CLS Conference 2025 – Workshop Outline

Revised: June 25, 2025

AI and Data Privacy

Legal Considerations for Using AI in the Workplace with a Brief Data Privacy Law Update

Presented By: Paul Z. Winters

I. Introduction

A. Timeliness and importance

1. AI's growing role in improving efficiency and client service in law firms

a) Operational efficiency: AI tools can automate repetitive tasks such as data entry, bill payment processing, and email responses, freeing up staff to focus on more strategic activities such as billable work.

UiPath: A leading robotic process automation (RPA) tool that automates data entry across multiple systems, reducing manual errors and saving time.

Zapier: Automates workflows by connecting different apps and transferring data between them without human intervention.

2. High level work support: Importantly, AI capabilities allow for legal professionals to significantly expedite legal researching processes, providing more comprehensive legal work products faster and cheaper.

3. Enhanced outreach: AI can analyze and automate marketing and communication strategies to increase engagement.

Jasper: Marketing and Social Media performance analytic features. Marketing content optimization to improve SEO.

4. Resource optimization: By optimizing resource allocation, AI ensures that firm resources are used most effectively, maximizing the quality and quantity of firm output.

Gmail's Smart Reply and Smart Compose: AI tools in Gmail that suggest quick responses and auto-complete sentences, speeding up email communication.
HubSpot: Uses AI to automate email responses based on predefined templates and workflows, allowing customer support and sales teams to respond more quickly.

Customer Support:
Chatbots like Drift or Intercom: AI-driven chatbots that handle routine inquiries, providing instant responses to common questions, and freeing up human agents for more complex issues.

B. The need for law firms to stay current with technological advancements

1. Competitive advantage: Staying updated with technological advancements like AI may help law firms remain competitive, attract more clients, increase their visibility, and provide better work products faster and for cheaper.

2. Client expectations: AI to enhance transparency, accountability, efficiency, and reduce manual errors.

3. Future-proofing: Adopting AI and other technologies may prepare law firms for future challenges and opportunities, ensuring long-term sustainability, growth, and efficiency.

II. Definition, history, and development of AI

A. AI is the simulation of human intelligence processed by machines

1. Core processes: AI simulates key human intelligence processes such as learning (acquiring knowledge and skills), reasoning (solving problems and making decisions), and self-correction (improving performance over time)

2. Types of AI: AI can be categorized into narrow AI (designed for specific tasks) and general AI (capable of performing any intellectual task a human can do, although this is more theoretical at present)

3. Applications: AI applications range from simple rule-based systems to complex neural networks and deep learning models used in areas like natural language processing, computer vision, and robotics

B. Historical context: From rule-based systems to machine learning and deep learning

1. Rule-based systems: Early AI systems used predefined rules and logic to perform tasks, such as expert systems for medical diagnosis

2. Machine learning: The advent of machine learning allowed AI systems to learn from data and improve over time without explicit programming. Algorithms such as decision trees, support vector machines, and clustering became common.

3. Deep learning: A subset of machine learning, deep learning involves neural networks with many layers (deep neural networks) that can model complex patterns and relationships in data. This has led to breakthroughs in image recognition, speech processing, and generative models.

C. Generative AI: Creating new content vs. traditional AI: analyzing existing data

1. Traditional AI: Focuses on analyzing existing data to identify patterns, make predictions, and provide insights. Examples include recommendation systems, fraud detection, and predictive analytics.

2. Generative AI: Goes beyond analysis to create new content such as text, images, music, and even videos. Examples include GPT-4o for text generation, DALL-E for image creation, and AI-driven music composition tools.

3. Complementary roles: Generative AI and traditional AI often work together to provide comprehensive solutions. For instance, an AI system might analyze donor data to identify trends (traditional AI) and then generate personalized communication materials (generative AI).

III. Legal Risks and Vulnerabilities – Case Studies

A. Intellectual property infringement allegations

1. Companies like Stability AI and MidJourney faced lawsuits for using copyrighted materials, known as Training Images, to train their AI models without permission[1]. These cases highlighted the unauthorized use of vast amounts of online content, including text, images, and other media.

[1] Andersen v. Stability AI Ltd., 700 F. Supp. 3d 853, 860 (N.D. Cal. 2023). "Stability is alleged to have 'downloaded o[r] otherwise acquired copies of billions of copyrighted images without permission to create Stable Diffusion,' known as 'training images'."

Initial Allegations[2]: The same set of allegations were brought against all three defendants* (Stability, Midjourney, and DeviantArt) as follows:

a) *1: Direct Copyright Infringement under 17 U.S.C §106[3]*

b) *2: Vicarious Copyright Infringement, 17 U.S.C. § 106[4]*

c) *3: Violation of the Digital Millennium Copyright Act ("DMCA")[5]*

d) *4: Violation of the Right to Publicity, Cal. Civil Code § 3344[6]*

e) *5: Violation of the Common Law Right of Publicity[7]*

f) *6: Unfair Competition, Cal. Bus. & Prof. Code § 17200[8]*

g) *7: Declaratory Relief[9]*

*A Breach of Contract claim was also sought against DeviantArt individually. Plaintiff has amended complaint twice to incorporate new claims such as

Commented [JM1]: For further review - thoughts on further context and ABA resource provided in footnote 7?

[2] Andersen v. Stability AI Ltd., 700 F. Supp. 3d 853, 862 (N.D. Cal. 2023).

[3] 17 U.S.C.A. § 106 (West). "Subject to sections 107 through 122, the owner of copyright under this title has the exclusive rights to do and to authorize any of the following: (1) to reproduce the copyrighted work in copies or phonorecords; (2) to prepare derivative works based upon the copyrighted work; (3) to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending; (4) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works, to perform the copyrighted work publicly; (5) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work, to display the copyrighted work publicly; and (6) in the case of sound recordings, to perform the copyrighted work publicly by means of a digital audio transmission."

[4] Ibid.

[5] Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) ; 17 U.S.C. §§ 1201–1205 (2024). *See full code in Addendum A.*

[6] Cal. Civ. Code § 3344 (West 2024). *See full code in Addendum B.*

[7] The principal of a "Right of Publicity" was foundationally litigated in Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc., 202 F.2d 866 (2d Cir. 1953), and first notably codified and acknowledged in the United States with the passage of California Civ. Code §§3344 in the early 1970's, which was recently amended in 2024. The Right of Publicity was further recognized by the Supreme Court in Zacchini v. Scripps-Howard Broad. Co., 433 U.S. 562, 564–65 (1977). For more information about the Right of Publicity, see the American Bar Association's following article: "What's in a Name, Likeness, and Image? The Case for a Federal Right of Publicity Law." (Malia Roesler & Gabrielle Hutchinson, *What's in a Name, Likeness, and Image? The Case for a Federal Right of Publicity Law*, 13 Landslide 20 (2020), https://www.americanbar.org/groups/intellectual_property_law/resources/landslide/archive/whats-name-likeness-image-case-federal-right-publicity-law/.

[8] Cal. Bus. & Prof. Code § 17200 (West 2024). "[…] unfair competition shall mean and include any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising and any act prohibited by Chapter 1 (commencing with Section 17500) of Part 3 of Division 7 of the Business and Professions Code.

[9] Authority to grant Declaratory Relief is provided for and defined in **Declaratory Judgment Act**, 28 U.S.C. § 2201 as follows; "In a case of actual controversy within its jurisdiction, … any court of the United States, upon the filing of an appropriate pleading, may declare the rights and other legal relations of any interested party seeking such declaration, whether or not further relief is or could be sought. Any such declaration shall have the force and effect of a final judgment or decree and shall be reviewable as such." in California specifically, Declaratory Relief is provided for and defined further through **Cal. Civ. Proc. Code § 1060 (West 2024), "**Any person interested under a written instrument, excluding a will or a trust, or under a contract, or who desires a declaration of his or her rights or duties with respect to another, […] may, in cases of actual controversy relating to the legal rights and duties of the respective parties, bring an original action or cross-complaint in the superior court for a declaration of his or her

Unjust Enrichment and violation of the Lantham Act and further substantiate the original claims, and naming an additional defendant (Runway AI, Inc.).

Procedural timeline: Filed in January 2023 by artists Karla Ortiz, Kelly McKernan, and Sarah Andersen. After initial motions to dismiss were largely granted with leave to amend, Plaintiffs filed amended complaints in November 2023 and October 2024, adding new parties including Runway AI. A special motion to strike by DeviantArt was denied. Discovery and ESI protocols were addressed in early 2025 by Magistrate Judge Cisneros. Status conferences are set for July and September 2025, with trial preliminarily scheduled for spring 2027.

Stability AI:
Product: Stability AI developed a tool called Stable Diffusion. It is a text-to-image generation model that allows users to create images from textual descriptions. The model was trained on a large dataset of images sourced from the internet for the purposes of mathematically generating images. Stability AI faced legal challenges due to concerns over copyright infringement. The lawsuit was centered around the use of copyrighted images in the training data without explicit permission from the original creators or rights holders.

MidJourney
Product: MidJourney offers a service similar to Stable Diffusion (Midjourney Product), where users can generate artwork or images based on text prompts. This tool also leverages a large dataset of images to generate the final artwork. MidJourney was a defendant in the same lawsuit over similar copyright issues, where the generated images were alleged to be derived from copyrighted works used in training the AI model without proper licensing or consent from the copyright holders.

DeviantArt
Product: DeviantArt agreed to be a primary source for a dataset created to train Stable Diffusion. The dataset was created by LAION's scraping and creation of training images at the direction of Stability. DeviantArt also distributed Stable Diffusion, which was used to run their own AI imaging product called DreamUp.

Runway AI, Inc.
Product: Runway AI allegedly collaborated, trained, and distributed Stable Diffusion.

---

rights and duties in the premises, including a determination of any question of construction or validity arising under the instrument or contract. He or she may ask for a declaration of rights or duties, either alone or with other relief; and the court may make a binding declaration of these rights or duties, whether or not further relief is or could be claimed at the time. The declaration may be either affirmative or negative in form and effect, and the declaration shall have the force of a final judgment. The declaration may be had before there has been any breach of the obligation in respect to which said declaration is sought."

B. Automated processing and discrimination claims

1. The Equal Employment Opportunity Commission (EEOC) settled its first lawsuit involving the discriminatory use of AI in hiring practices with iTutorGroup, Inc. The company was accused of using AI to automatically reject older job applicants, violating the Age Discrimination in Employment Act (ADEA)[10]. According to the EEOC's lawsuit, iTutorGroup programmed their tutor application software to automatically reject female applicants aged 55 or older and male applicants aged 60 or older. iTutorGroup rejected more than 200 qualified applicants based in the United States because of their age[11].

Commented [JM2]: For further caselaw development.

2. Discrimination claims and legal challenges: The settlement included a payment of $365,000 to over 200 affected applicants, and the company agreed to adopt anti-discrimination policies and conduct compliance training.

a) Organizations that utilize recruiting companies for recruitment must be particularly cautious when incorporating AI-driven job screening tools. While AI can streamline the hiring process by efficiently filtering candidates based on predefined parameters, it is crucial to ensure that these parameters do not unintentionally introduce bias or discrimination. Organizations, often guided by strong ethical principles, should ensure that AI tools are used appropriately to promote fairness.

[10] 29 U.S.C. § 626(a)–(b) (2022). *See Subsections a and b of the Code in Addendum C.*

[11] Equal Employment Opportunity Comm'n v. iTutorGroup, Inc., No. 1:22-cv-02565-PKC-PK, 2022 WL 20662185 (E.D.N.Y. May 5, 2022). Plaintiff alleged that, "Defendants intentionally discriminated against older applicants because of their age by programming their tutor application software to automatically reject female applicants age 55 or older and male applicants age 60 or older." This came to light when "On or about March 29, 2020, Charging Party applied using her real birthdate and was immediately rejected because she was over the age of 55. [and] On or about March 30, 2020, Charging Party applied using a more recent date of birth and otherwise identical application information and was offered an interview." Plaintiffs noted that, "The effect of the practices [...was deprivation for] older applicants rejected because of their age of equal employment opportunities and otherwise adversely affect their status as applicants for employment because of their age." The EEOC concluded, "The unlawful employment practices [...] were and are willful within the meaning of Section 7(b) of the ADEA, 29 U.S.C. § 626(b) [(2022)]."

C. AI's limitations with factual issues

1. Steven Schwartz, a New York lawyer, cited fake cases generated by ChatGPT in a legal brief filed in federal court and was fined. The incident occurred in a personal injury lawsuit filed by Roberto Mata against Avianca, a Colombian airline, in the Southern District of New York[12]. Schwartz admitted in an affidavit that he used ChatGPT to supplement his legal research. Judge P. Kevin Castel identified six cases in Schwartz's filing as bogus, calling the situation "unprecedented." The lawyer revealed that ChatGPT assured him of the authenticity of these cases, even confirming their existence in reputable legal databases like LexisNexis and Westlaw. Sanctions were issued by the court in accordance with Rule 11 of the Federal Rules of Civil Procedure.[13]

a) Schwartz's actions in conflict with the ABA's Model Rules of Professional Conduct, specifically Rule 1.1, 1.3, 3.1, and 3.3.[14]

2. Personal example – Delaware nonstock corporations.

[12] Mata v. Avianca, Inc., 678 F. Supp. 3d 443, 448–49 (S.D.N.Y. 2023). Judge P. Kevin Castel of the United States Southern District of New York's District Court opined and ruled that, "In researching and drafting court submissions, good lawyers appropriately obtain assistance from junior lawyers, law students, contract lawyers, legal encyclopedias and databases such as Westlaw and LexisNexis. Technological advances are commonplace and there is nothing inherently improper about using a reliable artificial intelligence tool for assistance. But existing rules impose a gatekeeping role on attorneys to ensure the accuracy of their filings. Rule 11, Fed. R. Civ. P. Peter LoDuca, Steven A. Schwartz and the law firm of Levidow, Levidow & Oberman P.C. (the "Levidow Firm") (collectively, "Respondents") abandoned their responsibilities when they submitted non-existent judicial opinions with fake quotes and citations created by the artificial intelligence tool ChatGPT, then continued to stand by the fake opinions after judicial orders called their existence into question. Many harms flow from the submission of fake opinions.[1] The opposing party wastes time and money in exposing the deception. The Court's time is taken from other important endeavors. The client may be deprived of arguments based on authentic judicial precedents. There is potential harm to the reputation of judges and courts whose names are falsely invoked as authors of the bogus opinions and to the reputation of a party attributed with fictional conduct. It promotes cynicism about the legal profession and the American judicial system. And a future litigant may be tempted to defy a judicial ruling by disingenuously claiming doubt about its authenticity. […] For reasons explained and considering the conduct of each individual Respondent separately, the Court finds bad faith on the part of the individual Respondents based upon acts of conscious avoidance and false and misleading statements to the Court. […] Sanctions will therefore be imposed on the individual Respondents […and, based on precedent, the] Levidow Firm."

[13] Fed. R. Civ. P. 11. *See Addendum D for Rule 11 full text.*

[14] 1.1 Competence: A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation. See Model Rules of Prof'l Conduct r. 1.1 (Am. Bar Ass'n 2023).
1.3 Diligence: A lawyer shall act with reasonable diligence and promptness in representing a client. See Model Rules of Prof'l Conduct r. 1.3 (Am. Bar Ass'n 2023).
3.1 Meritus Claims & Contentions: A lawyer shall not bring or defend a proceeding, or assert or controvert an issue therein, unless there is a basis in law and fact for doing so that is not frivolous, which includes a good faith argument for an extension, modification or reversal of existing law. A lawyer for the defendant in a criminal proceeding, or the respondent in a proceeding that could result in incarceration, may nevertheless so defend the proceeding as to require that every element of the case be established. See Model Rules of Prof'l Conduct r. 3.1 (Am. Bar Ass'n 2023).
3.3(a)(1-2) Candor Toward the Tribunal: a lawyer shall not knowingly: (1) make a false statement of fact or law to a tribunal or fail to correct a false statement of material fact or law previously made to the tribunal by the lawyer; and (2) fail to disclose to the tribunal legal authority in the controlling jurisdiction

IV. Current legal frameworks

A. EU frameworks

1. GDPR: Key provisions relevant to AI use

a) Data protection and privacy: The General Data Protection Regulation (GDPR) sets strict rules for protecting personal data within the EU, impacting how AI systems handle such data. For example, the data minimization principle requires AI to use only the data necessary for its purpose.[15]

b) Consent requirements for AI data processing: GDPR requires explicit consent from individuals to process their personal data[16]*, including data used by AI systems. Consent must be freely given, specific, informed, and unambiguous.*[17] *AI systems must provide clear information on how data will be used and obtain explicit consent. Processing of special categories of personal data. Additional conditions apply if AI systems process sensitive data, such as health or biometric data.*[18]

known to the lawyer to be directly adverse to the position of the client and not disclosed by opposing counsel. See Model Rules of Prof'l Conduct r. 3.3 (Am. Bar Ass'n 2023).

[15] Personal data shall be…adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'). See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), art. 5, 2016 O.J. (L 119) 1.

[16] Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. See Regulation (EU) 2016/679, art. 7, 2016 O.J. (L 119) 1.

[17] Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by written statement, including by electronic means, or an oral statement. See Regulation (EU) 2016/679, recital 32, 2016 O.J. (L 119) 1.

[18] Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. [This provision] shall not apply if one of the following applies:
(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes. See Regulation (EU) 2016/679, art. 9, 2016 O.J. (L 119) 1.

2. EU Artificial Intelligence Act, adopted March 13, 2024, effective August 1, 2024, with enforcement beginning August 2, 2026

a) Objectives and scope: The EU AI Act aims to regulate AI technologies to ensure they are safe, ethical, and respect fundamental rights.[19]

b) Risk levels definitions

(1) Unacceptable risk: Prohibited AI systems, such as those used for social scoring, employing deceptive techniques that can harm individuals, real-time remote biometric identification, and emotion recognition.20

(2) High risk: AI systems with the strictest compliance requirements, including safety components of products, AI systems in areas like education, employment, public services, law enforcement, migration, and justice[21]

(3) Limited risk: AI systems that must disclose their artificial nature, including Chatbots, emotion recognition, biometric categorization, and deep fakes[22]

(4) Low or minimal risk: AI systems not covered by the above categories

c) Regulatory requirements for AI systems

(1) The Act imposes various requirements on AI systems, particularly those classified as high-risk[23]

(2) High-risk AI systems must undergo conformity assessments before deployment[24]

(3) Continuous monitoring and human oversight are mandatory to ensure compliance[25]

(4) Transparency and traceability requirements ensure AI decision-making processes are understandable and accountable[26]

d) Impact on lawyers using AI

(1) Law firms using AI, especially in high-risk areas, must comply with the AI Act's provisions

(2) Law firms need to allocate resources for compliance, including risk assessments and documentation

(3) Training staff on AI-related ethical and legal standards becomes essential

(4) Law firms may need to adjust their AI strategies to align with regulatory requirements

B. US AI frameworks

1. Existing US privacy laws

a) Data minimization requirements

(1) US privacy laws, such as the California Consumer Privacy Act (CCPA)[27], emphasize data minimization, requiring organizations to collect only the data necessary for their purposes

(2) AI systems must be designed to minimize data collection and processing

(3) Regular audits are required to ensure compliance with data minimization principles

b) Consent requirements

(1) US privacy laws mandate obtaining consent from individuals before collecting or processing their personal data, similar to GDPR[28]

(2) AI systems must include functionalities to manage consent effectively

(3) Transparent communication about AI data processing practices is required

(4) Consent mechanisms need to be robust and easily accessible to users[29]

[19] The purpose of this Regulation is to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence (AI), while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union and supporting innovation. See Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 2024 O.J. (L 219) 1.

[20] See Regulation (EU) 2024/1689, art. 5, 2024 O.J. (L 219) 1.

[21] See Regulation (EU) 2024/1689, art. 6, 2024 O.J. (L 219) 1.

[22] See Regulation (EU) 2024/1689, art. 50, 2024 O.J. (L 219) 1.

[23] See Regulation (EU) 2024/1689, arts. 8–15, 2024 O.J. (L 219) 1.

[24] See Regulation (EU) 2024/1689, art. 11, 2024 O.J. (L 219) 1.

[25] See Regulation (EU) 2024/1689, art. 14, 2024 O.J. (L 219) 1.

[26] See Regulation (EU) 2024/1689, art. 13, 2024 O.J. (L 219) 1.

[27] A business' collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes. See Cal. Civ. Code §§ 1798.100–1798.199 (West 2023).

[28] A controller shall…not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent. See N.J. Stat. Ann. § 56:8-166.12 (West 2024).

[29] A controller shall provide an effective mechanism for a consumer to revoke the consumer's consent under this section that is at least as easy as the mechanism by which the consumer provided the consumer's consent. See Md. Code Ann., Com. Law §§ 14-4601-14-4613 (West 2024).

c) Control by data subjects

(1) Privacy laws grant individuals control over their personal data, including rights to access, correction, and deletion[30]

(2) AI systems must allow data subjects to exercise their rights easily

(3) Data portability features should be integrated into AI systems to comply with access and transfer requests

(4) Law firms must ensure that AI-generated insights and decisions are reversible if individuals exercise their rights

2. US AI protection laws

a) Overview of new laws in Colorado, California, and Utah: All states have introduced specific AI protection laws focusing on transparency, accountability, and consumer protection

b) Utah: On March 27, 2025 SB0226 became law, effective May 7, 2025. SB0226:

(1) Requires entities using generative AI to disclose this use to consumers[31]

(2) Prohibits entities from blaming AI for violations of consumer protection laws

(3) Disclosures must be prominent, verbal at the start of conversations, or in writing before the start of a written interaction.[32]

(4) Fines for violations can reach $2,500 per infraction, with additional penalties from the Utah Attorney General for repeated offenses

3. Colorado: On May 17, 2024, SB205[33] became law, effective February 1, 2026

a) This legislation focuses on "high-risk AI systems" and mandates developers and deployers to use reasonable care to prevent algorithmic discrimination, with a rebuttable presumption of care if certain criteria are met

b) Enforcement is exclusively handled by the Colorado State Attorney General

c) Similar to the EU AI Act

(1) Categorizes AI systems by risk levels

(2) Imposes stricter regulations on high-risk systems

(3) Requires transparency and disclosure to consumers regarding AI use and its decision-making processes

(4) Mandates that developers and deployers ensure their AI systems do not cause harm or discrimination and that they follow specific procedures to mitigate risks

4. California: As of September 28, 2024 SB 942 and AB 2013 became law, effective January 1, 2026.

a) SB 942

(1) Legislation focuses on Generative AI providers with over 1 million monthly subscribers and mandates developers offer access to a free, publicly accessible AI detection tool.

(2) Developers must also include visible and imperceptible disclosures in AI-generated content. Disclosures should clearly indicate AI-generated content and be challenging to remove.[34]

b) AB 2013

(1) Legislation applies to developers that design, code, produce, or substantially modify generative AI systems made publicly available to Californians.

(2) Developers must post a high-level summary of the datasets used to train their AI systems including:

- How the datasets further the AI system's purpose
- Whether the datasets contain personal or aggregated consumer data
- Any modification made to the dataset
- The use of synthetic data generation
- Whether the datasets include copyrighted, trademarked, or patented data, or are in the public domain.[35]

---

[30] A consumer may invoke the consumer rights authorized pursuant to this subsection at any time by submitting a request to a controller specifying the consumer rights the consumer wishes to invoke…A controller shall comply with an authenticated consumer request to exercise the right:

1. To confirm whether or not a controller is processing the consumer's personal data and to access such personal data;
2. To correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;
3. To delete personal data provided by or obtained about the consumer;
4. To obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hinderance, where the processing is carried out by automated means; and
5. To opt out of the processing of the personal data for purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

See Va. Code Ann. §§ 59.1-575–59.1-585 (2023).

[31] An individual providing services in a regulated occupation shall prominently disclose when an individual receiving services is interacting with generative artificial intelligence in the provision of regulated services if the use of generative artificial intelligence constitutes a high-risk artificial intelligence interaction. See Utah S.B. 226 § 3, 2025 Gen. Sess. (Utah 2025).

[32] See Id.

[33] See Colo. S.B. 24-205, 2024 Reg. Sess. (Colo. 2024).

[34] A covered provider shall offer the user the option to include a manifest disclosure in image, video, or audio content, or content that is any combination thereof, created or altered by the covered provider's GENAI system that meets all the following criteria:
(1) The disclosure identifies content as AI-generated content.
(2) The disclosure is clear, conspicuous, appropriate for the medium of the content, and understandable to a reasonable person.
(3) The disclosure is permanent or extraordinarily difficult to remove, to the extent it is technically feasible.
See Cal. S.B. 942, 2023–2024 Reg. Sess. (Cal. 2024).

[35] On or before January 1, 2026, and before each time thereafter that a generative artificial intelligence system or service, or a substantial modification to a generative artificial intelligence system or service, released on or after January 1, 2022, is made publicly available to Californians for use, regardless of

V. Best Practices and Legal Compliance for Organizations Using AI

A. Training staff on defining and understanding AI

1. Provide comprehensive training to staff on AI concepts, applications, and ethical considerations

a) Basics of AI: Machine learning, deep learning, and generative AI

b) Ethical use of AI: Fairness, transparency, and accountability

c) Ongoing education: Keeping up-to-date with AI developments and regulations

whether the terms of that use include compensation, the developer of the system or service shall post on the developer's internet website documentation regarding the data used by the developer to train the generative artificial intelligence system or service, including, but not be limited to, all of the following:
(a) A high-level summary of the datasets used in the development of the generative artificial intelligence system or service, including, but not limited to:
(1) The sources or owners of the datasets.
(2) A description of how the datasets further the intended purpose of the artificial intelligence system or service.
(3) The number of data points included in the datasets, which may be in general ranges, and with estimated figures for dynamic datasets.
(4) A description of the types of data points within the datasets. For purposes of this paragraph, the following definitions apply:
(A) As applied to datasets that include labels, "types of data points" means the types of labels used.
(B) As applied to datasets without labeling, "types of data points" refers to the general characteristics.
(5) Whether the datasets include any data protected by copyright, trademark, or patent, or whether the datasets are entirely in the public domain.
(6) Whether the datasets were purchased or licensed by the developer.
(7) Whether the datasets include personal information, as defined in subdivision (v) of Section 1798.140.
(8) Whether the datasets include aggregate consumer information, as defined in subdivision (b) of Section 1798.140.
(9) Whether there was any cleaning, processing, or other modification to the datasets by the developer, including the intended purpose of those efforts in relation to the artificial intelligence system or service.
(10) The time period during which the data in the datasets were collected, including a notice if the data collection is ongoing.
(11) The dates the datasets were first used during the development of the artificial intelligence system or service.
(12) Whether the generative artificial intelligence system or service used or continuously uses synthetic data generation in its development. A developer may include a description of the functional need or desired purpose of the synthetic data in relation to the intended purpose of the system or service.
See Cal. A.B. 2013, 2023–2024 Reg. Sess. (Cal. 2024).

B. Developing clear limitations on AI usage

1. Establish guidelines and policies to define the acceptable use of AI within the organization

2. Define permissible uses of AI: Ensure AI applications align with organizational values and mission

3. Set boundaries: Avoid uses of AI that could lead to discrimination or privacy breaches

4. Monitoring and enforcement: Regularly review and enforce AI usage policies

C. Intellectual property considerations

1. Ensure that AI-generated content respects intellectual property rights and avoids infringement

a) Licensing: Obtain licenses for all third-party content used in AI tools

b) Permissions: Secure permissions from content creators for use in AI tools

c) Originality: Ensure AI-generated content is original and does not violate existing copyrights

D. Implementing audit and fact-checking procedures

1. Develop protocols to audit AI systems and verify the accuracy of AI-generated outputs

a) Regular audits: Conduct periodic audits to assess AI system performance and compliance

b) Fact-checking: Verify the accuracy of AI-generated content before use or dissemination

c) Accountability: Assign responsibility for AI oversight to specific team members

E. Ensuring confidentiality of sensitive information

1. Protect the confidentiality of personal and sensitive information processed by AI systems

a) Data protection: Implement measures to safeguard personal data. Implement systems in keeping with consent requirements, data minimization principles under GDPR, EU AI Act, and US privacy and AI-oriented law.

b) Restrict use of organizational proprietary information

c) Secure storage: Ensure data is stored securely and access is restricted

d) Breach response: Develop protocols for responding to data breaches and mitigating their impact

F. Anti-discrimination measures

1. Implement measures to prevent discrimination and bias in AI systems

2. Bias detection: Regularly test AI systems for biases and discriminatory outcomes

3. Inclusive design: Involve diverse stakeholders in AI development to identify and mitigate biases

4. Policy enforcement: Ensure compliance with anti-discrimination policies through regular monitoring and training

VI. Recent Developments in US Data Privacy

A. Recent surge in data privacy laws in the US

1. There has been a significant increase in the number of states enacting data privacy laws aimed at protecting consumers' personal information, nearly 20[36] while nine[37] additional states have active bills introduced, in committee, or in cross committee.

2. Notable lack of exemptions in many states for nonprofits (Oregon, Colorado, Minnesota, Maryland, Delaware, New Jersey). Other states with limited definitions for "nonprofit" exemptions, e.g., Texas, Iowa, Montana, Indiana.

[36] California, Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, Virginia
[37] Illinois, Maine, Massachusetts, New York, North Carolina, Oklahoma, Pennsylvania, Vermont, Wisconsin

B. Basic requirements for user control over personally identifiable information (PII)

1. Data privacy laws impose several requirements to ensure users have control over their PII, with which AI systems must comply[38]:

a) *Right to access*

(1) Users must be able to access the personal data collected about them

(2) AI systems need to include mechanisms that allow users to request and obtain their data in a readable format

b) *Right to correct*

(1) Users must have the ability to correct inaccurate or incomplete personal data

(2) AI systems should enable users to request corrections and ensure that updated information is reflected in AI processing

c) *Right to delete*

(1) Users have the right to request the deletion of their personal data

(2) AI systems must support data erasure requests and ensure that deleted data is no longer processed

d) *Right to opt-out*

(1) Users can opt out of the sale or sharing of their personal data

(2) AI systems need to provide clear opt-out options and respect user preferences regarding data usage

e) *Data portability*

(1) Users have the right to transfer their data from one service provider to another

(2) AI systems must facilitate data portability, allowing users to move their data seamlessly

Please click here to download a sample AI Usage Policy courtesy of Wagenmaker & Oberly, LLC.

Note: *When you click the link, the file will not open in the web browser. Instead, it will trigger an instant file download. In order to access the file, please remember to check your device's downloads folder.*

[38] See supra note 19.

ADDENDUM A

17 U.S.C.A. §1201-1205 (Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998)

§1201. Circumvention of Copyright Protection Systems
(a) Violations regarding circumvention of technological measures.—

(1)(A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter.

(B) The prohibition contained in subparagraph (A) shall not apply to persons who are users of a copyrighted work which is in a particular class of works, if such persons are, or are likely to be in the succeeding 3-year period, adversely affected by virtue of such prohibition in their ability to make noninfringing uses of that particular class of works under this title, as determined under subparagraph (C).

(C) During the 2-year period described in subparagraph (A), and during each succeeding 3-year period, the Librarian of Congress, upon the recommendation of the Register of Copyrights, who shall consult with the Assistant Secretary for Communications and Information of the Department of Commerce and report and comment on his or her views in making such recommendation, shall make the determination in a rulemaking proceeding for purposes of subparagraph (B) of whether persons who are users of a copyrighted work are, or are likely to be in the succeeding 3-year period, adversely affected by the prohibition under subparagraph (A) in their ability to make noninfringing uses under this title of a particular class of copyrighted works. In conducting such rulemaking, the Librarian shall examine--

(i) the availability for use of copyrighted works;

(ii) the availability for use of works for organization archival, preservation, and educational purposes;

(iii) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research;

(iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and

(v) such other factors as the Librarian considers appropriate.

(D) The Librarian shall publish any class of copyrighted works for which the Librarian has determined, pursuant to the rulemaking conducted under subparagraph (C), that

noninfringing uses by persons who are users of a copyrighted work are, or are likely to be, adversely affected, and the prohibition contained in subparagraph (A) shall not apply to such users with respect to such class of works for the ensuing 3-year period.

(E) Neither the exception under subparagraph (B) from the applicability of the prohibition contained in subparagraph (A), nor any determination made in a rulemaking conducted under subparagraph (C), may be used as a defense in any action to enforce any provision of this title other than this paragraph.

(2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—

(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;

(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

(3) As used in this subsection--

(A) to "circumvent a technological measure" means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner; and

(B) a technological measure "effectively controls access to a work" if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.

(b) Additional violations.—

(1) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—

(A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;

(B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological

measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.

(2) As used in this subsection--

(A) to "circumvent protection afforded by a technological measure" means avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure; and

(B) a technological measure "effectively protects a right of a copyright owner under this title" if the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title.

(c) Other rights, etc., not affected.—

(1) Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title.

(2) Nothing in this section shall enlarge or diminish vicarious or contributory liability for copyright infringement in connection with any technology, product, service, device, component, or part thereof.

(3) Nothing in this section shall require that the design of, or design and selection of parts and components for, a consumer electronics, telecommunications, or computing product provide for a response to any particular technological measure, so long as such part or component, or the product in which such part or component is integrated, does not otherwise fall within the prohibitions of subsection (a)(2) or (b)(1).

(4) Nothing in this section shall enlarge or diminish any rights of free speech or the press for activities using consumer electronics, telecommunications, or computing products.

(d) Exemption for nonprofit libraries, archives, and educational institutions.—

(1) A nonprofit library, archives, or educational institution which gains access to a commercially exploited copyrighted work solely in order to make a good faith determination of whether to acquire a copy of that work for the sole purpose of engaging in conduct permitted under this title shall not be in violation of subsection (a)(1)(A). A copy of a work to which access has been gained under this paragraph--

(A) may not be retained longer than necessary to make such good faith determination; and

(B) may not be used for any other purpose.

(2) The exemption made available under paragraph (1) shall only apply with respect to a work when an identical copy of that work is not reasonably available in another form.

(3) A nonprofit library, archives, or educational institution that willfully for the purpose of commercial advantage or financial gain violates paragraph (1)—

(A) shall, for the first offense, be subject to the civil remedies under section 1203; and

(B) shall, for repeated or subsequent offenses, in addition to the civil remedies under section 1203, forfeit the exemption provided under paragraph (1).

(4) This subsection may not be used as a defense to a claim under subsection (a)(2) or (b), nor may this subsection permit a nonprofit library, archives, or educational institution to manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, component, or part thereof, which circumvents a technological measure.

(5) In order for a library or archives to qualify for the exemption under this subsection, the collections of that library or archives shall be—

(A) open to the public; or

(B) available not only to researchers affiliated with the library or archives or with the institution of which it is a part, but also to other persons doing research in a specialized field.

(e) Law enforcement, intelligence, and other government activities.
--This section does not prohibit any lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee of the United States, a State, or a political subdivision of a State, or a person acting pursuant to a contract with the United States, a State, or a political subdivision of a State. For purposes of this subsection, the term "information security" means activities carried out in order to identify and address the vulnerabilities of a government computer, computer system, or computer network.

(f) Reverse engineering.—

(1) Notwithstanding the provisions of subsection (a)(1)(A), a person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure that effectively controls access to a particular portion of that program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to the person engaging in the

circumvention, to the extent any such acts of identification and analysis do not constitute infringement under this title.

(2) Notwithstanding the provisions of subsections (a)(2) and (b), a person may develop and employ technological means to circumvent a technological measure, or to circumvent protection afforded by a technological measure, in order to enable the identification and analysis under paragraph (1), or for the purpose of enabling interoperability of an independently created computer program with other programs, if such means are necessary to achieve such interoperability, to the extent that doing so does not constitute infringement under this title.

(3) The information acquired through the acts permitted under paragraph (1), and the means permitted under paragraph (2), may be made available to others if the person referred to in paragraph (1) or (2), as the case may be, provides such information or means solely for the purpose of enabling interoperability of an independently created computer program with other programs, and to the extent that doing so does not constitute infringement under this title or violate applicable law other than this section.

(4) For purposes of this subsection, the term "interoperability" means the ability of computer programs to exchange information, and of such programs mutually to use the information which has been exchanged.

(g) Encryption research.—

(1) Definitions.--For purposes of this subsection--

(A) the term "encryption research" means activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products; and

(B) the term "encryption technology" means the scrambling and descrambling of information using mathematical formulas or algorithms.

(2) Permissible acts of encryption research.--Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure as applied to a copy, phonorecord, performance, or display of a published work in the course of an act of good faith encryption research if--

(A) the person lawfully obtained the encrypted copy, phonorecord, performance, or display of the published work;

(B) such act is necessary to conduct such encryption research;

(C) the person made a good faith effort to obtain authorization before the circumvention; and

(D) such act does not constitute infringement under this title or a violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986.

(3) Factors in determining exemption.--In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include--

(A) whether the information derived from the encryption research was disseminated, and if so, whether it was disseminated in a manner reasonably calculated to advance the state of knowledge or development of encryption technology, versus whether it was disseminated in a manner that facilitates infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security;

(B) whether the person is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology; and

(C) whether the person provides the copyright owner of the work to which the technological measure is applied with notice of the findings and documentation of the research, and the time when such notice is provided.

(4) Use of technological means for research activities.--Notwithstanding the provisions of subsection (a)(2), it is not a violation of that subsection for a person to--

(A) develop and employ technological means to circumvent a technological measure for the sole purpose of that person performing the acts of good faith encryption research described in paragraph (2); and

(B) provide the technological means to another person with whom he or she is working collaboratively for the purpose of conducting the acts of good faith encryption research described in paragraph (2) or for the purpose of having that other person verify his or her acts of good faith encryption research described in paragraph (2).

(5) Report to Congress.--Not later than 1 year after the date of the enactment of this chapter, the Register of Copyrights and the Assistant Secretary for Communications and Information of the Department of Commerce shall jointly report to the Congress on the effect this subsection has had on--

(A) encryption research and the development of encryption technology;

(B) the adequacy and effectiveness of technological measures designed to protect copyrighted works; and

(C) protection of copyright owners against the unauthorized access to their encrypted copyrighted works.

The report shall include legislative recommendations, if any.

(h) Exceptions regarding minors.--In applying subsection (a) to a component or part, the court may consider the necessity for its intended and actual incorporation in a technology, product, service, or device, which--

(1) does not itself violate the provisions of this title; and

(2) has the sole purpose to prevent the access of minors to material on the Internet.

(i) Protection of personally identifying information.--

(1) Circumvention permitted.--Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure that effectively controls access to a work protected under this title, if--

(A) the technological measure, or the work it protects, contains the capability of collecting or disseminating personally identifying information reflecting the online activities of a natural person who seeks to gain access to the work protected;

(B) in the normal course of its operation, the technological measure, or the work it protects, collects or disseminates personally identifying information about the person who seeks to gain access to the work protected, without providing conspicuous notice of such collection or dissemination to such person, and without providing such person with the capability to prevent or restrict such collection or dissemination;

(C) the act of circumvention has the sole effect of identifying and disabling the capability described in subparagraph (A), and has no other effect on the ability of any person to gain access to any work; and

(D) the act of circumvention is carried out solely for the purpose of preventing the collection or dissemination of personally identifying information about a natural person who seeks to gain access to the work protected, and is not in violation of any other law.

(2) Inapplicability to certain technological measures.--This subsection does not apply to a technological measure, or a work it protects, that does not collect or disseminate personally identifying information and that is disclosed to a user as not having or using such capability.

(j) Security testing.--

(1) Definition.--For purposes of this subsection, the term "security testing" means accessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network.

(2) Permissible acts of security testing.--Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to engage in an act of security testing, if such act does not constitute infringement under this title or a violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986.

(3) Factors in determining exemption.--In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include--

(A) whether the information derived from the security testing was used solely to promote the security of the owner or operator of such computer, computer system or computer network, or shared directly with the developer of such computer, computer system, or computer network; and

(B) whether the information derived from the security testing was used or maintained in a manner that does not facilitate infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security.

(4) Use of technological means for security testing.--Notwithstanding the provisions of subsection (a)(2), it is not a violation of that subsection for a person to develop, produce, distribute or employ technological means for the sole purpose of performing the acts of security testing described in subsection (2),[1] provided such technological means does not otherwise violate section[2] (a)(2).

(k) Certain analog devices and certain technological measures.--

(1) Certain analog devices.--

(A) Effective 18 months after the date of the enactment of this chapter, no person shall manufacture, import, offer to the public, provide or otherwise traffic in any--

(i) VHS format analog video cassette recorder unless such recorder conforms to the automatic gain control copy control technology;

(ii) 8mm format analog video cassette camcorder unless such camcorder conforms to the automatic gain control technology;

(iii) Beta format analog video cassette recorder, unless such recorder conforms to the automatic gain control copy control technology, except that this requirement shall not apply until there are 1,000 Beta format analog video cassette recorders sold in the United States in any one calendar year after the date of the enactment of this chapter;

(iv) 8mm format analog video cassette recorder that is not an analog video cassette camcorder, unless such recorder conforms to the automatic gain control copy control technology, except that this requirement shall not

apply until there are 20,000 such recorders sold in the United States in any one calendar year after the date of the enactment of this chapter; or

(v) analog video cassette recorder that records using an NTSC format video input and that is not otherwise covered under clauses (i) through (iv), unless such device conforms to the automatic gain control copy control technology.

(B) Effective on the date of the enactment of this chapter, no person shall manufacture, import, offer to the public, provide or otherwise traffic in--

(i) any VHS format analog video cassette recorder or any 8mm format analog video cassette recorder if the design of the model of such recorder has been modified after such date of enactment so that a model of recorder that previously conformed to the automatic gain control copy control technology no longer conforms to such technology; or

(ii) any VHS format analog video cassette recorder, or any 8mm format analog video cassette recorder that is not an 8mm analog video cassette camcorder, if the design of the model of such recorder has been modified after such date of enactment so that a model of recorder that previously conformed to the four-line colorstripe copy control technology no longer conforms to such technology.

Manufacturers that have not previously manufactured or sold a VHS format analog video cassette recorder, or an 8mm format analog cassette recorder, shall be required to conform to the four-line colorstripe copy control technology in the initial model of any such recorder manufactured after the date of the enactment of this chapter, and thereafter to continue conforming to the four-line colorstripe copy control technology. For purposes of this subparagraph, an analog video cassette recorder "conforms to" the four-line colorstripe copy control technology if it records a signal that, when played back by the playback function of that recorder in the normal viewing mode, exhibits, on a reference display device, a display containing distracting visible lines through portions of the viewable picture.

(2) Certain encoding restrictions.--No person shall apply the automatic gain control copy control technology or colorstripe copy control technology to prevent or limit consumer copying except such copying—

(A) of a single transmission, or specified group of transmissions, of live events or of audiovisual works for which a member of the public has exercised choice in selecting the transmissions, including the content of the transmissions or the time

of receipt of such transmissions, or both, and as to which such member is charged a separate fee for each such transmission or specified group of transmissions;

(B) from a copy of a transmission of a live event or an audiovisual work if such transmission is provided by a channel or service where payment is made by a member of the public for such channel or service in the form of a subscription fee that entitles the member of the public to receive all of the programming contained in such channel or service;

(C) from a physical medium containing one or more prerecorded audiovisual works; or

(D) from a copy of a transmission described in subparagraph (A) or from a copy made from a physical medium described in subparagraph (C).

In the event that a transmission meets both the conditions set forth in subparagraph (A) and those set forth in subparagraph (B), the transmission shall be treated as a transmission described in subparagraph (A).

(3) Inapplicability.--This subsection shall not--

(A) require any analog video cassette camcorder to conform to the automatic gain control copy control technology with respect to any video signal received through a camera lens;

(B) apply to the manufacture, importation, offer for sale, provision of, or other trafficking in, any professional analog video cassette recorder; or

(C) apply to the offer for sale or provision of, or other trafficking in, any previously owned analog video cassette recorder, if such recorder was legally manufactured and sold when new and not subsequently modified in violation of paragraph (1)(B).

(4) Definitions.--For purposes of this subsection:

(A) An "analog video cassette recorder" means a device that records, or a device that includes a function that records, on electromagnetic tape in an analog format the electronic impulses produced by the video and audio portions of a television program, motion picture, or other form of audiovisual work.

(B) An "analog video cassette camcorder" means an analog video cassette recorder that contains a recording function that operates through a camera lens and through a video input that may be connected with a television or other video playback device.

(C) An analog video cassette recorder "conforms" to the automatic gain control copy control technology if it--

(i) detects one or more of the elements of such technology and does not record the motion picture or transmission protected by such technology; or

(ii) records a signal that, when played back, exhibits a meaningfully distorted or degraded display.

(D) The term "professional analog video cassette recorder" means an analog video cassette recorder that is designed, manufactured, marketed, and intended for use by a person who regularly employs such a device for a lawful business or industrial use, including making, performing, displaying, distributing, or transmitting copies of motion pictures on a commercial scale.

(E) The terms "VHS format", "8mm format", "Beta format", "automatic gain control copy control technology", "colorstripe copy control technology", "four-line version of the colorstripe copy control technology", and "NTSC" have the meanings that are commonly understood in the consumer electronics and motion picture industries as of the date of the enactment of this chapter.

(5) Violations.--Any violation of paragraph (1) of this subsection shall be treated as a violation of subsection (b)(1) of this section. Any violation of paragraph (2) of this subsection shall be deemed an "act of circumvention" for the purposes of section 1203(c)(3)(A) of this chapter.

§1202. Integrity of Copyright Management Information

(a) False copyright management information.--No person shall knowingly and with the intent to induce, enable, facilitate, or conceal infringement--

(1) provide copyright management information that is false, or

(2) distribute or import for distribution copyright management information that is false.

(b) Removal or alteration of copyright management information.--No person shall, without the authority of the copyright owner or the law--

(1) intentionally remove or alter any copyright management information,

(2) distribute or import for distribution copyright management information knowing that the copyright management information has been removed or altered without authority of the copyright owner or the law, or

(3) distribute, import for distribution, or publicly perform works, copies of works, or phonorecords, knowing that copyright management information has been removed or altered without authority of the copyright owner or the law, knowing, or, with respect to civil remedies under section 1203, having reasonable grounds to know, that it will induce, enable, facilitate, or conceal an infringement of any right under this title.

(c) Definition.--As used in this section, the term "copyright management information" means any of the following information conveyed in connection with copies or phonorecords of a work or performances or displays of a work, including in digital form,

except that such term does not include any personally identifying information about a user of a work or of a copy, phonorecord, performance, or display of a work:

(1) The title and other information identifying the work, including the information set forth on a notice of copyright.

(2) The name of, and other identifying information about, the author of a work.

(3) The name of, and other identifying information about, the copyright owner of the work, including the information set forth in a notice of copyright.

(4) With the exception of public performances of works by radio and television broadcast stations, the name of, and other identifying information about, a performer whose performance is fixed in a work other than an audiovisual work.

(5) With the exception of public performances of works by radio and television broadcast stations, in the case of an audiovisual work, the name of, and other identifying information about, a writer, performer, or director who is credited in the audiovisual work.

(6) Terms and conditions for use of the work.

(7) Identifying numbers or symbols referring to such information or links to such information.

(8) Such other information as the Register of Copyrights may prescribe by regulation, except that the Register of Copyrights may not require the provision of any information concerning the user of a copyrighted work.

(d) Law enforcement, intelligence, and other government activities.--This section does not prohibit any lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee of the United States, a State, or a political subdivision of a State, or a person acting pursuant to a contract with the United States, a State, or a political subdivision of a State. For purposes of this subsection, the term "information security" means activities carried out in order to identify and address the vulnerabilities of a government computer, computer system, or computer network.

(e) Limitations on liability.--

(1) Analog transmissions.--In the case of an analog transmission, a person who is making transmissions in its capacity as a broadcast station, or as a cable system, or someone who provides programming to such station or system, shall not be liable for a violation of subsection (b) if--

(A) avoiding the activity that constitutes such violation is not technically feasible or would create an undue financial hardship on such person; and

(B) such person did not intend, by engaging in such activity, to induce, enable, facilitate, or conceal infringement of a right under this title.

(2) Digital transmissions.--

(A) If a digital transmission standard for the placement of copyright management information for a category of works is set in a voluntary, consensus

standard-setting process involving a representative cross-section of broadcast stations or cable systems and copyright owners of a category of works that are intended for public performance by such stations or systems, a person identified in paragraph (1) shall not be liable for a violation of subsection (b) with respect to the particular copyright management information addressed by such standard if--

(i) the placement of such information by someone other than such person is not in accordance with such standard; and

(ii) the activity that constitutes such violation is not intended to induce, enable, facilitate, or conceal infringement of a right under this title.

(B) Until a digital transmission standard has been set pursuant to subparagraph (A) with respect to the placement of copyright management information for a category of works, a person identified in paragraph (1) shall not be liable for a violation of subsection (b) with respect to such copyright management information, if the activity that constitutes such violation is not intended to induce, enable, facilitate, or conceal infringement of a right under this title, and if--

(i) the transmission of such information by such person would result in a perceptible visual or aural degradation of the digital signal; or

(ii) the transmission of such information by such person would conflict with--

(I) an applicable government regulation relating to transmission of information in a digital signal;

(II) an applicable industry-wide standard relating to the transmission of information in a digital signal that was adopted by a voluntary consensus standards body prior to the effective date of this chapter; or

(III) an applicable industry-wide standard relating to the transmission of information in a digital signal that was adopted in a voluntary, consensus standards-setting process open to participation by a representative cross-section of broadcast stations or cable systems and copyright owners of a category of works that are intended for public performance by such stations or systems.

(3) Definitions.--As used in this subsection--

(A) the term "broadcast station" has the meaning given that term in section 3 of the Communications Act of 1934 (47 U.S.C. 153); and

(B) the term "cable system" has the meaning given that term in section 602 of the Communications Act of 1934 (47 U.S.C. 522).

§1203. Civil Remedies

(a) Civil actions.--Any person injured by a violation of section 1201 or 1202 may bring a civil action in an appropriate United States district court for such violation.

(b) Powers of the court.--In an action brought under subsection (a), the court--

(1) may grant temporary and permanent injunctions on such terms as it deems reasonable to prevent or restrain a violation, but in no event shall impose a prior restraint on free speech or the press protected under the 1st amendment to the Constitution;

(2) at any time while an action is pending, may order the impounding, on such terms as it deems reasonable, of any device or product that is in the custody or control of the alleged violator and that the court has reasonable cause to believe was involved in a violation;

(3) may award damages under subsection (c);

(4) in its discretion may allow the recovery of costs by or against any party other than the United States or an officer thereof;

(5) in its discretion may award reasonable attorney's fees to the prevailing party; and

(6) may, as part of a final judgment or decree finding a violation, order the remedial modification or the destruction of any device or product involved in the violation that is in the custody or control of the violator or has been impounded under paragraph (2).

(c) Award of damages.--

(1) In general.--Except as otherwise provided in this title, a person committing a violation of section 1201 or 1202 is liable for either--

(A) the actual damages and any additional profits of the violator, as provided in paragraph (2), or

(B) statutory damages, as provided in paragraph (3).

(2) Actual damages.--The court shall award to the complaining party the actual damages suffered by the party as a result of the violation, and any profits of the violator that are attributable to the violation and are not taken into account in computing the actual damages, if the complaining party elects such damages at any time before final judgment is entered.

(3) Statutory damages.—

(A) At any time before final judgment is entered, a complaining party may elect to recover an award of statutory damages for each violation of section 1201 in the sum of not less than $200 or more than $2,500 per act of circumvention, device, product, component, offer, or performance of service, as the court considers just.

(B) At any time before final judgment is entered, a complaining party may elect to recover an award of statutory damages for each violation of section 1202 in the sum of not less than $2,500 or more than $25,000.

(4) Repeated violations.--In any case in which the injured party sustains the burden of proving, and the court finds, that a person has violated section 1201 or 1202 within 3 years after a final judgment was entered against the person for another such

violation, the court may increase the award of damages up to triple the amount that would otherwise be awarded, as the court considers just.

(5) Innocent violations.--

(A) In general.--The court in its discretion may reduce or remit the total award of damages in any case in which the violator sustains the burden of proving, and the court finds, that the violator was not aware and had no reason to believe that its acts constituted a violation.

(B) Nonprofit library, archives, educational institutions, or public broadcasting entities.--

(i) Definition.--In this subparagraph, the term "public broadcasting entity" has the meaning given such term under section 118(f).

(ii) In general.--In the case of a nonprofit library, archives, educational institution, or public broadcasting entity, the court shall remit damages in any case in which the library, archives, educational institution, or public broadcasting entity sustains the burden of proving, and the court finds, that the library, archives, educational institution, or public broadcasting entity was not aware and had no reason to believe that its acts constituted a violation.

§1204. Criminal Offenses and Penalties

(a) In general.--Any person who violates section 1201 or 1202 willfully and for purposes of commercial advantage or private financial gain--

(1) shall be fined not more than $500,000 or imprisoned for not more than 5 years, or both, for the first offense; and

(2) shall be fined not more than $1,000,000 or imprisoned for not more than 10 years, or both, for any subsequent offense.

(b) Limitation for nonprofit library, archives, educational institution, or public broadcasting entity.--Subsection (a) shall not apply to a nonprofit library, archives, educational institution, or public broadcasting entity (as defined under section 118(f)).

(c) Statute of limitations.--No criminal proceeding shall be brought under this section unless such proceeding is commenced within 5 years after the cause of action arose.

§1205. Saving Clause

Nothing in this chapter abrogates, diminishes, or weakens the provisions of, nor provides any defense or element of mitigation in a criminal prosecution or civil action under, any Federal or State law that prevents the violation of the privacy of an individual in connection with the individual's use of the Internet.

ADDENDUM B

Cal. Civ. Code § 3344

Use of another's name, voice, signature, photograph, or likeness for advertising or selling or soliciting purposes

(a) Any person who knowingly uses another's name, voice, signature, photograph, or likeness, in any manner, on or in products, merchandise, or goods, or for purposes of advertising or selling, or soliciting purchases of, products, merchandise, goods or services, without such person's prior consent, or, in the case of a minor, the prior consent of his parent or legal guardian, shall be liable for any damages sustained by the person or persons injured as a result thereof. In addition, in any action brought under this section, the person who violated the section shall be liable to the injured party or parties in an amount equal to the greater of seven hundred fifty dollars ($750) or the actual damages suffered by him or her as a result of the unauthorized use, and any profits from the unauthorized use that are attributable to the use and are not taken into account in computing the actual damages. In establishing such profits, the injured party or parties are required to present proof only of the gross revenue attributable to such use, and the person who violated this section is required to prove his or her deductible expenses. Punitive damages may also be awarded to the injured party or parties. The prevailing party in any action under this section shall also be entitled to attorney's fees and costs.

(b) As used in this section, “photograph” means any photograph or photographic reproduction, still or moving, or any videotape or live television transmission, of any person, such that the person is readily identifiable.

> (1) A person shall be deemed to be readily identifiable from a photograph when one who views the photograph with the naked eye can reasonably determine that the person depicted in the photograph is the same person who is complaining of its unauthorized use.
>
> (2) If the photograph includes more than one person so identifiable, then the person or persons complaining of the use shall be represented as individuals rather than solely as members of a definable group represented in the photograph. A definable group includes, but is not limited to, the following examples: a crowd at any sporting event, a crowd in any street or public building, the audience at any theatrical or stage production, a glee club, or a baseball team.
>
> (3) A person or persons shall be considered to be represented as members of a definable group if they are represented in the photograph solely as a result of being present at the time the photograph was taken and have not been singled out as individuals in any manner.

(c) Where a photograph or likeness of an employee of the person using the photograph or likeness appearing in the advertisement or other publication prepared by or in behalf of the user is only incidental, and not essential, to the purpose of the publication in which it appears, there shall arise a rebuttable presumption affecting the burden of producing evidence that the failure to obtain the consent of the employee was not a knowing use of the employee's photograph or likeness.

(d) For purposes of this section, a use of a name, voice, signature, photograph, or likeness in connection with any news, public affairs, or sports broadcast or account, or any political campaign, shall not constitute a use for which consent is required under subdivision (a).

(e) The use of a name, voice, signature, photograph, or likeness in a commercial medium shall not constitute a use for which consent is required under subdivision (a) solely because the material containing such use is commercially sponsored or contains paid advertising. Rather it shall be a question of fact whether or not the use of the person's name, voice, signature, photograph, or likeness was so directly connected with the commercial sponsorship or with the paid advertising as to constitute a use for which consent is required under subdivision (a).

(f) Nothing in this section shall apply to the owners or employees of any medium used for advertising, including, but not limited to, newspapers, magazines, radio and television networks and stations, cable television systems, billboards, and transit ads, by whom any advertisement or solicitation in violation of this section is published or disseminated, unless it is established that such owners or employees had knowledge of the unauthorized use of the person's name, voice, signature, photograph, or likeness as prohibited by this section.

(g) The remedies provided for in this section are cumulative and shall be in addition to any others provided for by law.

ADDENDUM C

29 U.S.C. § 626(a)–(b) (2022)

Prohibition of Age Discrimination

(a) Employer practices

It shall be unlawful for an employer—

> **(1)** to fail or refuse to hire or to discharge any individual or otherwise discriminate against any individual with respect to his compensation, terms, conditions, or privileges of employment, because of such individual's age;
>
> **(2)** to limit, segregate, or classify his employees in any way which would deprive or tend to deprive any individual of employment opportunities or otherwise adversely affect his status as an employee, because of such individual's age; or
>
> **(3)** to reduce the wage rate of any employee in order to comply with this chapter.

(b) Employment agency practices

It shall be unlawful for an employment agency to fail or refuse to refer for employment, or otherwise to discriminate against, any individual because of such individual's age, or to classify or refer for employment any individual on the basis of such individual's age.

ADDENDUM D

Fed. R. Civ. P. 11.

Signing Pleadings, Motions, and Other Papers; Representations to the Court; Sanctions

(a) Signature. Every pleading, written motion, and other paper must be signed by at least one attorney of record in the attorney's name--or by a party personally if the party is unrepresented. The paper must state the signer's address, e-mail address, and telephone number. Unless a rule or statute specifically states otherwise, a pleading need not be verified or accompanied by an affidavit. The court must strike an unsigned paper unless the omission is promptly corrected after being called to the attorney's or party's attention.

(b) Representations to the Court. By presenting to the court a pleading, written motion, or other paper--whether by signing, filing, submitting, or later advocating it--an attorney or unrepresented party certifies that to the best of the person's knowledge, information, and belief, formed after an inquiry reasonable under the circumstances:

(1) it is not being presented for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation;

(2) the claims, defenses, and other legal contentions are warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law;

(3) the factual contentions have evidentiary support or, if specifically so identified, will likely have evidentiary support after a reasonable opportunity for further investigation or discovery; and

(4) the denials of factual contentions are warranted on the evidence or, if specifically so identified, are reasonably based on belief or a lack of information.

(c) Sanctions.

(1) ***In General.*** If, after notice and a reasonable opportunity to respond, the court determines that Rule 11(b) has been violated, the court may impose an appropriate sanction on any attorney, law firm, or party that violated the rule or is responsible for the violation. Absent exceptional circumstances, a law firm must be held jointly responsible for a violation committed by its partner, associate, or employee.

(2) ***Motion for Sanctions.*** A motion for sanctions must be made separately from any other motion and must describe the specific conduct that allegedly violates Rule 11(b). The motion must be served under Rule 5, but it must not be filed or be presented to the court if the challenged paper, claim, defense, contention, or denial is withdrawn or appropriately corrected within 21 days after service or within another time the court sets. If

warranted, the court may award to the prevailing party the reasonable expenses, including attorney's fees, incurred for the motion.

(3) ***On the Court's Initiative.*** On its own, the court may order an attorney, law firm, or party to show cause why conduct specifically described in the order has not violated Rule 11(b).

(4) ***Nature of a Sanction.*** A sanction imposed under this rule must be limited to what suffices to deter repetition of the conduct or comparable conduct by others similarly situated. The sanction may include nonmonetary directives; an order to pay a penalty into court; or, if imposed on motion and warranted for effective deterrence, an order directing payment to the movant of part or all of the reasonable attorney's fees and other expenses directly resulting from the violation.

(5) ***Limitations on Monetary Sanctions.*** The court must not impose a monetary sanction:

(A) against a represented party for violating Rule 11(b)(2); or

(B) on its own, unless it issued the show-cause order under Rule 11(c)(3) before voluntary dismissal or settlement of the claims made by or against the party that is, or whose attorneys are, to be sanctioned.

(6) ***Requirements for an Order.*** An order imposing a sanction must describe the sanctioned conduct and explain the basis for the sanction.

(d) Inapplicability to Discovery. This rule does not apply to disclosures and discovery requests, responses, objections, and motions under Rules 26 through 37.