Tuesday, January 9 at 2:00pm

GIBSON DUNN 2024 CA MCLE BLITZ

AI Regulation + Governance:

Recapping the Year Behind, Previewing the Year Ahead

GIBSON DUNN

Agenda

01 State of AI

02 Recapping 2023: Legislation + Regulation

03 Recapping 2023: Enforcement + Litigation

04 Recapping 2023: Commercial Risk + Governance

05 Previewing 2024

1. State of AI

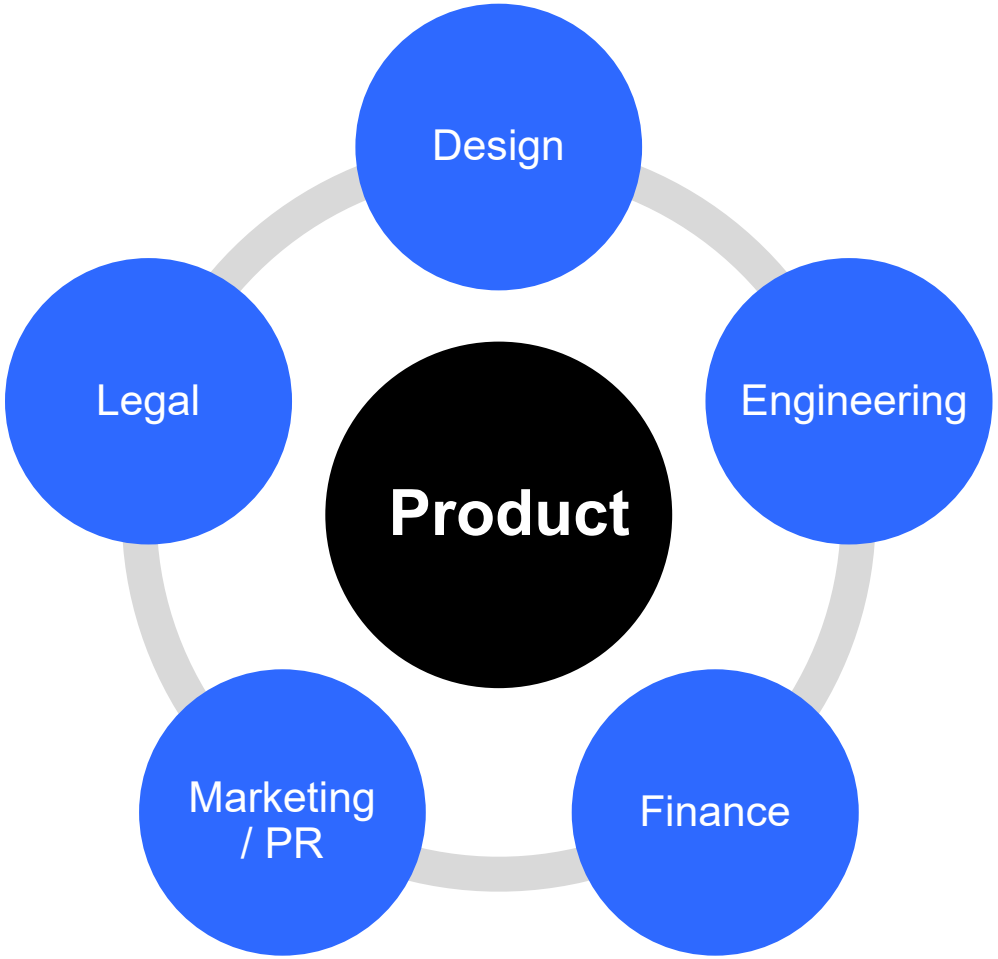
01

What Is AI?

“New” terminology

AI Use Cases

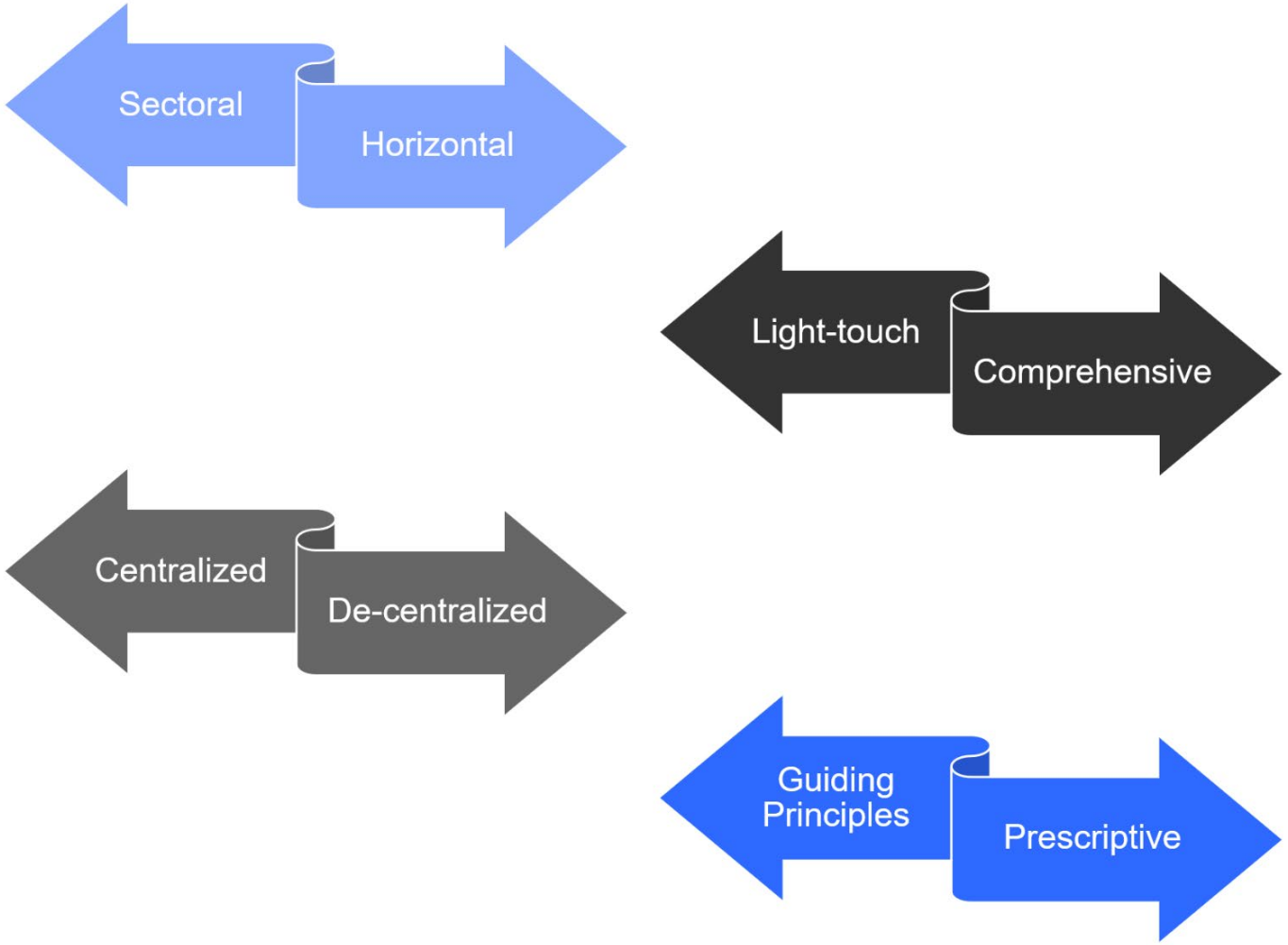
Affect Entire Company



AI-assisted...

- Coding / engineering
- Program recommendations
- Display / sequencing of recommendations
- Script / image / content generation
- Advertisements
- Pricing decisions
- Fraud detection / account misuse
- Creation of marketing assets
- Employment decisions
- Automating misc. high-volume tasks
- Product design
- Supporting R&D
- Customer service

Approaches to Regulating AI



2. Recapping 2023:
Legislation + Regulation

Select International
Regulatory Regimes / Proposals

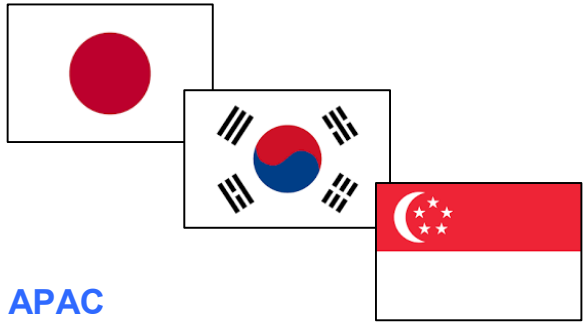
United Kingdom

- **Sectoral approach**: responsibility placed on existing regulators.
- Regulation based on five cross-cutting principles:

1. safety, security, and robustness;
2. appropriate transparency and explainability;
3. fairness;
4. accountability and governance; and
5. contestability and redress.

China

- **Centralized distributed approach**: various regulators are responsible for regulation.
- The Cyberspace Administration of China's rules regulating Generative AI came into effect in August.
- Proposed genAI Standards announced in October by the National Information Security Standardization Technical Committee (TC260).
- A draft AI law expected to be submitted to the legislative body of the PRC in 2024.



APAC

- **Japan**: Light touch approach to AI regulation. Recent regulatory reform has been to promote the development and use of AI.
- **South Korea**: Centralized regulation. Passed the Law on Nurturing the AI Industry and Establishing a Trust Basis in February 2023.
- **Singapore**: Light touch approach with a focus on fostering AI innovation. Instead of legislation, AI best-practice guidelines and an AI testing framework and toolkit.

European Union

- **Single comprehensive legislative framework** in the form of the AI Act.
- **Horizontal** (i.e., cross-sector) and **risk-based** approach.
- Complementary **product liability regimes** being developed.
- **Harmonized technical standards** to ensure interoperability.

EU AI Act
Overview

The EU AI Act Adopts a Risk-Based Approach to Regulating AI

- **Likely to become the first law on AI** by a major regulator, **directly** regulates AI systems based on **inherent risk.**
  - **Classifies AI use by risk level** (unacceptable, high, limited, and minimal), meaning that the AI Act tailors rules to the level of fundamental rights risks that AI systems can generate, and describes documentation, auditing, and process requirements for each risk level.
  - **High-risk systems** subject to onerous, ongoing requirements, including pre-deployment conformity assessments, technical and auditing requirements, and monitoring.
  - **Bans certain "unacceptable" use cases**, including facial recognition in public and indiscriminate web scraping of biometrics.
- **Extraterritorial effects** applicable to businesses that place AI systems on the market or put them into service in the EU, irrespective of whether providers are established in the EU or a third country.
- Regulation of **generative AI and copyright protections** will be enhanced.
- Procedural steps remain - notable staggered and rapid planned enforcement of certain provisions:
  - Provisions related to prohibited AI systems are set to become enforceable six months after the Act is finalized.
  - Provisions related to so-called General Purpose AI ("**GPAI**") become enforceable 12 months after this date.
  - The rest of the AI Act is expected to become enforceable in 2026.

Timeline of the AI Act

April 2021

The European Commission proposed the AI Act.

December 2022

The Council of the European Union adopted its common position ("general approach") on the AI Act.

June 2023

The European Parliament adopted its negotiating position on the AI Act.

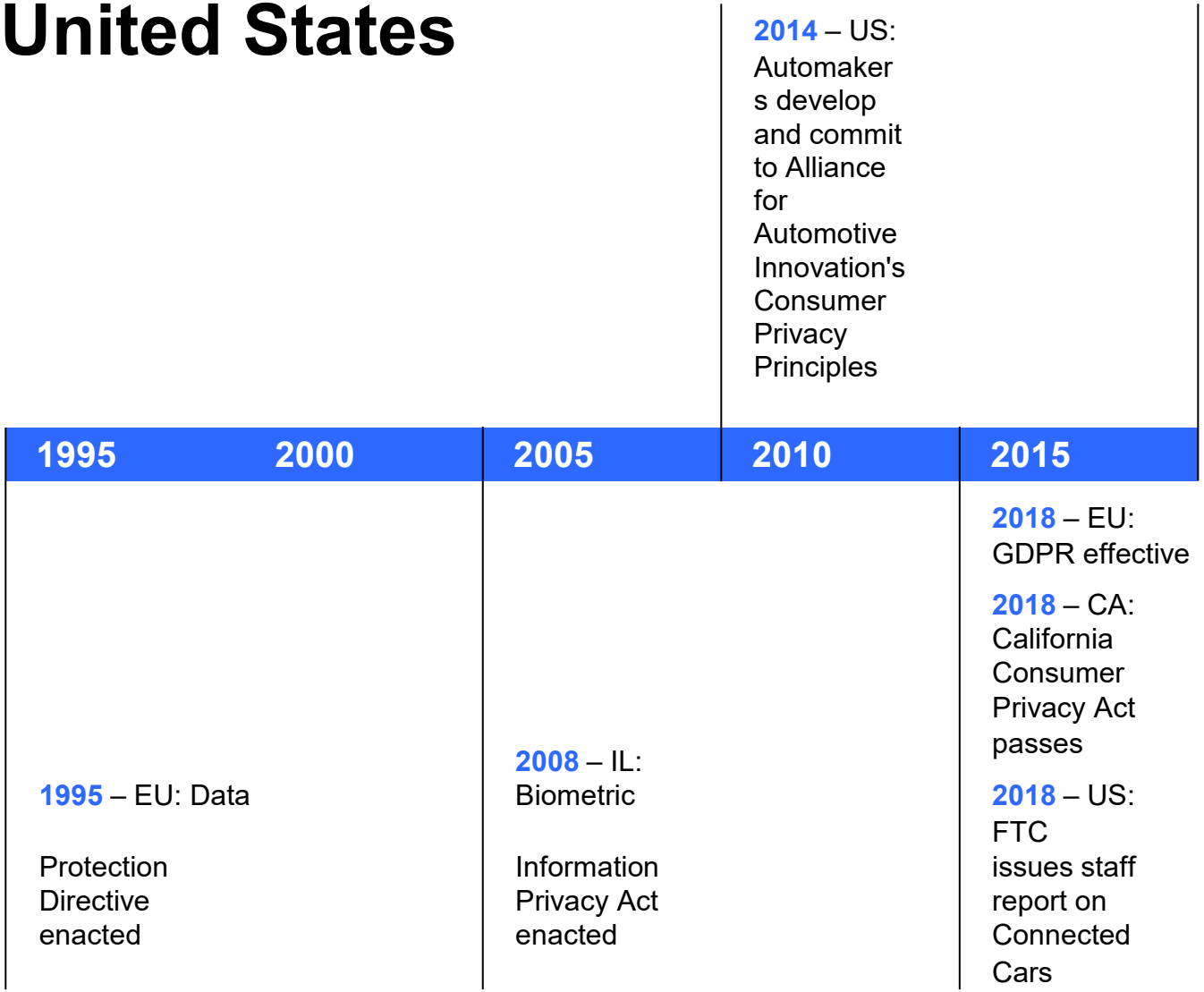
December 2023

Reconciliation of the three different versions of the AI Act through the "trilogue" procedure.*

*Procedural steps remain, including negotiations with member states over technical fineprint, scrutiny from regulators, sectoral agencies, and industry bodies, and integrating the AI Act proposals with existing regulatory frameworks. The final text is anticipated in **February 2023.**

Key Legal Developments

United States



2020 – CA: CCPA comes into effect; voters enact CPRA effective 2023

2020 – Illinois AI Video Interview Act (January 2020)

2020 – Maryland Use of Facial Recognition Services Law (October 2020)

2021 – VA, CO, CT, UT: 4 additional states pass comprehensive privacy laws

2022 – US: FTC ANPR re: "Commercial Surveillance and Data Security"

2022 – CA & Others: States consider vehicle-focused privacy legislation (e.g., CA SB 346)

2022 – US: White House Blueprint for an AI Bill of Rights

2022 – NYC: Local Law 144 on AEDTs is passed (in force July 5, 2023)

2023 – CPRA, other state privacy laws, and NYC Local Law 144 go into effect

2023 – NIST RMF 1.0

2023 – Proposed bills in California, Colorado, New Jersey, New York, Washington, D.C., Massachusetts, Vermont

2023 – White House Executive Order

Looking toward the future…

2024/5 – US: AI-focused federal + state legislation?

2025/6 – EU: AI Act?

United States
Regulatory Regimes / Proposals

- **Largely sectoral, self-regulatory approach – for now**
- **Presidential executive order** to create a reporting requirement for large foundational models and compute clusters
- **Regulatory guidance** and emergent **best practices/enforcement outcomes** that become "soft law," both cross-sector and sector-specific (FTC, EEOC, CFPB)
- White House-private sector **voluntary AI commitments**; publication of a Blueprint for AI Bill of Rights, ongoing efforts by the Senate to develop **AI legislative frameworks**
- **AI-specific legislation** mainly enacted at state and local level (e.g., NYC LL144, IL BIPA, CCPA/CPRA)
- Technical standards and benchmarks (e.g., **NIST AI Risk Management Framework**)
- **Court rulings and additional frameworks with impact** (*e.g.*, data access laws such as Massachusetts Right to Repair, copyright, anti-discrimination, antitrust, and product liability laws

Consumer Protection + Algorithmic Discrimination

Depending on the use case, AI models may implicate existing laws prohibiting bias or discrimination.

- April 25, 2023: **CFPB, DOJ, EEOC, and FTC** issued an "Interagency Enforcement Policy Statement on Artificial Intelligence" outlining balanced datasets, transparency, and contextualized design of AI systems as top enforcement priorities.
- FTC blogs emphasize:
  - "**Fair Credit Reporting Act**.
    - The FCRA comes into play in certain circumstances **where an algorithm is used to deny people employment, housing, credit, insurance, or other benefits**."
  - "**Equal Credit Opportunity Act.**
    - The ECOA **makes it illegal for a company to use a biased algorithm that results in credit discrimination** on the basis of race, color, religion, national origin, sex, marital status, age, or because a person receives public assistance."

Select State AI Laws + Regulations

NYC's Automated Employment Decision Tool (AEDT) Law

- On July 5, NYC's Department of Consumer and Worker Protection began enforcing its Automated Employment Decision Tool (AEDT) law, which went into effect in January 2023.
- Requires that employers and employment agencies in NYC complete a bias audit of the AEDT before using it to evaluate NYC job candidates and employees to ensure that the AI and algorithm-based technologies do not perpetuate biases.

State AI and Privacy Laws

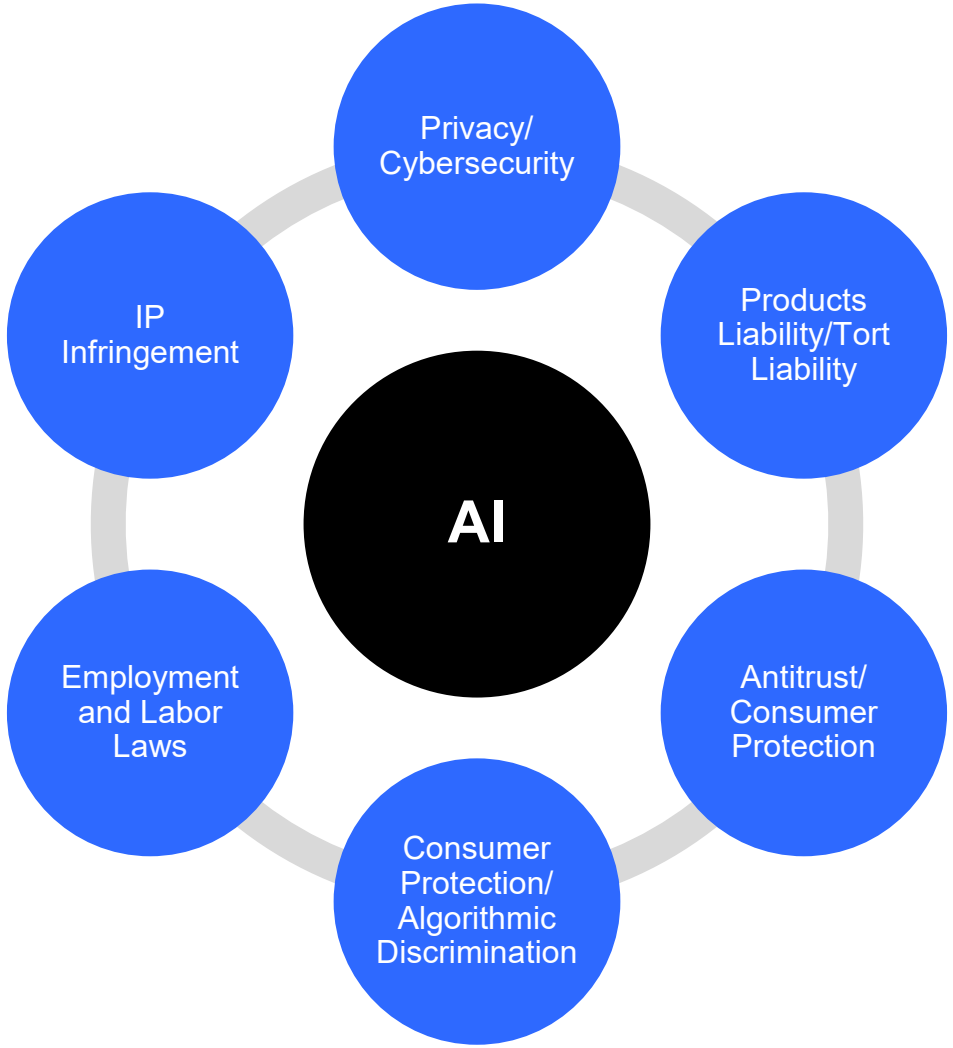
- State AI-related laws (including in Connecticut, the District of Columbia, and Massachusetts) have focused on "developing and maintaining trust" in AI.
- Existing state consumer privacy laws (including in California, Colorado, Connecticut, Delaware, Indiana, Montana, Oregon, Tennessee, Texas, Utah, and Virginia) require that companies provide opt-outs in connection with profiling in furtherance of automated decisions and conduct data protection assessments for processing activities that present a heightened risk of harm to consumers.

CPPA Draft Rulemaking on ADMT/AI

- On November 27, the CPPA released a set of draft regulations on automated decision-making technologies (ADMT) to facilitate discussion between CPPA board members. The formal rulemaking process has not yet begun; at a meeting on December 8, board members elected to revise the ADMT and risk assessment regulations for further discussion.
- The proposed rules reflect requirements to provide users with: (1) **notice of the ADMT use**; (2) **the ability to opt out of such use**; (3) **access rights**. The proposal also carves out key areas of discussion for the CPPA Board, including the profiling of children under 16 and the use of consumer information for model training.

3. Recapping 2023:
Enforcement + Litigation

Liability Risk Areas



Regulatory Enforcement – FTC Focus on AI

January 2021

FTC required **deletion of models and algorithms** allegedly developed using photos and videos obtained without express consent from users.

March 2022

FTC required company to **destroy models/algorithms** allegedly developed with the use of impermissibly collected data.

May 31, 2023

FTC filed a complaint and proposed settlement against a tech company for allegedly violating COPPA and the FTC Act by allegedly misrepresenting its data deletion practices, including the **use of personal data and human review for model training**.

June 29, 2023

FTC published a number of **guidelines on fairness and transparency in AI**, most recently warning companies not to use AI, including generative AI, in ways it deems **unfair or deceptive** under the FTC Act or that violates **competition laws**.

~July 13, 2023

FTC served a sweeping Civil Investigative Demand on ChatGPT developer OpenAI alleging **violations of privacy and consumer protection laws**.

November 2023

FTC approved a resolution streamlining FTC Staff's ability to **issue CIDs in investigations relating to AI**. The resolution will be in place for 10 years.

Regulatory Enforcement
FTC Spotlight

"… [N]o one should walk away from this settlement thinking that this Commission affirmatively supports the use of biometric surveillance in commercial settings […] there is a powerful policy argument that ***there are some decisions that should not be automated at all***; many technologies should never be deployed in the first place."
- Statement by Commissioner Bedoya

FTC Order Banning A Company's Use of AI

- On **December 19**, the FTC announced a proposed stipulated order that would ban a retail company from deploying, using, or assisting in the deployment or use of a facial recognition or analysis system for 5 years.

- The Order also directs the company to destroy all photos and videos of consumers that had been collected from facial recognition or analysis systems, as well as all data, models, or algorithms derived from those photos and videos.

- Notably, the complaint and Commissioner Bedoya's accompanying statement hints at the FTC's expectation for an effective algorithmic fairness compliance program and could be read as a blueprint for the FTC's future AI enforcement:

    - The settlement "**offers a strong baseline for what an algorithmic fairness program should look like**" beyond facial recognition use.

    - "Beyond giving people notice, ***industry should carefully consider how and when people can be enrolled in an automated decision-making system***, particularly when that system can substantially injure them."

Litigation Risk

A new wave of litigation

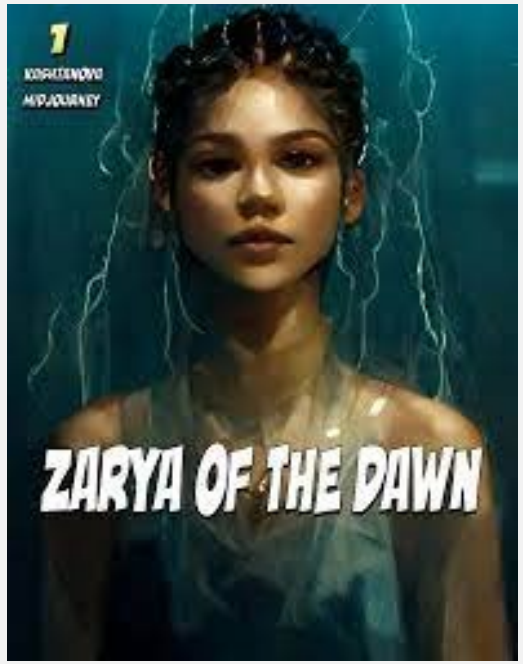
Numerous lawsuits (many proposed class actions) broadly allege that generative AI models/tools were trained on datasets that include copyrighted works and personal data. Clear litigation risks have emerged in connection with:

- **IP** - where **data used for model training** are subject to copyright or database rights; where **model outputs** may be substantially similar to copyrighted works
- **Data privacy** - where personal data was collected and used to train models

Another set of lawsuits alleges the use of AI to make decisions impacting individuals in discriminatory and biased ways, demonstrating there is also litigation risk around the **use / implementation** of AI tools (whether proprietary or third-party acquired).

➢ Early notable rulings in **copyright** and **patent** cases.

Copyright Office Guidance + NOI



- (Probably) **no copyright protection for AI-generated outputs**
- Guidance from the U.S. Copyright Office (USCO) in March 2023: applicants have a **duty to disclose the inclusion of AI-generated content** in a work submitted for registration and must provide an explanation of the human author's contributions.
- In August 2023, the USCO concluded that AI-generated material will be copyrightable to the extent that it is the author's "**own original mental conception, to which [the author] gave visible form**."
- On August 30, the **Copyright Office published a Notice of Inquiry (NOI)** announcing that it is seeking input on "the copyright law and policy issues" raised by AI to help the agency study "whether legislative or regulatory steps in this area are warranted."
- On October 30, the FTC submitted a comment outlining **the FTC's views on the intersection of copyright AI policy and its enforcement mandate**, including that:
  - Content generated by AI replicating a creator's work may **unfairly harm creator's ability to compete while deceiving the consumer**.
  - Moves by large technology companies to indemnify customers' use of their generative AI tools may **entrench these firms' market power**.
- The FTC is also considering questions about **how liability should be apportioned** for the development and deployment of generative AI tools, including open source models or models "trained on data scraped from websites hosting pirated data."

AI + IP

Copyright

Inputs

- Copyright law prohibits reproduction and derivative works of protected material without permission
- **Data needed to train ML algorithms** (e.g., images, text, videos, software) may be protectable
- **Training involves making at least interim copies** of these existing works without permission
- Creates **risk any output may be deemed a derivative work and found infringing or trigger other license obligations**

Fair use

- Highly fact-specific, multi-factor test, subject to pending litigation
- Use *may* be "fair" if it does not negatively affect the potential market value of the copyrighted work and is **sufficiently transformative**
- Creators of AI tools may argue that use of training data is "fair" and characterize their use as "transformative," as the training does not impact demand for the original work and instead **creates and improves the generative AI system**

Outputs

- Outputs such as code or product designs may not be protectable
- A number of global jurisdictions, including the U.S., take the position that **an AI system cannot author content protectable by IP laws**
- If AI-generated outputs are not copyrightable, the "creator" of such outputs **will not have the exclusive rights** conferred by the copyright law
- Some protection may be possible in hybrid cases where there is **both the use of an AI tool and human effort**

4. Recapping 2023:
Commercial Risk + Governance

Compliance Challenges + Risks

Key Challenges

- Comprehensive frameworks governing AI as a technology, ranging from risk-based or rights-based approaches
- AI regulation as an outgrowth of existing consumer protection and privacy/data protection laws
- Sector or state/city-specific approaches
- Additional frameworks with impact (e.g., copyright, anti-discrimination, and product liability laws)
- Regulatory guidance and emergent best practices that become “soft law”
- Reliance on toolkits, testing frameworks, or voluntary guidance
- Regulatory sandboxes, certifications, and licensing regimes
- Technical standards and benchmarks

Key Risks

- Copyright / patent infringement / outputs may not be protectable
- Privacy
- Cybersecurity
- Loss of confidentiality / trade secrets
- Algorithmic discrimination / disparate impact
- Inaccuracy / quality control
- Business / reputational risk

AI + Privacy

General considerations

- The use of AI systems will **intensify** regulatory scrutiny over privacy practices, leading to **greater organizational reputational risk** and **compliance-based risks**
- The design and use of AI/ML systems should take into account **privacy principles**, as well as ensure their security, explainability, fairness, and human oversight (already covered by GDPR and other global privacy laws)
- Privacy regulators and data protection authorities continue expanding into AI governance, publishing guidelines (e.g., FTC Act, CCPA, and other state privacy laws, GDPR, BIPA, and other biometric laws)
- Regulatory / litigation risk in connection with the collection, processing, and use (**including secondary use for model training**) of personal information (e.g., biometric data / information that can be reasonably be linked with a particular individual)
- Frameworks for ethical algorithms, overseeing regulatory sandboxes, and testing

Specific touchpoints/risks

- Automated decision-making
- Datasets used to train AI systems (particularly legacy data)
- Use of third parties as vendors or contractors can increase organizational liability, due to difficulty with insufficient or impossible third-party vendor assessments, and uncertainty about controller and processor responsibilities

Confidentiality + Commercial Terms

Private or confidential user, company, or customer information may be **collected or exposed by AI systems**, especially by generative models and tools	Sharing customers', clients', or other third parties' confidential information with third parties via AI systems may also **violate contractual provisions**
Terms of service typically grant AI tools rights to collect and **share with third parties** personal information and often to use the data/content they ingest to **develop and improve their services**	Even where developers provide options to limit the use of inputs or outputs for model training, they will still generally have **some degree of access** to prompts and information shared
Risks can include **loss of IP** (e.g., insufficient protection of trade secrets or misappropriation of confidential information) and **litigation exposure** due to misuse of employee or user confidential information	Data leakage of company or employee, customer, or other third party information can also lead to **system security vulnerabilities and increased susceptibility to cyber attacks**

Compliance Programs

5. Previewing 2024

Legislative + Regulatory Trends

- **EU AI Act** finalized?
- **FTC likely to flex enforcement mandate** across privacy, consumer protection, antitrust, and copyright/digital ownership
- The IP landscape taking shape: **Copyright Office + US Patent Office Guidance**
- State legislation and regulatory enforcement focus on **data governance and usage in connection with AI** (e.g., employment, insurance, healthcare)
- Regulatory focus on the use of **sensitive data for model training** (e.g., biometric, financial, health)
- CPPA Draft Rulemaking Process on **ADMT/AI**
- **Executive Order** implementation
- Congressional legislative focus on **CSAM, deepfakes, and social media moderation/election issues**
- **NIST RMF** updates and NIST Working Group conclusions

Key Commercial Risks + Challenges

- **Aggressive federal agencies (particularly the FTC) and state AGs** with broad enforcement priorities across **privacy, consumer protection, digital ownership, and antitrust**
- Potential **impactful court rulings** on copyright/trademark and the fair use defense, potentially leading to a wave of litigation against model developers and - potentially - users, as well as on product liability and Section 230
- IP lawsuits against users of AI tools would see the various **indemnification provisions and waivers** tested
- **Cyber incidents and data leakages**, prompting widespread concern for deployers and users
- Continued **fragmentation of regulatory and governance requirements** across federal, state, and local agencies and laws
- Challenges in connection with data/model preservation and legal privilege in the context of **AI litigation**
- **Hardware** shortages

Technical Developments

- Proliferation of **open source** models and data sets
- Convergence of data modalities in **multimodal models**
- **AI-generated content creation** (e.g., digital replicas, music)
- Generative AI tools trained only on **licensed content**
- **Synthetic data**
- **Privacy-protective** approaches to data collection and model training
- **Watermarking** and other IP protections
- Increasing use of AI tools in cyber-**threat detection**

Presenters

Vivek Mohan

Partner
Palo Alto
+1 650.849.5345
vmohan@gibsondunn.com

Eric Vandevelde

Partner
Los Angeles
+1 213.229.7186
evandevelde@gibsondunn.com

Cassandra L. Gaedt-Sheckter

Partner
Palo Alto
+1 650.849.5203
cgaedt-sheckter@gibsondunn.com

Frances Waldmann

Of Counsel
Los Angeles
+1 213.229.7914
fwaldmann@gibsondunn.com