APPLICATION OF EXISTING U.S. LAWS TO ARTIFICIAL INTELLIGENCE APPLICATIONS

Introduction

ACT | The App Association (ACT) is developing a comprehensive report on how current laws—federal, state, and local—apply to artificial intelligence (AI) systems. This endeavor is vast and wide-ranging, and we need the help of experts and stakeholders from all sides of the issue. At this stage in the process, we are providing a high-level overview of how current laws apply in general as a preview of the forthcoming report. In tandem, we are opening this overview for comment to help us account for existing laws and their applicability as accurately and comprehensively as possible.

AI systems are being used in employment, financial decision making, healthcare, consumer services, public communications, and creative industries. These systems provide substantial benefits, from identifying certain types of cancer better than human physicians to saving small businesses hundreds of thousands per year in operations costs. They also pose a combination of long-existing and novel risks including those related to discrimination, fraud, privacy, and safety hazards. Although the United States has not adopted a single comprehensive federal AI law, there exists a wide set of federal, state, and municipal statutes and regulations that already govern the design, marketing, sale, and use of AI applications.

This document serves as a high-level outline for a comprehensive research project examining the legal accountability of AI applications under existing U.S. law. It organizes major AI use cases of concern for policymakers and identifies the specific legal authorities that apply to each area. These statutes and regulations demonstrate that AI's use, development, and deployment is generally within the scope of established legal frameworks, which creates enforceable obligations for developers, suppliers, and deployers of AI systems across consumer protection, civil rights, privacy, safety, labor, liability, and competition.

We invite written comments on the scope, accuracy, and completeness of this overview.

Please submit comments **no later than January 16, 2026** to: gdufault@actonline.org and ksankararaman@actonline.org.

AI Use Cases and Applicable Legal Frameworks

The use cases are grouped into major risk categories.

Bias, Discrimination, and Civil Rights

Use Cases: Hiring algorithms, resume screening tools, tenant screening, credit underwriting, school admissions evaluation, biometric identification.

Laws and Explanations[1]

Title VII of the Civil Rights Act
Prohibits employment discrimination based on race, color, religion, sex, or national origin. If an employer uses an AI system that disproportionately screens out protected groups, the employer may be liable under the statute's prohibition on unlawful employment practices. Delegating a decision to an algorithm does not reduce or shift this responsibility.

Americans with Disabilities Act (ADA)
Requires equal access for individuals with disabilities and prohibits hiring practices that screen out individuals based on disability unless the practice is job related and consistent with business necessity. An employer that relies on AI systems that evaluate speech, facial expression, or cognitive patterns may be liable for ADA violations if they disadvantage individuals with speech impairments, autism, or other conditions.

Age Discrimination in Employment Act (ADEA)
Protects workers age 40 and older from discriminatory hiring or employment practices. If an employer uses an AI system in a way that filters based on age or age proxies, doing so may violate this law.

Equal Credit Opportunity Act (ECOA)
Prohibits discrimination in credit decisions. When AI is used to make underwriting decisions, creditors must still provide specific reasons for adverse action. The use of a model does not excuse compliance.

---

[1] https://www.huschblackwell.com/newsandinsights/ai-and-workplace-discrimination-what-employers-need-to-know-after-the-eeoc-and-dol-rollbacks; U.S. Department of Justice, Civil Rights Division. (2022, May 12). *Algorithms, artificial intelligence, and disability discrimination in hiring*. ADA.gov. Retrieved from https://www.ada.gov/resources/ai-guidance/; Holistic AI. (2023, April 27). *The EEOC releases a joint statement on AI and automated systems*. Retrieved from https://www.holisticai.com/news/eeoc-joint-statement-on-ai-automated-systems; Zadikany, R. (2023, July 6). *EEOC issues Title VII guidance on employer use of AI, other algorithmic decision-making tools*. Mayer Brown. Retrieved from https://www.mayerbrown.com/en/insights/publications/2023/07/eeoc-issues-title-vii-guidance-on-employer-use-of-ai-other-algorithmic-decisionmaking-tools; NYC Department of Consumer and Worker Protection. (n.d.). *Automated Employment Decision Tools (AEDT)*. Retrieved from https://www.nyc.gov/site/dca/about/automated-employment-decision-tools.page.

Fair Housing Act

Prohibits discrimination in housing, tenant screening, and real estate advertising. Reliance on automated systems in a manner that discriminates against protected groups may violate this law.

State Civil Rights Statutes

For example, Massachusetts General Laws Chapter 151B prohibits discriminatory practices in employment, housing, and credit. Covered entities relying on algorithmic decision-making to make decisions that produce discriminatory results can constitute a violation even when the system appears neutral.

Developers' and Deployers' Responsibilities

Developers must ensure that deployers and users understand how to use their AI systems in ways that comply with civil rights law. Developers can be liable if they knowingly induce or fail to properly disclose proper ways to use or deploy AI systems they produce to prevent harmful bias or other kinds of unlawful discrimination. Liability arises from developer conduct (e.g., deception, negligent design).

Consumer Protection, Deception, and Market Harm

Use Cases

False advertising of AI capabilities, deceptive chatbots, deepfake impersonation, automated fraud, algorithmic pricing tools, AI misinformation.

Laws and Explanations[2]

Federal Trade Commission Act Section 5a

Prohibits unfair or deceptive acts and practices. Claims about AI must be truthful, substantiated, and not misleading. The Federal Trade Commission has enforced this law against companies selling AI systems that do not perform as advertised or that are used for

[2] Federal Trade Commission. (2022, June 16). *Combatting online harms through innovation: Report to Congress*; Federal Trade Commission. (2024, September 25). *FTC announces crackdown on deceptive AI claims and schemes*. Retrieved from https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes; Consumer Financial Protection Bureau. (2023, September 19). *CFPB issues guidance on credit denials by lenders using artificial intelligence*. Retrieved from https://www.consumerfinance.gov/about-us/newsroom/cfpb-issues-guidance-on-credit-denials-by-lenders-using-artificial-intelligence/; Consumer Financial Protection Circular 2024-06: Background Dossiers and Algorithmic Scores for Hiring, Promotion, and Other Employment Decisions, 89 Fed. Reg. 88875 (Nov. 12, 2024), https://www.consumerfinance.gov/compliance/circulars/consumer-financial-protection-circular-2024-06-background-dossiers-and-algorithmic-scores-for-hiring-promotion-and-other-employment-decisions/; U.S. Department of Justice, Statement of Interest, *In re RealPage, Inc., Rental Software Antitrust Litigation*, Case No. 3:23-MD-3071, https://www.justice.gov/d9/2023-11/418053.pdf.

harmful or deceptive purposes. The agency may also require deletion of models trained on unlawfully obtained data.

Consumer Financial Protection Act
Authorizes the Consumer Financial Protection Bureau to prevent unfair, deceptive, or abusive practices in financial products and services. Covered financial institutions must comply with existing consumer finance obligations when using AI in lending, credit scoring, or financial advertising.

Fair Credit Reporting Act (FCRA)
Regulates consumer reporting agencies and the use of consumer data in credit decisions. Consumer reporting agencies must comply with FCRA obligations when using AI systems in order to generate risk scores or eligibility determinations, among other things.

State Unfair and Deceptive Acts and Practices Laws (UDAP)
State consumer protection laws often provide broader protections than federal law. They prohibit deceptive marketing, misleading AI claims, or the sale of AI systems that do not meet ordinary expectations of reliability and safety.

Sherman Antitrust Act
Section 1 prohibits agreements that restrain trade. While competitors commonly and legally use algorithms to help price their products and services, Section 1 bars competitors from using shared pricing algorithms to coordinate or stabilize prices. Section 2 prohibits monopolization and attempted monopolization. The use of AI to entrench dominance or exclude rivals can trigger investigation.

Developers' and Deployers' Responsibilities

Developers must avoid overstating AI capabilities, ensure AI systems are not created primarily to facilitate deception, and avoid creating pricing algorithms that are primarily used for illegal price fixing.

Privacy, Data Protection and Biometric Information

Use Cases

Training data scraping, face recognition, voice analysis, behavior tracking, AI driven advertising, consumer profiling.

Laws and Explanations[3]

Children's Online Privacy Protection Act (COPPA)
Regulates data collection from children under 13. Entities subject to COPPA must obtain verifiable parental consent and follow strict data handling practices when using AI systems.

Health Insurance Portability and Accountability Act (HIPAA)
Applies to medical AI tools that process protected health information. Covered entities and Business Associates processing data on behalf of covered entities must follow strict privacy and security rules.

State Comprehensive Privacy Laws
Numerous states, including California, Colorado, Virginia, Connecticut, Texas, Kentucky, and Utah have enacted consumer data privacy statutes. These laws require transparency, data minimization, opt-out rights, and obligations for automated decision-making in some jurisdictions.

Illinois Biometric Information Privacy Act (BIPA)
Requires informed consent before collecting biometric identifiers such as faceprints or voiceprints. AI systems that create facial recognition databases without consent may violate this law.

Massachusetts Data Security Law and Regulations (Chapter 93H and 201 CMR 17.00)
Requires companies to safeguard personal information of Massachusetts residents, implement written information security programs, and report breaches. Entities subject to

[3] Georgetown Law Institute for Technology & Policy, *How Existing Laws Apply to AI Chatbots for Kids and Teens* (Nov. 10, 2025), https://www.law.georgetown.edu/tech-institute/insights/how-existing-laws-apply-to-ai-chatbots-for-kids-and-teens/; Electronic Privacy Information Center. (2021, January 11). *FTC orders photo app to delete algorithms built on personal data*. https://epic.org/ftc-orders-photo-app-to-delete-algorithms-built-on-personal-data/; Zhu, L, Harris, L. (2023, May 23). *Generative artificial intelligence and data privacy: A primer* (CRS Report No. R47569). Congressional Research Service. https://www.congress.gov/crs-product/R47569/; U.S. Department of Health and Human Services, Office for Civil Rights. (n.d.). *Summary of the HIPAA Security Rule*. Retrieved November 18, 2025, from https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html; National Conference of State Legislatures. (2025). *State laws related to digital privacy*. https://www.ncsl.org/technology-and-communication/state-laws-related-to-digital-privacy; International Association of Privacy Professionals. (2025). *US state comprehensive privacy laws report*. https://iapp.org/resources/article/us-state-privacy-laws-overview/; Office of the Attorney General, Commonwealth of Massachusetts. (2024, April 16). *AG Campbell issues advisory providing guidance on how state consumer protection and other laws apply to artificial intelligence*. Mass.gov. https://www.mass.gov/news/ag-campbell-issues-advisory-providing-guidance-on-how-state-consumer-protection-and-other-laws-apply-to-artificial-intelligence.

the law must meet these standards when using AI systems that process or store personal information.

Developers' and Deployers' Responsibilities

Developers and deployers must obtain required consent, secure personal data, document processing activities, and refrain from collecting or using personal data in ways that violate existing privacy statutes and best practices.

Safety, Health, and High-Risk Physical Systems

Use Cases

Medical AI devices, autonomous vehicles, robotics, safety critical AI in transportation and infrastructure.

Laws and Explanations[4]

Food and Drug Administration (FDA) Software as a Medical Device Guidance
Requires premarket review and ongoing monitoring for AI-driven diagnostic and treatment tools. Systems must be validated, tested, and monitored post-deployment.

National Highway Traffic Safety Administration Safety Framework
Applies to automated driving systems. Manufacturers remain responsible for defects in autonomous systems and may be required to submit safety assessments. State and local laws also apply to limited testing projects in cities.

Product Liability Law
Manufacturers may be strictly liable for defects in design, manufacturing, or warnings. If a product incorporating AI malfunctions or produces harmful outputs unpredictably in ways that cause injury, the producer may face product liability.

[4] Saltman, A. (2024, September 25). FDA's Regulation of AI/ML SaMD. *NAMSA*. https://namsa.com/resources/blog/fdas-regulation-of-ai-ml-samd/; National Highway Traffic Safety Administration. (n.d.). Automated Driving Systems. *U.S. Department of Transportation*, https://www.nhtsa.gov/vehicle-manufacturers/automated-driving-systems; Sharkey, C. (2024, September 25). Products Liability for Artificial Intelligence. *Lawfare*. https://www.lawfaremedia.org/article/products-liability-for-artificial-intelligence; Impact of Automation on Workplace Safety. *BradyID.com*, https://www.bradyid.com/resources/how-robots-ai-impact-safety-protocols; Sansone, M. (2023, March 23). *Motor Vehicle Accidents Caused by Autonomous Vehicles: Exploring AI Liability in the Tort System*. Arizona State Law Journal. https://arizonastatelawjournal.org/2023/03/23/motor-vehicle-accidents-caused-by-autonomous-vehicles-exploring-ai-liability-in-the-tort-system/.

Occupational Safety and Health Act (OSH Act)
Employers must provide safe workplaces. Employers are prohibited from creating unsafe working conditions, including through AI-driven robotics and monitoring tools.

Obligations

Manufacturers must ensure AI systems are safe, validated, and tested. Companies deploying AI in safety critical contexts remain responsible for foreseeable harms.

Intellectual Property and Digital Replica Rights

Use Cases

AI generated content, training data ingestion, generative image and audio systems, trademark and identity imitation.

Laws and Explanations[5]

Copyright Act
Protects works of human authorship. Courts have held that AI generated content without human creative input cannot be copyrighted. How copyright applies to model training is still unsettled, including whether training constitutes "copying" under the statute and, if it does, whether that use is permissible under fair use.

---

[5] https://www.cnet.com/tech/services-and-software/ai-has-sent-copyright-laws-into-chaos-what-you-need-to-know-about-your-rights-online/; https://www.congress.gov/crs-product/LSB11251; Yaros, O., & Nolan, B. W. (2025, October 8). *Protecting AI with IP: Comparing approaches taken in the US and UK*. Mayer Brown. https://www.mayerbrown.com/en/insights/publications/2025/10/protecting-ai-with-ip-comparing-approaches-taken-in-the-us-and-uk; **Zirpoli, C. T.** (2025, July 18). *Generative artificial intelligence and copyright law*, https://www.congress.gov/crs-product/LSB10922; U.S. Patent and Trademark Office. (2024, July 17). 2024 guidance update on patent subject matter eligibility, including on artificial intelligence. *Federal Register*, https://www.federalregister.gov/documents/2024/07/17/2024-15377/2024-guidance-update-on-patent-subject-matter-eligibility-including-on-artificial-intelligence; U.S. Copyright Office. (2024, July). *Copyright and artificial intelligence part 1: Digital replicas* (Report of the Register of Copyrights), https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-1-Digital-Replicas-Report.pdf; U.S. Copyright Office. (2025, January). *Copyright and artificial intelligence part 2: Copyrightability* (Report of the Register of Copyrights), https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-2-Copyrightability-Report.pdf; U.S. Copyright Office. (2025, May). *Copyright and artificial intelligence part 3: Generative AI training PRE-PUBLICATION VERSION* (Report of the Register of Copyrights), https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-3-Generative-AI-Training-Report-Pre-Publication-Version.pdf; Proskauer Rose LLP. (2024, June 4). *The King is Back (in the Digital Era) | The ELVIS Act, Generative AI and Right of Publicity*. New Media and Technology Law Blog. https://www.proskauer.com/blog/the-king-is-back-in-the-digital-era-the-elvis-act-generative-ai-and-right-of-publicity; Chedraoui, K. (2025, November 11). *AI has sent copyright laws into chaos. What you need to know about your rights online*. CNET. https://www.cnet.com/tech/services-and-software/ai-has-sent-copyright-laws-into-chaos-what-you-need-to-know-about-your-rights-online/; Boyden, B. E. (2024). Generative AI and IP under US law, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5024667.

Patent Act
Defines an inventor as a natural person. AI cannot be listed as an inventor. Humans must contribute to conception of an invention for patent protection.

Lanham Act
Prohibits trademark infringement and false endorsement. Entities that use AI outputs to imitate brands, logos, or personas may be liable.

Right of Publicity Laws
State laws protect individuals from unauthorized commercial use of their likeness, voice, name, or persona. Entities using AI tools that create synthetic replicas can violate these rights.

Trade Secret Law
Protects confidential information and proprietary algorithms. Misappropriation of AI models or training data can result in liability.

Developers' and Deployers' Responsibilities

Developers and deployers must avoid unauthorized use of copyrighted content, protect proprietary models, and obtain permission for the use of likenesses in some circumstances.

Labor Rights

Use Cases

Automated employee monitoring, productivity tracking, scheduling, performance scoring.

Laws and Explanations[6]

National Labor Relations Act (NLRA)
Protects employees' rights to organize and engage in concerted activity. AI monitoring that chills organizing or disciplines employees for protected activity may violate this law.

[6] NYC Department of Consumer and Worker Protection. (n.d.). *Automated Employment Decision Tools (AEDT)*. Retrieved from https://www.nyc.gov/site/dca/about/automated-employment-decision-tools.page; Graham, J. K., & Gaytán, R. (2024, November 21). *NLRB Joins Regulatory Assault on Electronic Surveillance of the Workplace*. Labor Relations Law Insider, https://www.laborrelationslawinsider.com/2024/11/nlrb-joins-regulatory-assault-on-electronic-surveillance-of-the-workplace/; Proskauer Rose LLP. (2023, October 23). *AI At Work: Safety And NLRA Best Practices For Employers*, https://www.proskauer.com/pub/ai-at-work-safety-and-nlra-best-practices-for-employers.

Fair Labor Standards Act (FLSA)
Regulates wages and hours. Employers using AI scheduling systems must still ensure compliance with overtime and minimum wage requirements.

Federal Trade Commission Act and Fair Credit Reporting Act
Apply when employers use AI tools that generate worker scores or affect employment opportunities.

State Monitoring Laws
Some states require notice before employee monitoring. Entities using AI tools that track keystrokes, video, or audio must comply with such requirements.

Developers' and Deployers' Responsibilities

Developers and deployers must take steps to ensure that AI systems for workplace purposes can be used in a manner that prioritizes transparency, avoids unlawful monitoring, and ensures AI driven employment decisions do not violate labor rights.

Liability, Accountability, and AI Generated Speech

Use Cases

Defamatory outputs, automated professional advice, harmful recommendations, autonomous agent conduct.

Laws and Explanations[7]

Negligence Law
Requires reasonable care. If an organization deploys or uses an AI system that causes foreseeable harm, it may be liable. A key question is whether upstream developers themselves owe a duty of care for downstream injuries, or whether they are too remote in the causal chain for those harms to be considered foreseeable.

---

[7] Smith, G., Stanley, K. D., Marcinek, K., Cormarie, P., & Gunashekar, S. (2024, November 20). *Liability for harms from AI systems*. RAND Corporation, https://www.rand.org/pubs/research_reports/RRA3243-4.html; Portner, C. (2025, July 22). *Liability considerations for developers and users of agentic AI systems.* Lathrop GPM LLP, https://www.lathropgpm.com/insights/liability-considerations-for-developers-and-users-of-agentic-ai-systems/; Choi, B. H. (2024, September 26). *Negligence liability for AI developers.* Lawfare, https://www.lawfaremedia.org/article/negligence-liability-for-ai-developers; Frazier, K. (2024). We're not ready for AI liability. *AI Frontiers*, https://ai-frontiers.org/articles/options-for-ai-liability; Brown, C. F., & Hummel, J. P. (2024, January 24). *Judge denies motion to dismiss AI defamation suit*. Ballard Spahr. Retrieved from https://www.ballardspahr.com/insights/alerts-and-articles/2024/01/judge-denies-motion-to-dismiss-ai-defamation-suit; Silverman, Katherine. (2025, May 28). *Georgia court dismisses defamation claim against OpenAI: A win for AI developers and legal clarity in defamation defense*. Retrieved from https://www.bfvlaw.com/georgia-court-dismisses-defamation-claim-against-openai-a-win-for-ai-developers-and-legal-clarity-in-defamation-defense/.

Product Liability
Applies if AI functions as part of a product and contains defects that cause injury.

Defamation Law
Applies when AI generates false statements that harm a person's reputation. Courts have permitted claims to proceed against AI developers, but recent rulings show a conflict, with some courts dismissing defamation claims, which may create legal clarity in defense. Liability applies to developers or deployers who publish or rely on AI-generated statements, depending on fault.

Section 230 of the Communications Decency Act
Limits liability for third-party content. Courts have not resolved whether this immunity applies to content created by AI.

Professional Malpractice
Professionals remain responsible for decisions made with the assistance of AI. Application of the relevant standard of care typically determines whether liability attaches.

Developers' and Deployers' Obligations

Developers and deployers must enable end users to verify that AI outputs are accurate, prevent foreseeable harms, and provide or enable the provision of safeguards around critical decisions.

Preliminary Findings and Future Research

The analysis presented here suggests that actors who develop or deploy AI systems are subject to a wide-ranging set of existing federal, state, and municipal laws, governing critical areas like discrimination, consumer protection, privacy, safety, intellectual property, labor, competition, and negligence liability.

While this high-level outline identifies broad legal coverage across many AI use cases, it also highlights potential gaps in the law, enforcement challenges, and key opportunities for standards development. Specifically, challenges such as the "black box" problem (lack of model interpretability), data provenance issues (tracing the source of training data), and the creation of digital replicas present opportunities for standards development to provide further definition on how best to address risks in specific circumstances. In parallel, enforcement agencies and policymakers have work ahead of them to better understand how current law applies to the development, deployment, and use of AI systems in order to best mitigate these risks through enforcement.

The overall research project will delve deeper into each of these legal and technological challenges, providing a detailed analysis of case law, regulatory precedents, and policy proposals. The findings will lay the groundwork for policymakers to develop a comprehensive national framework that builds upon this existing legal base, avoiding state-specific fragmentation and relying on risk-based, standards-driven governance to tackle these emerging difficulties.