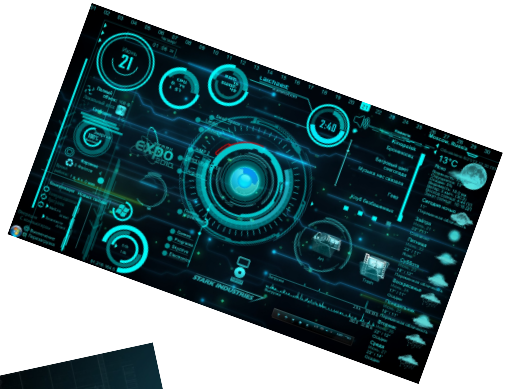
ARTIFICIAL INTELLIGENCE: MANAGING COMPLIANCE WHEN USING AI AND MACHINE LEARNING IN YOUR COMPANY

MOORE & VAN ALLEN, PLLC

JULES CARTER, BARBARA MEEKS, KARIN MCGINNIS

FEBRUARY 24, 2022

What is AI?



Artificial General Intelligence refers to the hypothetical ability of an intelligent agent to understand or learn any intellectual task that a human being can.

Moore&VanAllen

What is AI? (cont.)

Algorithm		Artificial Intelligence
An encoded procedure (basically, a set of rules) used to analyze and transform selected input into desired output based on mathematical assumptions.	**vs.**	A network of complex and adaptable algorithms capable of responding to the input they encounter by modifying or adding new algorithms to the network in order to better perform their target function.

What is AI?

- AI v. Machine Learning*
- **Basic AI (rule based).** (e.g. automated decision support) (e.g., pharma systems that group meds by therapeutic class, map drug-allergy cross-sensitivity, detect drug interactions, make dosage suggestions); planning and scheduling (i.e. smart thermostats); motion and manipulation (i.e., robotics, inc. prosthetics).
- **Machine Learning/ Computational Learning.** (e.g. self-driving cars; text to speech; spam-filtering programs; facial recognition, and many other things considered AI)
  - Involves human input, data and training.
  - **"Deep learning"**. Evolution of ML. Requires more data and artificial neural networks (to work like the human brain does).
- **Many types can fall into either category.** e.g. Chatbots -- computer program humans can have a conversation with (i.e., Siri, call center assistants, website assistants) and many can analyze data (customer needs)
  - AI: Rule based (programmed to recognize word or phrase and provide standard answer or take specific action); or
  - Machine learning (can recall what callers say to them and use for future interactions, so appear more flexible/human in interaction).

AI Across Applications

Artificial Intelligence

Knowledge Representation	Planning and Scheduling	Social Intelligence (Affective Computing)	Natural Language Processing
Automated video annotation/retrieval Automated clinical decision support	Smart thermostats **Unmanned vehicles**	Virtual assistants Customer support **Unmanned vehicles**	Virtual assistants Automated online assistants and "chatbots" Text auto-complete **Unmanned vehicles**

Perception	Motion and Manipulation (Robotics)	Computational Learning (Machine Learning)	Artificial General Intelligence
Speech Recognition Facial Recognition **Unmanned Vehicles**	Prosthetics Drones Industrial/manufacturing robots **Unmanned vehicles**	Email filtering Product and content recommendation **Unmanned vehicles**	*Refers to the **hypothetical** ability of an intelligent agent to understand or learn any intellectual task that a human being can.

How Does the Law Define AI?

How Does the Law Define AI? (cont.)

NAIIA National Artificial Intelligence Initiative Act of 2020. H.R. Res. 6395, 116th Cong. §§ 5001 et seq. (2020)

NAIIA defines "**artificial intelligence**" as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to—

(A) perceive real and virtual environments;
(B) abstract such perceptions into models through analysis in an automated manner; and
(C) use model inference to formulate options for information or action."

(2020 NDAA, Division E (NAIIA), § 5002(3)) It defines "**machine learning**" as "an application of artificial intelligence that is characterized by providing systems the ability to automatically learn and improve on the basis of data or experience, without being explicitly programmed."

(NDAA, Division E, § 5002(11))

EU – AI Proposed Regs COM/2021/206

- Risk based (High Risk AI is subject to greater requirements)
- Title II—certain AI prohibited (i.e., exploiting vulnerabilities of protected groups causing harm or subliminal messages to cause harm)
- Title III—significant obligations on providers of AI, and some obligations on users.
- Audits and government review and certification requirements.
- Transparency, instructions important.

EU—"Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Act" COM/2021/206 final

EU Proposed regulation

"Artificial Intelligence System": Software that is developed with one or more techniques and approaches listed in Annex 1 and can for a given set of human-defined objectives, generate outputs such as content, recommendations or decisions influencing the environments they interact with." (Art. 3(1)) The techniques and approaches in Annex 1 include:

(a) **machine learning approaches** including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;

(b) **logic and knowledge-based approaches** including knowledge representation, inductive (logic) programming, knowledge bases inference and deductive engines, (symbolic) reasoning and expert systems;

(c) **statistical approaches,** Bayesian estimation, search and optimization methods.

NYC Admin Code on Automated Employment Decision Tools

- Notice and audit requirements for AEDT used to screen candidates for employment or employees for promotion within NYC.

- *The term "automated employment decision tool" means any computational process, derived from machine learning, statistical modeling, data analytics, or artificial intelligence, that issues simplified output, including a score, classification, or recommendation, that is used to substantially assist or replace discretionary decision making for making employment decisions that impact natural persons. (NYC Admin Code 20-870, Eff. 1/1/2023)*

What are the Legal Concerns with AI?

- **Bias/Discrimination –** AI that that discriminates on the basis of a protected classification (constitutional issues; employment statutes; FTC; comprehensive privacy statutes/regulations; NYC Automated Employment Decision Tools; Illinois Artificial Intelligence Video Interview Act; see also consumer regulations below)
- **Privacy** – Data that is not properly obtained, or data that is used for a secondary purpose; issues of notice, consent, opt-in/outs, etc. (data broker laws; public records laws; GLBA; GDPR; comprehensive privacy legislation; Illinois and NYC laws).
- **Information Security** – Sensitive data that is not properly secured/protected (privacy and data security statutes).

What are the Legal Concerns with AI? (cont.)

- **Contract** – Use of proprietary AI or data in a manner that exceeds licenses or breaches agreements with third-party vendors.
- **Consumer Protection** – (FCRA; FTC Act; Equal Credit Opportunity Act; Fair Housing; Fair Lending)
- **Copyright** – Use of copyrighted material in a training dataset, resulting in exposure to civil liability.
- **Employment** – Collective bargaining in addition to discrimination issues.
- **Regulatory Risk** – Entrenched structures and systems that will likely be incompatible with future legislation (evolution of FTC guidance; CPRA/VCDPA/CPA and new states; CFPB possible regulations and UDAAP; NAIIA; SEC/FINRA/state laws regarding robo-advisory and digital investment advice tools; proposed EU regs).

Federal Trade Commission (FTC) Guidance

- *Aiming for truth, fairness, and equity in your company's use of AI.* https://www.ftc.gov/news-events/blogs/business-blog2021/04/aiming-truth-fairness-equity-your-companys-use-ai. Is the use of the algorithm " likely to cause substantial injury to consumers that is not reasonably avoidable by consumers and not outweighed by countervailing benefits to consumers or to competition."

    1. ***Start with the right foundation.*** (data integrity/robustness)
    2. ***Watch out for discriminatory outcomes.*** Testing.
    3. ***Embrace transparency and independence.***
    4. ***Don't exaggerate what your algorithm can do or whether it can deliver fair or unbiased results.***
    5. ***Tell the truth about how you use data.*** (Don't be an Everalbum)
    6. ***Do more good than harm*** (see above)
    7. ***Hold yourself accountable – or be ready for the FTC to do it .***

Federal Trade Commission Cases

- Using AI under the Fair Credit Reporting Act without reasonably assuring accuracy of AI-generated results
  - *FTC v. RealPage, Inc.* (3:18-cv-02739 (N.D. Tex. (Oct. 16, 2018)(FCRA. automated tenant applicant background screening)
- Lack of transparency in collecting data, misrepresentations regarding consumer rights, and failure to monitor vendors
  - *FTC v. Facebook, Inc.* 1:19-cv-02184 (D.D.C. July 24, 2019)(misrepresentation about user control over privacy/consent to use of data of user and "affected friends" by FB and third party developers; failure to vet vendors; retention of data; and misrepresentation regarding facial recognition opt-in).
- Lack of transparency and failure to gain consent for data collection activities
  - *FTC v. EverAlbum*, (May 6, 2021) (consumer photo-tagging used to develop Ever facial recognition software).

Bias and Discrimination – Case Studies

Targeted Advertising (who will get what ad)

- *Bradley v. T-Mobile (ND Cal. 2020)* (ADEA claim because defendants used age restricted Facebook job ads targeting younger users)

Criminal Justice

- *State v. Loomis (Wisc. 2016)* (COMPAS risk assessment AI based on interviews and aggregated data to predict recidivism based on groups in which the defendant belongs. The court also found that the trial court did not rely solely on the results of the risk assessment, but also considered factors outside of the COMPAS score.)

Addressing Multiple Issues:
State Comprehensive Privacy Laws

Comprehensive Privacy Laws: Colorado Privacy Act

- "Profiling" means "Any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location or movements." CRS §6-1-1303(20).

- "Targeted Advertising" means "displaying to a consumer an advertisement that is selected based on personal data obtained or inferred over time from the consumer's activities across nonaffiliated websites, applications, or online services to predict consumer preferences or interests" CRS §6-1-1303(25).

Comprehensive Privacy Laws: Colorado Privacy Act (cont.)

Transparency/Notice Requirements. Controllers must provide a reasonably accessible, clear and meaningful privacy notice to consumers that includes, among other things: (1) the categories of personal data collected or processed by the controller or a processor; (2) purposes for which personal data is processed; (3) how and where to exercise a consumer's individual rights; (4) the categories of personal data shared with third parties; (5) the categories of third parties with whom the controller shares personal data; and (6) the express purposes for which personal data is processed.

Comprehensive Privacy Laws: Colorado Privacy Act (cont.)

- *Nondiscrimination*. Controllers have duty to avoid unlawful discrimination "A controller shall not process personal data in violation of state or federal laws that prohibit unlawful discrimination against consumers." CRS §6-1-1308(6)
- *Data adequacy and minimization.* Collection of personal data must be adequate, relevant and limited to what is reasonably necessary in relation to the specified purposes for which the data is processed. CRS §6-1-1309(c)(3)
- *Secondary use.* Need consent for processing for purposes not reasonably necessary to or compatible with the specified purposes. CRA §6-1-1309(c)(4)

Comprehensive Privacy Laws: Colorado Privacy Act (cont.)

Risk-Based Rights. Right to opt out of processing for the purposes of targeted advertising, the sale of personal data or profiling for decisions in furtherance of "decisions that produce legal or similarly significant effects concerning a consumer."* Controller must provide "clear and conspicuous method." CRS §6-1-1306(1)(a).

*"a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services or access to essential goods or services" CRS § 6-1-1303(10)

Comprehensive Privacy Laws: Colorado Privacy Act (cont.)

Data Protection Assessments. (eff. 7/1/2023) Prohibits processing that presents a heightened risk of harm to a consumer without conducting and documenting a data protection assessment of each of its processing activities that involve personal data, including where the processing involves…:

- Targeted advertising or profiling that presents a reasonably foreseeable risk of
  - unfair or deceptive treatment of, or unlawful disparate impact on, consumers;
  - Financial or physical injury to consumers;
  - Physical or other intrusion...that would be offensive to a reasonable person; or
  - Other substantial injury to consumers.

The controller is required to make the assessment available to the Attorney General upon request. CRS § 6-1-1309

NAIIA

National Artificial Intelligence Initiative Act of 2020. H.R. Res. 6395, 116th Cong. §§ 5001 et seq. (2020)

- Coordinated effort of the Federal Government to accelerate AI research with Interagency Committee to support research on the ethical, legal, environmental, safety, security, bias, and other issues associated with AI
- Common definitions, characterizations, and other properties related to AI systems across all sectors
- National Institute of Standards will also include best practices and voluntary standards
- Objectives:
  - "[P]rovide or facilitate the availability of curated, standardized, secure, representative, aggregate, and privacy- protected data sets for artificial intelligence research and development." (NDAA, Section E, § 5103(d)).
  - Expand mission of the National Institute of Standards and Technology to include supporting the development of
    - "risk mitigation framework for deploying artificial intelligence systems;…
    - technical standards and guidelines that promote trustworthy artificial intelligence systems; and
    - technical standards and guidelines by which to test for bias in artificial intelligence training data and applications." (NDAA, Section E, § 5301)

White House: Office of Science and Technology Policy

- RFI on biometric technologies. https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies
- AI Bill of Rights. https://www.whitehouse.gov/ostp/news-updates/2021/11/10/join-the-effort-to-create-a-bill-of-rights-for-an-automated-society/ ; https://www.whitehouse.gov/ostp/news-updates/2021/10/22/icymi-wired-opinion-americans-need-a-bill-of-rights-for-an-ai-powered-world/
- Concerns about discrimination, incorrect results, bad data sets, training based on prior examples embedding prejudice, transparency, privacy, abuse, marginalization.
- ”AI developers not using appropriate data sets and not auditing systems comprehensively, as well as not having diverse perspectives around the table to anticipate and fix problems before products are used (or to kill products that can’t be fixed).”

Practical Recommendations for Risk Management and Governance

Moore&VanAllen

AI Risk Management Framework

- Model Inventory
- Training Data
- Usefulness and Sustainability Analysis
- Impact Assessments

- Testing
- Effective Challenge

- Governance
- Transparency
- Employee Training
- Data Privacy

- Live Monitoring
- Risk-Based Controls
- Recordkeeping and Retention
- Third-Party Risk Management

Moore&VanAllen

Model Inventory

- Establish and update enterprise-wide model inventory.

Training Data

- Determine the integrity of data by reviewing data collection protocols.
- Ensure training data population appropriately represent the population that the AI will ultimately be applied to. Limit use of model where necessary to account for data gaps.

Usefulness and Sustainability Analysis

- The legitimate purpose of AI and how the components (algorithm, data inputs etc.) are reasonably related or necessary to that legitimate purpose.

Impact Assessments

- Assess potential enterprise impacts and, where applicable, consumer impacts.
- Assess risk of AI being wrong.

Testing

- Backtesting – A form of cross-validation that involves testing a predictive model on historical data to estimate the performance of model if it had been employed during a past period.
- Stress testing – In what situations will the AI perform poorly or become unreliable?
- Bias testing
- Business-context metrics testing

Effective challenge

- Ensure model output is reviewed by subject-matter expert.
- Consider of alternative models that can achieve the legitimate purpose with a less discriminatory outcome, less risky variable or more accurate result.

Governance

- Establish appropriate operational performance thresholds based on business-context metrics testing.
- Ensure senior leadership and Board of Directors understand uses, risks and potential liability.
- Create formal policies and procedures for use of AI, including protocols for reporting results/impacts and escalation of material issues or policy breaches.
- Establish formal remediation and change-management process.
- Establish procedures to address internal and external complaints and feedback.

Transparency

- Update disclosures, privacy notices, and terms of use so that they are clear about use of AI and not misleading.

Employee Training

- Train employees on assigned responsibilities, escalation mechanisms, workflow management, and recordkeeping requirements. Employees must be retrained periodically and in response to conduct-based compliance failures.

Data Privacy

- Follow applicable data privacy laws.
- Use anonymized data sets where possible. Only use identifiable data if that is supported by a strong business justification.

Live Monitoring

- Conduct risk-based human oversight and supervision.
- Implement automated logging and audit-trail generation.

Audit

- Periodic audit, ideally, conducted by an independent party.

Recordkeeping and Retention

- Ensure remediation efforts are appropriately documented in model inventory.
- Follow retention schedule and keep the data secure.

Third-Party Risk Management

- Conduct risk-based diligence for vendors, evaluating the following:
  - business experience,
  - strategic plan,
  - financial condition,
  - risk management and controls,
  - information security,
  - legal and regulatory compliance, and
  - operational resilience (i.e. business continuity plan).
- Require third-party vendors to provide transparent and clear description of algorithm's operation, factors/criteria used, and other information needed to verify AI tool results and compliance with regulatory requirements.
- Subject AI tools to initial and ongoing inspection and testing.
- For licensed third-party software, review use restrictions.
- Require third-party vendors to warrant that AI tools comply with applicable laws and regulations.
- Address ongoing rights to consumer data.

Model Risk Management Guidance Examples (Financial Services Industry)

OCC Model Risk Management Handbook:

https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/model-risk-management/index-model-risk-management.html

FDIC Supervisory Guidance on Model Risk Management:

https://ww.fdic.gov/news/financial-institution-letters/2017/fil17022a.pdf

Tips with ongoing evolution of AI and the legal environment

- Keep up with your neighbors. Without clear do's and don't's, the reasonableness of what a company has done with its AI may depend on what other similarly situated companies have been able to do.
- Monitor state and federal legislation: Proposed 2022 Algorithmic Accountability Act (originally introduced 2019) would require commercial entities to conduct assessments of use of high-risk systems including AI
- Read comments to proposed regulations for potential comparables.

Questions?

Karin McGinnis
Member
704-331-1078
karinmcginnis@mvalaw.com

Jules Carter
Associate
704-331-3723
julescarter@mvalaw.com

Barbara Meeks
Member
704-331-1034
barbarameeks@mvalaw.com

Moore&VanAllen