devices. (Civ. Code, § 56 et seq.) The rise of mental health and reproductive apps led to recent amendments to clarify that mental health and reproductive or sexual health digital services, such as apps and websites, are subject to the requirements of CMIA. Developers and users should ensure that any AI systems used for healthcare, including direct-to-consumer services, comply with the CMIA.

New California AI Laws

California has recently enacted the following legislation, effective January 1, 2025,[12] which addresses the use of AI and has broad impact for businesses and individuals:

Disclosure Requirements for Businesses

- **AB 2013 (Irwin**) requires AI developers to disclose information on their websites about their training data on or before January 1, 2026, including a high-level summary of the datasets used in the development of the AI system or service. (Civ. Code, § 3110 et seq.)
- **AB 2905 (Low)** requires telemarketing calls that use AI-generated or significantly modified synthetic marketing to disclose that use. (Pub. Util. Code, § 2874.)
- **SB 942 (Becker)** places obligations on AI developers, starting January 1, 2026, to make free and accessible tools to detect whether specified content was generated by generative AI systems. These developers are required to offer visible markings on AI-generated content to identify it as such and other detection features. (Bus. & Prof. Code, § 22757 et seq.)

Unauthorized Use of Likeness in the Entertainment Industry and Other Contexts

- **AB 2602 (Kalra)** requires that contracts authorizing the use of an individual's voice and likeness in a digital replica created through AI technology include a "reasonably specific description" of the proposed use and that the individual be represented by legal counsel or by a labor union. Absent these requirements, the contract is unenforceable, unless the uses are otherwise consistent with the terms of the contract and the underlying work. (Lab. Code, § 927.)
- **AB 1836 (Bauer-Kahan)** prohibits the use of a deceased personality's digital replica without prior consent within 70 years of the personality's death, imposing a minimum $10,000 fine for the violation. A deceased personality is any natural person whose name, voice, signature, photograph, or likeness has commercial value at the time of that person's death, or because of that person's death. (Civ. Code, § 3344.1.)

Use of AI in Election and Campaign Materials

- **AB 2355 (Carrillo)** requires any campaign advertisements generated or substantially altered using AI to include the following disclosure: "Ad generated or substantially altered using artificial intelligence." (Gov. Code, § 84504 et seq.)
- **AB 2655 (Berman)** requires that large online platforms (with at least one million California users) develop and implement procedures using state-of-the-art techniques to identify and remove certain materially deceptive election-related content—deepfakes—during specified periods before and after elections in California. It also requires certain additional content be labeled as manipulated, inauthentic, fake, or false during a longer period of time around elections in California. Platforms must provide an easy mechanism for California users to report the prohibited materials. (Code. Civ. Proc., § 35; Elec. Code, § 20510.)[13]

12 All bills discussed below become effective January 1, 2025. AB 2013 and SB 942 have additional operative dates, as specified, which determine when the laws impact covered entities and when violations of the provisions of the laws may be enforced.

13 A federal court has stayed enforcement of AB 2655 through June 28, 2025. (*Kohls v. Bonta* (E.D. Cal. Nov. 15, 2024, No. 2:24-cv-02527 JAM-CKD).) See also AB 2839 (Pellerin) prohibiting distribution of campaign or election-related materials that contain materially deceptive digital or audio media, including deepfake depictions of candidates, which was preliminarily enjoined by the same federal court on October 2, 2024. (*Ibid.* (Oct. 2, 2024).)

Expanded Prohibitions and Reporting of Exploitative Uses of AI

- **AB 1831 (Berman)** and **SB 1381 (Wahab)** expands existing criminal prohibitions on child pornography to include the use of AI in the creation of visual depictions of the sexual abuse and exploitation of children. (Pen. Code, §§ 311, 311.2, 311.3, 311.4, 311.11, 311.12, 312.3.)
- **SB 926 (Wahab)** extends criminal penalties to the creation of nonconsensual pornography using deepfake technology. (Pen. Code, § 647.)
- **SB 981 (Wahab)** requires social media platforms to provide a mechanism for California users to report sexually explicit digital identity theft or deepfake pornography. (Bus. & Prof. Code, § 22670 et seq.)

Supervision of AI Tools in Healthcare Settings

- **SB 1120 (Becker)** requires health insurers to ensure that licensed physicians supervise the use of AI tools that make decisions about healthcare services and insurance claims. (Health & Saf. Code, § 1367.01; Ins. Code, § 10123.135.)

Entities Should Remain Vigilant About Other Laws and Regulations Which May Be Applicable to AI Technologies

Beyond the laws and regulations discussed in this advisory, other California laws—including tort, public nuisance, environmental and business regulation, and criminal law—apply equally to AI systems and to conduct and business activities that involve the use of AI. Conduct that is illegal if engaged in without the involvement of AI is equally unlawful if AI is involved, and the fact that AI is involved is not a defense to liability under any law.

This overview is not intended to be exhaustive. Entities that develop or use AI have a duty to ensure that they understand and are in compliance with all state, federal, and local laws that may apply to them or their activities. That is particularly so when AI is used or developed for applications that could carry a potential risk of harm to people, organizations, physical or virtual infrastructure, or the environment.

FRESHFIELDS

November 26, 2024 | 5 minute read
Reposted from A Fresh Take

More California Privacy Rules: California Agency Issues Proposed Regulations on Automated Decisionmaking, Cybersecurity Audits, and Risk Assessments


Christine Lyon
Partner and Global Co-Head of Data Privacy and Security


Beth George
Partner


Megan Kayo
Partner

+4 more...

The California Privacy Protection Agency (CPPA) has opened the public comment period on its long-awaited proposed regulations on automated decisionmaking technology (ADMT), cybersecurity audits, privacy risk assessments, and general application of the CCPA to insurance companies (the "draft regulations"). If adopted in their current form, these draft regulations would impose substantial new obligations on companies subject to the California Consumer Privacy Act (CCPA), including detailed notice and procedural requirements for use of ADMT and formal cybersecurity

audit and/or privacy risk assessments for many covered businesses.

Below, we provide an overview of key topics in the current draft regulations and next steps.

New Proposed Rules for Automated Decisionmaking Technology

The draft regulations regarding automated decision-making technology ("ADMT") would apply to businesses using ADMT for "significant decisions" that have a "legal or similarly significant effect" on consumers. "Significant decisions" are defined by the draft regulations to include decisions related to essential goods and services and criminal justice, as well as opportunities related to financial services, lending, insurance, healthcare, housing, educational, employment, or independent contracting opportunities. Decisions affecting compensation or work status or that involve profiling in the workplace or educational settings, or profiling for use in targeted advertising and marketing, are also likely to fall within the ambit of the regulations.

The draft regulations would require businesses to provide a clear and conspicuous **Pre-use Notice** to consumers before using ADMT for such "significant decisions." This notice would, among other things:

- Explain that ADMT is being used and describe the purpose;
- Describe the logic or key parameters involved in the decision-making process;
- Describe what the ADMT is designed to output or generate (e.g. a numerical score) and how that will be used;
- Where applicable, explain the consumer's right to opt out or appeal the decision;
- Describe the consumers right to access ADMT (see below); and
- State that the business is prohibited from retaliating against a consumer for exercising any CCPA rights.

This Pre-use Notice address two other rights provided by the draft regulations. First, consumers must be given a **right to "access ADMT,"** meaning the right to an explanation of and relevant information about the ADMT. The information that must be provided significantly overlaps with the information required in the Pre-use Notice. Second, consumers must be provided a **right to opt-out of ADMT**, with limited exceptions, for example, where ADMT is used for fraud detection and prevention or where the business provides the consumer with an opportunity to appeal the decision to a human reviewer. Other exceptions may apply in defined circumstances, and regulated companies should consult counsel to ensure proper application of these exceptions when finalized. If the right to opt-out of ADMT applies, the business must provide at least two means for the consumer to opt out, including one via the primary medium through which the business interacts with the consumer (e.g. online via a link in the Pre-use Notice).

Finally, when a business is using physical or biological identification or profiling in its ADMT, it must conduct an evaluation to ensure that the ADMT works as intended and does not result in discrimination based on protected characteristics.

Cybersecurity Audits

The draft regulations would require covered businesses to conduct annual cybersecurity audits if they engage in activities where the "processing of consumers' personal information presents significant risk to consumers' security," including businesses that:

- Process personal information of 250,000 or more consumers or households or the sensitive personal information of 50,000 or more consumers; or
- Derive 50 percent or more of their annual revenue from selling or sharing consumers' personal information.

These audits would require use of a qualified, objective, independent auditor using generally accepted standards, such as those established by the National Institute of Standards and

Technology (NIST) or the International Organization for Standardization (ISO) to evaluate the adequacy of the business's technical, administrative, and physical safeguards for protecting personal information. These audits would need to include the name, affiliation and relevant qualifications of each auditory, as well as a certification that each auditor completed an independent, objective and impartial review and did not primarily rely on assertions or attestations by the business' management. These audits would need to be reported to the business' board, governing body, or highest-ranking executive responsible for the program. The scope of the audit includes, but is not limited to, authentication, encryption, zero trust architecture, access controls, asset inventory and management, vulnerability scans, penetration testing, network segmentation, oversight of service providers, and data retention schedules, as well as assessing the effectiveness of incident response, business continuity and disaster recovery protocols.

The findings of the audit must be documented in a report, which would need to assess the effectiveness of the business' cybersecurity program, identify any gaps and the measures taken to address those gaps, note the titles of the individuals responsible for the cybersecurity program, and include the date that the program was presented to the board, governing body, or highest-ranking executive responsible for the program. Businesses required to perform cybersecurity audits would be required to submit a written certification of completion to the CPPA annually.

Risk Assessments

The draft regulations would require many, if not most, businesses subject to the CCPA to undertake formal privacy-related risk assessments, and to submit annual certifications and documentation about these assessments to the CPPA.

Under the draft regulations, businesses subject to the CCPA would be required to conduct risk assessments for any of the following types of activities:

- "selling" personal information (within the broad meaning of this term under the CCPA) or "sharing" personal information for cross-contextual behavioral advertising;
- processing sensitive personal information (such as Social Security numbers or other government identifiers, health-related data, precise geolocation data, biometric data, and information about children under the age of 16);[1]
    - Even businesses that do not collect such information in the commercial context are likely to collect sensitive personal information in the employment context, such as Social Security numbers for tax reporting and citizenship or immigration status to verify right to work in the US. Thus, covered businesses with employees who are California residents are likely to need to perform privacy risk assessments in the employment context.
- using ADMT for a "significant decision" concerning a consumer or for "extensive profiling," as discussed above; or
- processing personal information to train ADMT or AI that is capable of being used to establish individual identity, for the generation of a deepfake, or for the operation of generative models, such as large language models.

Given the breadth of these covered activities (such as sales/sharing related to targeted advertising), it is likely that most CCPA-covered businesses would be required to perform regular risk assessments. These risk assessments would need to include detailed information about the processing, address a number of operational elements, and assess risks and safeguards. Additional requirements would apply to risk assessments for ADMT-related activities.

Businesses would need to perform risk assessments before initiating the covered processing activities, and to review and update them at least every 3 years—or immediately if there will be a material change in the processing. The draft regulations also detail requirements for annual certifications and submissions.

Next Steps

The public will have the opportunity to provide formal written comments through January 14, 2025, at 6 p.m. PST. The CPPA will also hold a virtual public hearing for oral comments on January 14, 2025.

[1] "Sensitive personal information" includes Social Security numbers or other government-issued identification numbers, health-related data, precise geolocation data, biometric or genetic data, racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, sexual orientation, union membership, account log-in credentials, contents of certain consumer communications unless the business is the intended recipient of the communication, and information about children under 16.

FRESHFIELDS

October 07, 2024 | 5 minute read
Reposted from A Fresh Take

California's Legislative Push on AI: A Wave of New Obligations and Prohibitions


Beth George
Partner


Janet Kim
Partner


Sean Quinn
Counsel

+2 more...

California Governor Gavin Newsom recently signed into law a wave of legislation – totaling 19 laws – addressing the opportunities and risks of AI and placing California at the forefront of AI regulation in the United States. From election integrity to performer rights and healthcare transparency, the state has enacted measures aimed at managing potential negative impacts of the AI boom. At the same time, Governor Newsom vetoed SB 1047, the most comprehensive bill on his desk, signaling his interest in balancing the need for regulation to promote the safe deployment of AI with an interest in fostering growth in this important new sector of the California tech economy.

Enacted AI Legislation:

These new laws, summarized and grouped by subject matter below, are a patchwork of regulation that is likely to grow and change over the coming months and years.

Election Integrity and Disinformation in the Age of AI: Recognizing risks posed by AI-generated disinformation in elections, California enacted three laws to address this emerging issue:

- AB 2655 (Defending Democracy from Deepfake Deception Act of 2024): Requires large online platforms to set up a reporting system and then to label or take down "materially deceptive content" AI-generated content 120 days before and after an election, and continue to label or takedown content for 60 days after an election where deceptive content calls into question the validity of the electoral process. The law also provides for enforcement options for the State AG and providing enforcement mechanisms for candidates and officials. Exemptions apply to certain media and satire.
- AB 2355: Mandates that audio, video, imaged based political ads generated or altered by AI carry a disclaimer, and outlining specific formatting requirements based on the advertising medium The Fair Political Practices Commission will enforce compliance.
- AB 2839[i]: Prohibits the malicious distribution of deceptive election materials, explicitly including AI-generated content, and expands the prohibition period consistent with AB 2665's 120- and 60-day periods. The law provides a private right of action for injunctive or equitable relief and fee-shifting for successful plaintiffs.

Transparency in AI Development and Use: California passed several laws addressing transparency in the development and use of AI:

- SB 942 (California AI Transparency Act): Requires developers of widely-used generative AI systems to provide a free AI detection tool for users and mandates both visible and hidden "watermark" disclosures on AI-generated content to improve transparency.

- AB 2013 (Artificial Intelligence Training Data Transparency Act): Imposes transparency requirements on generative AI developers to disclose the datasets used for training, including the data's origins and whether personal or copyrighted information is involved.
- AB 2885: Standardizes the definition of "artificial intelligence" across various California statutes, facilitating consistent application in state agencies, social media compliance, and education systems.

Consumer Privacy and AI Transparency: California has amended the California Consumer Privacy Act (CCPA) to close potential loopholes:

- AB 1008: Clarifies that the CCPA definition of "personal information" includes personal information which is within an AI system capable of outputting personal information.

Protections Against AI-Generated Harmful Sexual Content: Recognizing the potential for AI to generate harmful sexual content, California passed the following laws:

- AB 1831 and SB 1381: Clarifies and expands child pornography laws to include AI-generated child sexual abuse material, criminalizing the production, distribution, and possession of such content.
- SB 926: Criminalizes the creation or distribution of non-consensual, AI-generated intimate images, addressing the emotional harm caused by deepfake content.
- SB 981: Requires social media platforms to provide reporting mechanisms for California residents to report non-consensual sexually explicit digital identity theft, also known as deepfake pornography. The law requires online platforms to promptly investigate, report, and remove violative content, generally within 30 days and blocking the content during the pendency of the investigation.

Regulation of AI in Specific Sectors: In addition to the generally applicable laws above, the set of new laws addresses AI applications in specific sectors as well:

Healthcare and Insurance:

- AB 3030: Mandates disclosure of AI in patient communications and ensures patients have direct communication options with human providers.
- SB 1120: Requires health care plans using AI for reviewing patient care to base decisions on individual patient information, have licensed professionals make medical decisions, and ensure proper oversight of AI systems.

Education:

- AB 2876: Mandates the inclusion of AI literacy in California's curriculum frameworks for subjects such as mathematics, science, and history, preparing students for AI's role in everyday life.
- SB 1288: Establishes a working group tasked with guiding the use of AI in public schools, creating guidelines for safe AI use, and developing a model policy for responsible AI integration.
- AB 2602: Regulates the use of "digital replicas," AI-generated likenesses of performers, requiring explicit terms in a contract describing the intended use of the replica and that performers have legal representation.
- AB 1836: Prohibits the unauthorized commercial use of a deceased performer's digital replica, protecting postmortem publicity rights and requiring consent from their estate.

Telemarketing:

- AB 2905: Requires disclosures for the use of AI-generated voices in telemarketing calls.

Government Agencies:

- SB 896: Regulates the use of GenAI in California's state government, mandating notification of AI interactions in online interfaces or by phone, and risk analyses and reporting related to the benefits and risks of AI, especially as related to critical infrastructure.

Vetoed Legislation: SB 1047

One major piece of legislation that did not make it into law was SB 1047, which aimed to introduce stringent safety requirements for developers of large-scale AI models costing over $100 million to train. Key provisions included:

- Mandatory Safety and Security Protocols: Developers were required to implement and publish safety procedures, with access to be granted to the California Attorney General.
- Emergency Shutdown Capabilities: Developers needed to ensure their AI systems could be promptly shut down in emergencies.
- Risk Assessments: Developers were mandated to conduct pre-deployment risk assessments for potential harms and to review safety protocols annually.
- Whistleblower Protections: Provisions were included to protect employees who anonymously report safety violations.
- Know Your Customer (KYC) Obligations: Operators of computing clusters had to maintain records of customers using significant resources to train AI models.

Governor Newsom vetoed the bill, citing concerns that it applied stringent standards even to low-risk applications of AI, potentially stifling innovation. He also highlighted the need for adaptability and differentiated regulation, particularly when smaller developers could be disproportionately affected by broad mandates. The governor indicated that while public safety is paramount, future legislation should be informed by empirical data and should not unnecessarily hinder AI advancements.

Looking Forward: States Lead the Way in AI Regulation

As California enacts a diverse set of AI regulations, participants in the AI sector should remain vigilant about other emerging state-level legislation. With multiple states expanding their regulatory frameworks the patchwork of AI laws across the United States is

becoming increasingly complex, presenting both challenges and opportunities for shaping best practices and compliance postures. Staying informed and adaptable will be crucial for navigating the evolving landscape of AI governance and ensuring alignment with state-specific requirements. It's important that individuals, businesses, and other entities involved in the deployment of AI seek legal advice about the applicability and impact of such laws.

If you have questions about these or other laws affecting AI development and deployment, contact Beth George, Janet Kim, Sean Quinn, Madeline Cimino, Christine Chong, or other FBD attorneys that advise you.

[i] A majority of the provisions in AB 2839 were temporarily blocked from enforcement in California Federal Court on October 2, 2024 on constitutional grounds. Requirements pertaining to audio-only content remain enforceable.

FRESHFIELDS

February 25, 2025 | 6 minute read

The rise of audits as a regulatory tool for tech


Janet Kim
Partner


Matthew Bruce
Partner


Lutz Riede
Partner

+4 more...

As technology evolves, so do challenges in effectively regulating it. In an era where there is increasing focus on effective oversight of digital platforms, legislators are turning to audits as a go-to tool. This blog explores the reasons behind the growing adoption of audits in digital regulation, focusing on key legislative frameworks such as the EU's Digital Services Act (DSA) and the UK's Online Safety Act (OSA), and also explores the scope of audits in AI and other digital regulation. It also includes some practical tips for businesses navigating these new audit regimes.

Audits in context

Audits in digital regulation typically fall into three categories: internal audits, external audits and regulator-driven information gathering.

- **Internal audits:** audits typically conducted by a business' assurance function to self-assess compliance, helping it identify and address compliance or controls gaps proactively.
- **External audits:** audits performed by independent third party auditors who provide an objective assessment of a business' compliance to a specified standard.
- **Regulator-driven information gathering:** regulatory bodies may also be empowered to conduct or direct audits or reviews of a business' compliance, which may involve direct access to a business' systems and records.

This blog focuses on the second and third categories, while touching on the first in the context of existing regulation.

Why audits?

Audits have been used as a regulatory tool since at least the 19th century, initially emerging in the context of financial oversight. The UK's Companies Act of 1844 was one of the first to mandate external audits for corporate financial records to protect shareholders and enhance accountability. In the United States, the role of audits expanded following the creation of the Securities and Exchange Commission (SEC) in 1934.

The rise of digital platforms has ushered in challenges that traditional regulatory frameworks may struggle to address. In particular, the complexity of new technologies presents challenges for regulators seeking to understand the operation of systems, and their compliance with laws, in an efficient and accurate manner.

External audits are increasingly being encouraged, and in some cases required, as a potential means to address these challenges. There are various factors that may be contributing to a growing recognition of audits as essential tools within the digital regulatory toolkit:

- **Accountability and transparency:** The belief that independent audits can increase trust by involving external

examiners who offer objective insights into an organization's practices and compliance measures, offering a comparative basis for public scrutiny.

- **Cost effectiveness:** The belief that audits enable companies to independently manage compliance assessments, reducing the regulatory burden while ensuring a thorough review process. This theoretically allows regulatory bodies to focus their resources on higher-priority tasks, such as developing standards, reviewing audit results and enforcement. On the other hand, audits place significant financial and operational demands on businesses, particularly smaller operations that may struggle to allocate the necessary resources without compromising growth-focused priorities.
- **Standardization:** The belief that independent audits can bring a uniform approach to assessing compliance, applying consistent criteria across the industry, and making it easier to identify trends, spot systemic risks and ensure fair enforcement across the board. Standardization, however, is an area in need of development in this space, as discussed in the next section. This can present challenges in industries without existing standardization and may risk incentivizing certain practices even where no genuine 'best practice' standard yet exists.

DSA and OSA audits

The DSA, which fully came into effect in February 2024, is a landmark digital regulation (to learn more about the DSA, read our DSA Decoded Blog Services). Audits form a key component of the DSA's compliance and enforcement architecture, requiring very large online platforms and search engines (VLOPSEs), ie those with over 45 million active EU users, to undergo annual external audits conducted by independent third party auditors. The first round of audits were finalized in mid-2024, focusing on the platforms' compliance approach to illegal content and systemic risks, transparency in advertising and the protection of user rights – capturing the obligations under Chapter III of the DSA. Audit reports and implementation reports, the latter addressing how

VLOPs and VLOSEs would remediate gaps, were published in November 2024.

The delegated regulation on the performance of DSA audits (DR), adopted by the European Commission in October 2023, outlines the audit procedures and framework to guide VLOPSEs and auditing organizations in preparation of the audit reports. Despite the global significance of the DSA's audit regime, key concerns remain about implementation and verification, particularly due to the lack of standard methodologies or benchmarks in the DR, its overambitious expectations and challenges related to auditor independence and eligibility.

Operating alongside the DSA, the 2022 Code of Practice on Disinformation (EU CoP), which has been signed by a broad range of actors including major online platforms such as Google, Meta and TikTok, is a voluntary and co-regulatory instrument. It monitors platforms across areas such as political advertising, financial disinformation and misleading content. While the EU CoP is voluntary, it will soon become a recognized Code of Conduct under the DSA. As a result, any commitments undertaken voluntarily under the EU CoP will form part of the DSA audit.

Similar to the DSA, the OSA empowers Ofcom to issue notices requiring providers to commission an audit of the provider's compliance. Unlike the DSA, however, such audits are not automatically mandated. In a consultation undertaken in November 2023, Ofcom sought feedback on a proposal to impose an annual risk management audit requirement alongside its information gathering powers. Ofcom is also consulting on plans to assess the accuracy of proactive content moderation technologies through an audit-based assessment.

As other jurisdictions look to adopt laws related to content moderation, the approach of the OSA and DSA to audits may influence policy approaches globally.

Auditing AI systems

Artificial intelligence is another context where legislators are looking to audits as a potential regulatory tool. Some academics and third sector stakeholders have emphasized the importance of AI auditability is important for assessing compliance with standards in areas such as ethics and data security.

The EU AI Act enables third party Notified Bodies and Market Surveillance Authorities to, under particular risk and monitoring conditions, access a system provider's technical documentation, source code and training datasets - to be assessed for a reasonable assurance of compliance under various fairness, biases and accuracy principles. This is a relatively novel audit requirement.

In the United States, the New York City Department of Consumer and Worker Protection in November 2022 implemented regulations mandating employers utilizing AI in hiring practices to undergo independent audits to verify that their systems are free from racial or gender biases. By contrast, in California, a bill proposing mandatory annual third-party audits for AI models was vetoed by Governor Newsom in September 2024. The main criticism of the proposed auditing requirement, and the stringent obligations of the bill as a whole, were the substantial compliance costs and potential impacts on innovation, with Governor Newsom calling for adaptable and differentiated oversight to avoid a disproportionate regulatory burden on smaller developers – a reminder that one size does not fit all.

Other digital regulation with audit requirements

Audits are gaining traction as a critical oversight mechanism in various domains of digital regulation.

- In the domain of cybersecurity, the NIST Framework, mandated for federal agencies and voluntarily adopted by the private sector, requires regular audits to ensure compliance and maintain strong defences against cyber threats.

- Similarly, the NIS2 Directive 2022 in the EU equips national competent authorities with the power to demand ad hoc and regular independent audits of 'essential entities', alongside the authority to issue requests for information and conduct the audits themselves.
- The regulations proposed by the California Privacy Protection Agency (CPPA) in November 2024 mandate annual independent cybersecurity audits for certain businesses that meet revenue and personal data processing thresholds.

By embedding audits into compliance structures, these regulations may set a precedent for their expansion into other areas, such as algorithmic transparency and ethical AI use.

Practical tips for tech businesses

As audits become an increasingly common feature of digital regulation, tech companies should proactively prepare to manage risks. Specifically, we recommend:

1. **Advocate thoughtfully:** Engage in regulatory consultations to provide feedback on proposed audit requirements, particularly to highlight disproportionate burdens to the innovation focused approach of emerging technologies.
2. **Prepare for audit obligations:** If subject to audits, ensure robust internal compliance and assurance systems are in place, and allocate resources to meet external audit demands effectively–including explaining legal requirements to external auditors who may be new to the regulatory regime in question.
3. **Plan for adverse outcomes:** Develop contingency plans to address findings from negative audits, including transparent remediation strategies and stakeholder communication to rebuild trust.
4. **Leverage audit insights:** Use audit reports constructively to identify areas for improvement, streamline operations and enhance compliance efforts, turning audits into a tool for innovation and growth.

With preparation and strategic engagement, businesses can better navigate the challenges and opportunities audits bring. Our team at Freshfields has extensive experience guiding businesses through complex regulatory landscapes, from advising on compliance with established frameworks like the OSA, DSA, and privacy laws to preparing for emerging audit requirements. We help clients anticipate challenges, develop practical strategies and leverage audits as opportunities to strengthen trust and innovation. Reach out to explore how we can support your organization in staying ahead of regulatory developments.