AI on Campus: Governance, Contracts, and Risk in a Rapidly Expanding Digital Landscape

CLE Written Materials

SAUL EWING LLP

CLE Materials Include:

1. Article: AI Corporate Policy – Top Ten Tips
2. Colorado Artificial Intelligence Act (SB24-205)
3. The EU AI Act
4. NYC Local Law 144
5. The Utah AI Policy Act
6. The FTC Act
7. The Civil Rights Act

AI Corporate Policy – Top Ten Tips

Original Publication Date: April 2024
By: Matt Kohel, Partner, Saul Ewing LLP

The use of artificial intelligence (AI) technologies in the workplace has become a regular occurrence and its adoption by companies is only going to increase. The unmanaged employee use of AI creates significant risks that can negatively impact an organization and even have broader social effects due to the unique nature of this evolving technology. It is therefore important that organizations develop policies addressing employee use of AI that are clear, practical, and tailored to its business to promote the responsible use of AI, while also mitigating the potential risks and challenges posed by AI systems.

Matt Kohel
Partner, Artificial Intelligence
Saul Ewing LLP
P: (410) 332-8710
E: matthew.kohel@saul.com

Saul Ewing attorneys can help clients develop corporate policies and respond to incidents when they arise. We believe that companies should follow these steps when preparing a corporate AI policy:

1. Take a proactive approach to managing the potential risks from employee use of AI.
2. Identify the risks specific to your organization, as well as individuals, and even the broader societal risks that may arise from the irresponsible use of AI. Prioritize those risk in the context of your organization's business operations.
3. Explain the risks to the executives in your organization and get buy-in from the C-suite in the formulation of your AI policy.
4. Design an AI policy that fits your organization's business operations and particular needs.
5. Work with a cross-functional team to utilize their expertise and make sure that your AI policy meets the needs of different stakeholders (e.g., IT, Sales and Marketing, Data Privacy, HR, Legal).
6. Draft an AI policy that is clear and easy to follow for employees in various roles and levels within your organization.

7. Draft a policy that explains the risks and scope of use – when and how employees can use AI to perform their work and what is not permitted. Make clear that non-compliance can result in discipline, including termination.
8. Access and security are key considerations. Implement electronic record-keeping to document and allow for auditing of AI use by employees.
9. Responsible AI use requires training and awareness programs. incorporate these initiatives into your organization's AI use procedures.
10. Develop and periodically measure metrics to determine employee compliance and identify gaps in your organization's AI policy.

Above all, understand that an AI policy is not a static but a "living document" that should be re-visited and updated to reflect changes in technology and trends in the use of AI. The landscape is continuously changing and new AI technologies are being made available to users at a rapid rate. The implementation of an effective AI policy requires adapting to the evolution of this emerging technology. Keep this card as a handy reminder of the steps to consider in formulating an AI policy for your organization.

Colorado Artificial Intelligence Act (SB24-205)

https://leg.colorado.gov/bill_files/47770/download

Bill Summary from Colorado General Assembly (2024 Regular Session):

BILL SUMMARY:

On and after February 1, 2026, the act requires a developer of a high-risk artificial intelligence system (high-risk system) to use reasonable care to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination in the high-risk system. There is a rebuttable presumption that a developer used reasonable care if the developer complied with specified provisions in the act, including:

- Making available to a deployer of the high-risk system a statement disclosing specified information about the high-risk system;
- Making available to a deployer of the high-risk system information and documentation necessary to complete an impact assessment of the high-risk system;
- Making a publicly available statement summarizing the types of high-risk systems that the developer has developed or intentionally and substantially modified and currently makes available to a deployer or other developer and how the developer manages any known or reasonably foreseeable risks of algorithmic

discrimination that may arise from the development or intentional and substantial modification of each of these high-risk systems; and

- Disclosing to the attorney general and known deployers or other developers of the high-risk system any known or reasonably foreseeable risks of algorithmic discrimination, within 90 days after the discovery or receipt of a credible report from the deployer, that the high-risk system has caused or is reasonably likely to have caused.

The act also, on and after February 1, 2026, requires a deployer of a high-risk system to use reasonable care to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination in the high-risk system. There is a rebuttable presumption that a deployer used reasonable care if the deployer complied with specified provisions in the act, including:

- Implementing a risk management policy and program for the high-risk system;
- Completing an impact assessment of the high-risk system;
- Annually reviewing the deployment of each high-risk system deployed by the deployer to ensure that the high-risk system is not causing algorithmic discrimination;
- Notifying a consumer of specified items if the high-risk system makes, or will be a substantial factor in making, a consequential decision concerning the consumer;
- Providing a consumer with an opportunity to correct any incorrect personal data that a high-risk system processed in making a consequential decision;
- Providing a consumer with an opportunity to appeal, via human review if technically feasible, an adverse consequential decision concerning the consumer arising from the deployment of a high-risk system;
- Making a publicly available statement summarizing the types of high-risk systems that the deployer currently deploys, how the deployer manages any known or reasonably foreseeable risks of algorithmic discrimination that may arise from deployment of each of these high-risk systems, and the nature, source, and extent of the information collected and used by the deployer; and
- Disclosing to the attorney general the discovery of algorithmic discrimination, within 90 days after the discovery, that the high-risk system has caused.

A person doing business in this state, including a deployer or other developer, that deploys or makes available an artificial intelligence system that is intended to interact with consumers must ensure disclosure to each consumer who interacts with the artificial intelligence system that the consumer is interacting with an artificial intelligence system.

The act does not restrict a developer's, deployer's, or other person's ability to engage in specified activities, including:

- Complying with federal, state, or municipal laws, ordinances, or regulations;
- Cooperating with and conducting specified investigations;
- Taking immediate steps to protect an interest that is essential for the life or physical safety of a consumer;
- Conducting and engaging in specified research activities; and
- Effectuating a product recall or repairing technical errors that impair product functionality.

The act provides an affirmative defense for a developer, deployer, or other person if:

- The developer, deployer, or other person involved in a potential violation is in compliance with a nationally or internationally recognized risk management framework for artificial intelligence systems that the act or the attorney general designates; and
- The developer, deployer, or other person takes specified measures to discover and correct violations of the act.

An insurer, a fraternal benefit society, or a developer of an artificial intelligence system used by an insurer is in full compliance with the act if the entity is subject to specified laws governing insurers' use of external consumer data and information sources, algorithms, and predictive models and rules adopted by the commissioner of insurance.

A bank, out-of-state bank, credit union chartered by the state of Colorado, federal credit union, out-of-state credit union, or any affiliate or subsidiary thereof, is in full compliance with the act if the entity is subject to examination by a state or federal prudential regulator under any published guidance or regulations that apply to the use of high-risk systems and the guidance or regulations meet criteria specified in the act.

The act grants the attorney general rule-making authority to implement, and exclusive authority to enforce, the requirements of the act. A person who violates the act engages in a deceptive trade practice pursuant to the "Colorado Consumer Protection Act".

APPROVED by Governor May 17, 2024

EFFECTIVE May 17, 2024

(Note: This summary applies to this bill as enacted.)

The EU AI Act

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

https://artificialintelligenceact.eu/wp-content/uploads/2021/08/The-AI-Act.pdf

High-level summary of the AI Act
Found at: https://artificialintelligenceact.eu/high-level-summary/

Four-point summary

The AI Act classifies AI according to its risk:

- Unacceptable risk is prohibited (e.g. social scoring systems and manipulative AI).
- Most of the text addresses high-risk AI systems, which are regulated.

- A smaller section handles limited risk AI systems, subject to lighter transparency obligations: developers and deployers must ensure that end-users are aware that they are interacting with AI (chatbots and deepfakes).
- Minimal risk is unregulated (including the majority of AI applications currently available on the EU single market, such as AI enabled video games and spam filters – at least in 2021; this is changing with generative AI).

The majority of obligations fall on providers (developers) of high-risk AI systems.

- Those that intend to place on the market or put into service high-risk AI systems in the EU, regardless of whether they are based in the EU or a third country.
- And also third country providers where the high risk AI system's output is used in the EU.

Users are natural or legal persons that deploy an AI system in a professional capacity, not affected end-users.

- Users (deployers) of high-risk AI systems have some obligations, though less than providers (developers).
- This applies to users located in the EU, and third country users where the AI system's output is used in the EU.

General purpose AI (GPAI):

- All GPAI model providers must provide technical documentation, instructions for use, comply with the Copyright Directive, and publish a summary about the content used for training.
- Free and open license GPAI model providers only need to comply with copyright and publish the training data summary, unless they present a systemic risk.
- All providers of GPAI models that present a systemic risk – open or closed – must also conduct model evaluations, adversarial testing, track and report serious incidents and ensure cybersecurity protections.

NYC Local Law 144

https://www.nyc.gov/site/dca/about/automated-employment-decision-tools.page

Summary: A Local Law to amend the administrative code of the city of New York, in relation to automated employment decision tools.

Utah AI Policy Act

S.B. 149 Artificial Intelligence Amendments

https://le.utah.gov/~2024/bills/static/SB0149.html

Highlighted Provisions:

This bill:

- defines terms;
- establishes liability for use of artificial intelligence (AI) that violates consumer protection laws if not properly disclosed;
- creates the Office of Artificial Intelligence Policy (office) and a regulatory AI analysis program;
- enables temporary mitigation of regulatory impacts during AI pilot testing;
- establishes the Artificial Intelligence Learning Laboratory Program to assess technologies, risks, and policy;
- requires disclosure when an individual interacts with AI in a regulated occupation; and grants the office rulemaking authority over AI programs and regulatory exemptions.

Continued on the following page...

Federal Trade Commission Act

https://www.ftc.gov/sites/default/files/documents/statutes/federal-trade-commission-act/ftc_act_incorporatingus_safe_web_act.pdf

SUMMARY:

Found at: https://www.ftc.gov/legal-library/browse/statutes/federal-trade-commission-act

The Federal Trade Commission Act is the primary statute of the Commission. Under this Act, as amended, the Commission is empowered, among other things, to (a) prevent unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce; (b) seek monetary redress and other relief for conduct injurious to consumers; (c) prescribe rules defining with specificity acts or practices that are unfair or deceptive, and establishing requirements designed to prevent such acts or practices; (d) gather and compile information and conduct investigations relating to the organization, business, practices, and management of entities engaged in commerce; and (e) make reports and legislative recommendations to Congress and the public. A number of other statutes listed here are enforced under the FTC Act.

H.R.6356 - Artificial Intelligence Civil Rights Act of 2025

https://www.congress.gov/bill/119th-congress/house-bill/6356/text

Official Title as Introduced: To establish protections for individual rights with respect to computational algorithms, and for other purposes.