

AI in 2023-24: Legal Risks & Practical Considerations



John Yates
Partner
CORPORATE TECH GROUP
[jyates@mmmlaw.com](mailto: jyates@mmmlaw.com)
404-504-5444

October 25, 2023



AI in 2023-24: Legal Risks & Practical Considerations

1. Beware of Hallucinations & Resulting Legal Liability
2. Understand & Comply with Customer AI Restrictions
3. Assess Ownership of Your AI Outputs
4. Protect Confidentiality of Your AI Outputs
5. Develop Your AI Policy & Train Continually
6. Be Prepared for Onerous Licensing Terms
7. Include Protective Licensing Terms
8. Practical Considerations to Increase Your Valuation
9. Comply with AI Consumer Regulations
10. Where is AI Regulation Going?

OVERVIEW: Internal vs. External Use

Internal use: Use of AI as a *productivity tool* by company and its employees.

External use: Use of AI as an *integrated part* of the company's customer-facing products and services





Beware of Hallucinations & Resulting Legal Liability

Beware of over-reliance on potentially low-quality AI outputs:

- The generative natural language of AI hallucinates an answer to important questions requiring expertise, such as a legal question
- Inclusion of fake citations in a legal brief
- Contracts that read grammatically correct but do not actually serve the company
- Internal security policies which read beautifully but create fresh material risk for the company
- Can you disclaim liability in your customer agreements?



Understand & Comply with Customer AI Restrictions

Customer Restrictions: You might be violating a customer contract by using AI

- Beware of service and vendor contracts with big financial institutions
- Check with your customers first!
- Educate your team on the customer restrictions
- In addition to straight prohibitions, these could include onerous review and approval processes taking months to complete



Assess Ownership of Your AI Outputs

IP Ownership: You may not own the *outputs* of a third party AI.

- Degree of concern depends on the use case
- Beware of outputs that reflect important source of IP value for a company like source code
- In general, copyright law is unsettled about the copyrightability of AI outputs
- The U.S. Copyright Office is considering what position to take.



Protect Confidentiality of Your AI Outputs

Confidential Information: Companies or employees may be disclosing company or customer secrets to public available AIs. Such actions could:

- Violate customer agreements
- Be a data breach if the input is personal information
- Undermine your own trade secret protection
- Generally be a bad idea if public AIs ever start mining or disclosing their queries publicly



Develop Your AI Policy & Train Continually

Develop an internal AI Policy for your organization.

- Define for your employees *permitted* versus *prohibited* use of AI.
- Define data that can and cannot be input into an AI
- Address security risks
- Monitor and audit standards
- Develop incident reporting protocol

Define and implement training and awareness.

- *A policy that is merely a piece of paper on a shelf likely does your organization no real good!*



Be Prepared for Onerous Licensing Terms

Tech Dependencies

AI technology or computing infrastructure on which you rely may become unavailable or subject to restrictive licenses and unreasonable commercial terms



Include Protective Licensing Terms

Limit the License Scope & Disclaim Liability

Be Aware if you're using Open Source:

--If your AI uses certain open source licenses, you may have to share or distribute your own proprietary code and thereby substantially lose the commercial value of your own custom, costly development

Know the restriction on use of Biometrics:

--Use of 'biometric' information (including facial scans, fingerprints, voiceprints, and other data) requires special notice and individual, executed consent under some law (and may be restricted by some states)

Training Rights:

- You may not have the necessary rights to use data to train your AI
- Use of training data could therefore violate third party intellectual property rights or privacy rights



Practical Considerations

- AI helps drive valuations for businesses. If the value of *your* business is premised on integrating AI into your products and services, *do not treat AI legal issues as an afterthought.*
- Seek expert advice on contracting, IP ownership and licensing, data privacy and regulatory compliance.
- Define fundamental business positions for customer negotiations
 - For example -- we will not agree to customer terms that bring the ownership of our AI itself into question, no matter how valuable the contract.
 - Sometimes helpful to think through these issues in advance (before your core principles will be challenged in a particular context).



Other Considerations

- Important to understand that legal and compliance issues are best modelled as a *process* of continual evaluation and refinement of approach, rather than a one-and-done assessment.
- Think carefully about how your business will monitor and stay on top of these developments.
- Consider scheduling regular reviews of contracts, evolving business practices, customer demands, etc.



Comply with AI Consumer Regs

1. **Substantial Legal Effects.**

Companies must provide special notices, opt-outs, appeal rights, and/or conduct detailed 'impact assessments' for AIs that result in decisions 'substantially' impacting consumers

2. **Data Brokerage.** If AI scores, reports on, or produces output about individuals, companies are required by some new state laws to:

- A. Register with state authorities
- B. Provide notices
- C. Offer opt-outs
- D. Take other steps



Where is AI Regulation Going?

- AI is already regulated under existing laws (copyright, privacy, etc.), though the AI context sometimes presents novel issues of application.
 - The issues exist today and are not merely hypothetical
- Regulation will increase
 - Calls for comprehensive regulation in the U.S. (e.g., Chuck Schumer, White House AI Bill of Rights, legislation introduced in 17 states, other proposals)
 - Europe anticipated to pass AI Act:
 - Components such as consumer notice, regulatory review and registration, compliance assessments, transparency requirements (record keeping and logging of all *use* of your AI, publication of data used to train your AI)
 - Outright prohibitions on some uses such as predictive policing or social scoring
 - Substantial fines possible: 6% of global revenue and application outside the territory of the EU.
 - Other jurisdictions like Brazil are following the EU model.



Existing AI Laws and Regulations

Enacted

- California: Privacy Rights Act
- Connecticut: Personal Data Privacy and Online Monitoring Act
- Colorado: Privacy Act
- Indiana: Data Protection Act
- Montana: Consumer Data Privacy Act
- Tennessee: Information Protection Act
- Texas: Data Privacy and Security Act
- Virginia: Consumer Data Protection Act

Proposed Regulations/Guidelines

- United States: AI Bill of Rights
- United States: NTIA Inquiry
- European Union: AI Liability Directive
- United Kingdom: AI White Paper
- China: Measures for the Management of Generative AI Services

Proposed Laws

- European Union: AI Act
- District of Columbia: Stop Discrimination by Algorithms Act
- Maine: Data Privacy and Protection Act
- Massachusetts: Data Privacy Protection Act
- Massachusetts: HB1974
- Massachusetts: An Act Preventing a Dystopian Work Environment
- Massachusetts: SB31
- New Hampshire: SB 225
- Oregon: SB619
- New York: SB 365
- Pennsylvania: HB49
- Pennsylvania: HB708
- Rhode Island: Data Transparency and Privacy Protection Act
- Rhode Island: SB146
- Vermont: H114



National AI Proposals

United States

- [SAFE Innovation Framework](#): preemptive legislation with five central pillars—security, accountability, foundations, explanation, and innovation—which will be used to establish regulatory guardrails.
- [AI Bill of Rights](#): principles to guide the design, use, and deployment of automated systems.
- [NTIA Inquiry](#): an inquiry into AI to allow the National Telecommunications and Information Administration to formulate regulations creating accountability for AI.

International

- [AI Act](#) (European Union): legislation that would provide principles for ensuring human oversight, safety, transparency, traceability, non-discrimination, and environmental friendliness while taking a risk-based approach to AI.
- [AI Liability Directive](#) (European Union): introduces rules specific to damages caused by AI systems and is complementary to the AI Act.
- [Measures for the Management of Generative AI Services](#) (China): proposed regulations that would make companies providing generative AI services to the public responsible for the outputs of their systems and require that data used to train algorithms meet strict requirements.
- [AI White Paper](#) (United Kingdom): suggests a principles-based framework for regulators consistent with the UK's National AI Strategy.



State AI Laws

Enacted

- New York City: ***began enforcement on July 6 of its AI law, which requires employers to conduct audits of AI-enabled tools used for employment decisions.***

Proposed

- District of Columbia: would prohibit organizations from using algorithms that make decisions based on protected personal traits.
- Massachusetts: would regulate the use of AI for mental health services, regulate the use of automated decision making by employers, and create operating standards for companies with large-scale generative AI.
- Pennsylvania: would establish a registry of businesses operating artificial intelligence.
- Rhode Island: would prohibit certain uses of automated decision systems and algorithms in connection with video-lotteries and sports-betting.
- Vermont: would restrict the use of electronic monitoring of employees and the use of automated decision making for employment decisions.
- California, Hawaii, Illinois, Minnesota, New York, Washington, and West Virginia proposed laws in 2023 that would impact AI, which failed to pass.



State AI Laws

Privacy Laws Impacting AI

- Privacy laws passed in California, Connecticut, Colorado, Indiana, Montana, Texas and Virginia give consumers the right to opt-out of profiling and/or automated decision making.
- Colorado, Tennessee, and Texas also require data protection assessments for profiling that poses varying degrees of risk.

Proposed Privacy Laws Impacting AI

- Proposed laws in New Hampshire, Oregon, Pennsylvania, and Rhode Island would also give consumers the right to opt-out of profiling and/or automated decision making.
- Proposed laws in Pennsylvania and Rhode Island would also require data protection assessments for profiling that poses varying degree of risk.
- Maine: would require entities that use algorithms, including machine learning AI, complete an impact assessment and design evaluation of the algorithm.
- Massachusetts: would require companies to conduct an impact assessment if they use a covered algorithm.
- New York: would require companies to disclose their use of automated decision-making that could have a materially detrimental effect.

Thank you!



John Yates

Partner

CORPORATE TECH GROUP

[jyates@mmmlaw.com](mailto: jyates@mmmlaw.com)

404-504-5444