


The image features a dark blue background with a complex, abstract pattern of white lines and dots, resembling a network or data flow. A solid orange vertical bar is positioned on the left side. The text 'MAYER | BROWN' is displayed in white, uppercase letters, with a thin orange vertical line separating the two names.

MAYER | BROWN

Artificial Intelligence & Financial Services Symposium

October 27, 2022


The background features a gradient from orange on the left to deep purple on the right. Overlaid on this are several sets of white, curved lines that resemble orbits or data paths, each with small white dots at various points. These lines are more prominent on the right side of the slide.

8:50a.m.-9:00a.m.
Opening Remarks

Opening Remarks



Jon Van Gorp
Chairman
Mayer Brown



9:00a.m.-9:55a.m.

Panel 1 - How Financial Institutions and Insurance Companies are Using AI

Speakers



Elizabeth (Eli) Corbett
*General Counsel and Chief
Compliance Officer*
Petal



Steve Kaplan
Partner
Mayer Brown



Gabriel Morgan Asaftei
Partner
McKinsey & Company



David Rosen
Co-Founder
Catylex

What is Artificial Intelligence (AI)

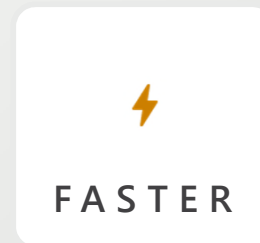
Use of machines to perform cognitive functions associated with human minds

INTENTIONALITY
INTELLIGENCE
ADAPTABILITY



Why Use AI

- Efficiency
- Scalability
- Risk management
- Market expectations





Historical Development of AI

Use Cases

1

Consumer credit and data
aggregation



**ELI
CORBETT**
*General Counsel and Chief
Compliance Officer
Petal*

2

Contract analytics and other
data management



**DAVID
ROSEN**
*Co-Founder
Catylex*

3

Other (asset managers,
banks, broker dealers,
insurers, investors)



GABRIEL
*Morgan
Partner
McKinsey & Company*

Opportunities and Challenges for Adopting AI

What are
short- and
long-term
opportunities?

What are the
greatest
obstacles to
adoption?



9:55a.m.-10:50a.m.

Panel 2 – Algorithmic Bias and “Unfair” Discrimination

Speakers



Dr. Lori Cenci
*US Head of
Unauthorized Trade
Surveillance*
HSBC



Niketa Patel
Partner
Mayer Brown



Jennifer Rosa
Partner
Mayer Brown



Tori Shinohara
Partner
Mayer Brown



Agenda

- AI Applications Gone Awry
- Regulation of AI
- How to Mitigate Against Bias In AI Applications

AI Applications Gone Awry



Regulation of AI

- Existing State Regulation/Guidance:
 - AI Task Forces and Commissions
 - Privacy laws and AI-specific laws
- Existing Federal Regulation/Guidance:
 - National AI Initiative Act
 - OMB Guidance
 - White House AI Bill of Rights
- In the pipeline:
 - AI-specific Bills in Congress



AI-Specific Federal Legislation and Guidance

EXISTING

- **National AI Initiative Act**
 - AI Risk assessment framework
 - NIST's AI Risk Management framework
- **OMB Guidance for AI Regulation**
 - 10 policy considerations
- **White House AI Bill of Rights**
 - 5 core principles



AI-Specific Federal Legislation In the Pipeline

- **The American Data Privacy And Protection Act (ADPPA)**
 - Proposed by the House Energy and Commerce Committee
 - Would be the first comprehensive federal legislation regarding privacy, AI bias, and data security issues
 - Would create national standards and safeguards for collection and use of personal information
 - Would establish protections for marginalized communities affected by potentially discriminatory uses of personal information

The ADPPA - Scope

- **Covered data**
 - Information that identifies or is linked or reasonably linkable to one or more individuals, including derived data and unique identifiers.
 - Excludes employee data and publicly-available data
- **Sensitive covered data**
 - Government identifiers (such as driver's license or Social Security numbers), as well as information related to health, geolocation, financials, log-in credentials, race, sexual history, and identity
- Who does ADPPA apply to?
 - **Covered Entities**
 - **Service Providers**
 - **Third Party Collecting Entities**

The ADPPA – Section 207

- AI Assessments
 - **Algorithm** – “computation process that uses machine learning, natural language processing, artificial intelligence techniques, or other computational processing techniques of similar or greater complexity that makes a decision or facilitate human decision-making with respect to covered data, including to determine the provision of products or services or to rank, order, promote, recommend, amplify, or similarly determine the delivery or display of information to an individual”
 - **Algorithmic Design Evaluation** – covered entities must evaluate the design, structure, and data inputs of the algorithm to reduce the risk of potential discriminatory impacts
 - **Algorithm Impact Assessment** – large data holders who use algorithms that may cause potential harm to an individual are required to assess the impacts of their AI use and submit a report to the FTC

Future FTC Regulation

- Advance Notice of Proposed Rulemaking (August 11, 2022)
 - **95 questions** regarding many of the same areas as the ADPPA
 - This ANPR also makes clear that the FTC is interested in expanding its ability to protect consumers, including by expanding the FTC's authority to seek **financial penalties for first-time violations**.
 - Comments must be received on or before **November 21, 2022**

State Task Forces and Commissions

- AI task forces and commissions:
 - Alabama Council on Advanced Technology and Artificial Intelligence
 - California Future of Work Commission
 - Illinois Future of Work Task Force
 - Massachusetts Future of Work Special Commission
 - New York Artificial Intelligence, Robotics, and Automation Commission; New York Commission on the Future of Work
 - Utah Deep Technology Talent Initiative
 - Vermont Artificial Intelligence Commission
 - Washington Automated Decisions-Making System Workgroup
 - Colorado Task Force for the Consideration of Facial Recognition Services
 - And more bills pending in **Rhode Island, New Jersey, Pennsylvania, North Carolina, Maryland, Virginia, and Maine.**

AI Specific State Legislation & Guidance

- California Privacy Rights Act (CPRA)
 - Established a new agency (the **CPPA**) to promulgate new AI-related regulations
- Illinois AI Video Interview Act
 - **Notify applicants** on how the AI works, and **obtain consent**



AI Specific State Legislation & Guidance

- New York DFS Guidance and Discrimination Guidelines
 - NY Circular Letter No. 1 (2019): Insurers should **not use an algorithm or predictive model unless** they can establish that the underwriting or rating guideline is **not discriminatory**
 - Local Regulation: New York City Local Law 144
- Colorado 2021 S.B. 169: Restrict Insurers' Use Of External Consumer Data
 - Requires insurers to create **compliance programs** to ensure insurers' use of external data does not result in unfair discrimination.
- Connecticut Insurance Department Notice (April 2022)
 - Reminds insurance licensees of their obligation to use algorithms, models and big data in compliance with anti-discrimination laws and requires an annual certification
- California Department of Insurance Bulletin 2022-05
 - Reminds insurers of their obligation not to discriminate in connection with the use of AI and/or big data

Other Laws Implicated by Algorithmic Bias: Federal and State Anti-Discrimination Laws

Primary sources of law prohibiting discrimination in financial services

ECOA and Regulation B	Fair Housing Act	State Laws
<ul style="list-style-type: none">Prohibited basis characteristics:<ul style="list-style-type: none">RaceColorReligionNational originSex (incl. sexual orientation & gender identity)Marital statusAgeReceipt of public assistance income, andExercise of rights under the Consumer Credit Protection ActApplies to consumer and commercial lending	<ul style="list-style-type: none">Prohibited basis characteristics:<ul style="list-style-type: none">RaceColorReligionNational originSex (incl. sexual orientation & gender identity)Disability/handicapFamilial statusApplies to single-family and multi-family real estate transactionsThere does not need to be a credit transaction	<ul style="list-style-type: none">Some states have analogous anti-discrimination laws that prohibit discrimination in connection with housing, credit, insurance, or places of public accommodation.Some states provide for additional prohibited bases, such as military statusExample: NY Executive Law 296-a - Unlawful discriminatory practices in relation to creditExample: California's Unruh Civil Rights Act prohibits discrimination on the basis of sex, race, color, religion, ancestry, age, disability, military status, medical status, sexual orientation, genetic information, medical condition, citizenship, primary language and immigration status.

Other Laws Implicated by Algorithmic Bias: Federal and State UDAP/UDAAP Laws

- The Dodd-Frank Act and Section 5 of the FTC Act prohibit unfair and deceptive (and abusive) acts and practices (UDAP/UDAAPs) in connection with **consumer financial products or services** or **“in or affecting commerce.”**
- Most states have corollary UDAP laws.
- Unfairness is an act or practice that:
 - (1) causes or is likely to cause substantial injury to consumers,
 - (2) the injury is not reasonably avoidable by consumers, and
 - (3) the injury is not outweighed by countervailing benefits to consumers or to competition
- The CFPB and the FTC have taken the position that discrimination can constitute an “unfair” act or practice.

Coordination Among US Financial Sector Regulators



- **State of the Industry.** In March 2021, five agencies issued a request for information (RFI) on financial institutions' use of AI/ML.
 - **Explainability.** Addressing the lack of accessibility of underlying theory and logic of AI, including post-hoc methods of explainability.
 - **Bias.** Identifying existing controls for data quality assurance procedures.
 - **Overfitting.** Mitigating algorithms from learning from anomalous patterns in data.
 - **Dynamic updating.** Managing risks that arise from evolution: difficulties with validating, monitoring, tracking, and documenting AI approaches.
 - **Third-party oversight.** Developing safe processes for leveraging third-party tools and technologies.
 - **Fair lending.** Upholding legal and regulatory obligations to consumer protection, fairness, and transparency.
- **Replicable Approach.** The interagency RFI can be implemented internally to build a sustainable, protective AI governance framework.
- In October 2021, another joint RFI about the use of AI, hinting that future regulation in the sector is likely.

OCC Supervisory Expectations

- **Four areas of risk**

- Explainability
- Data Management
- Privacy and Security
- Third-Party Providers



- **Five supervisory expectations**

- Risk and Compliance Management Programs
- Model Risk Management
- Third-Party Risk Management
- New and Modified Products Principles
- Responsible Use of Alternative Data



How To Mitigate Against Bias in AI Applications - Challenges

- What are the primary challenges with AI approaches?
 - No “AI Lawyer” to identify and resolve risks
 - No silver bullet for AI governance
 - The lack of definite scope of “AI” inhibits effective and legally defensible governance structures
 - Different tools used for different purposes create a vast array of issues to consider and mitigate risks.

How To Mitigate Against Bias in AI Applications – Guiding Principles

- 1) Begin with a **clearly defined purpose**
- 2) Understand your **training data** and **identify limitations**
- 3) Gather a **diverse team** to work on the application

How To Mitigate Against Bias in AI Applications – Guiding Principles

- 4) Think about your **end users**
- 5) **Consider** and **debate** issues of bias
- 6) Document, document, **document**

How To Mitigate Against Bias in AI Applications – Guiding Principles

7) Create avenues for feedback and **use** the **feedback**

8) Increase **human involvement**

9) Build a set of recommended **best practices** and/or **ethical principles**



10:50a.m.-11:00a.m.

Break



11:00a.m.-11:55a.m.

Panel 3 – Navigating Litigation Challenges in Explainable AI

Speakers



Reginald Goeke
Partner
Mayer Brown

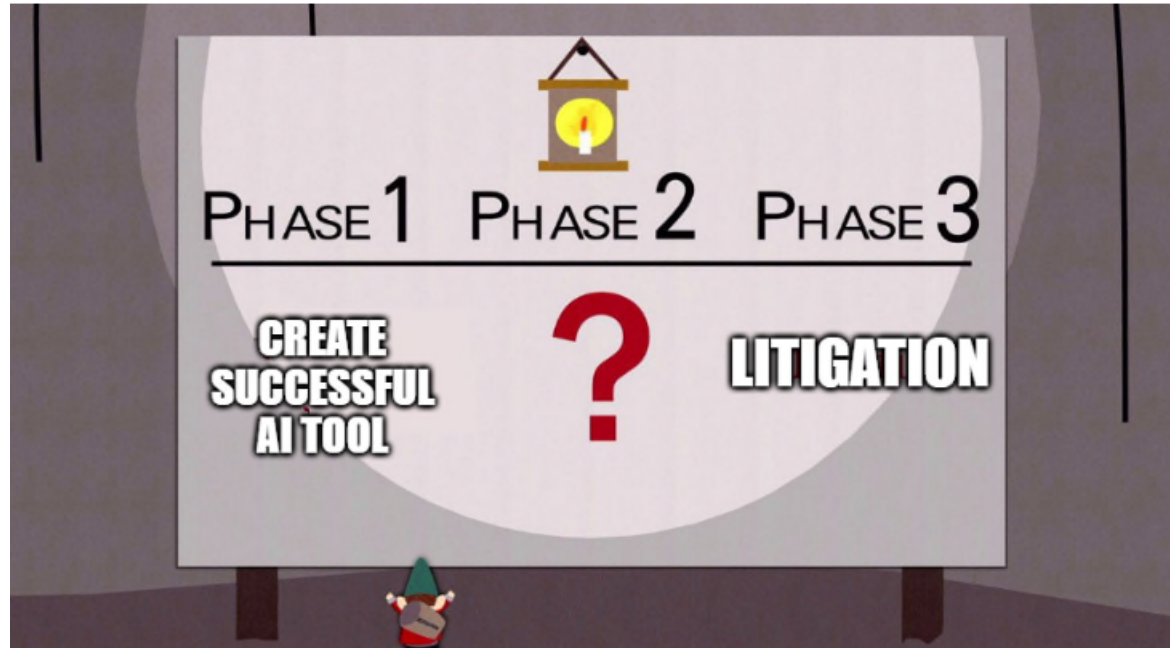


Alex Lakatos
Partner
Mayer Brown



Christopher Leach
Partner
Mayer Brown

Litigation, the Byproduct of Success



Today's Discussion

- **Risks:** Plaintiff's lawyers, media, and regulators
- **Challenges:** Special litigation risks posed by models
- **Possible Solutions for litigation:** Governance, Validation, Explainability

Risks: Litigation, Regulatory and Public Relations

Loan Mod Algorithms

- Errors in scoring loan modification eligibility led to decline of loan modification applications that should have been accepted
- Must demonstrate to regulators and enforcement that models well-controlled and reasons for not taking action sooner

Credit Algorithms

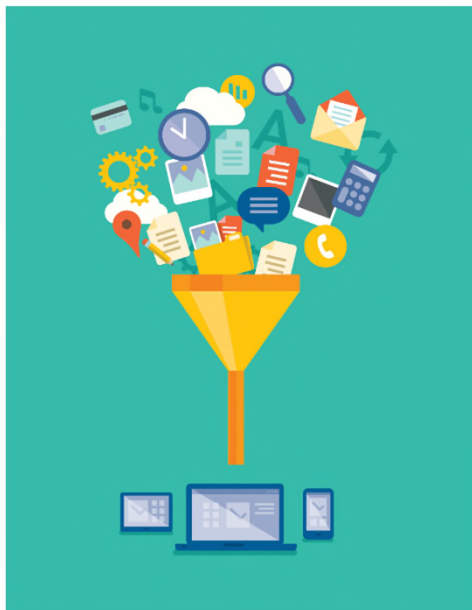
- AI-driven credit scoring leads to allegations of gender bias
- Must be able to demonstrate to public, regulators (and potentially litigants) that model decisions are not unlawfully discriminatory

Investment Algorithms

- Errors in quantitative investment models lead to investments made over many years arguably affected by model error
- Must decide on disclosure, self reporting, whether error policies apply, and then quantify impact

Challenges: Data

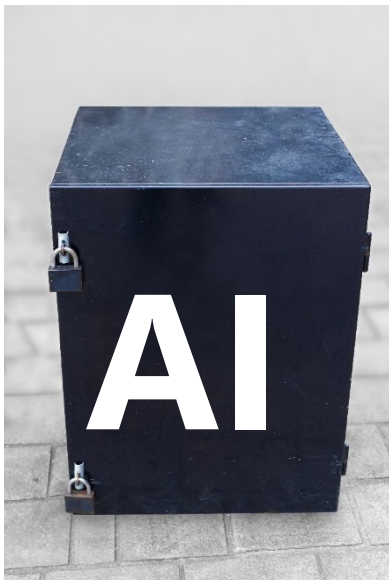
Complex Inputs



- Increasing volume of data
- Data is increasing personalized
- Data privacy
- Potential bias embedded in data
- Data evolution: can you recreate data from which model was developed? Data used as basis for decision?
- Data consistency: Does data from multiple sources used over time mean the same thing?
- Data retention: how much data to preserve, and what types?

Challenges: Describing how models work

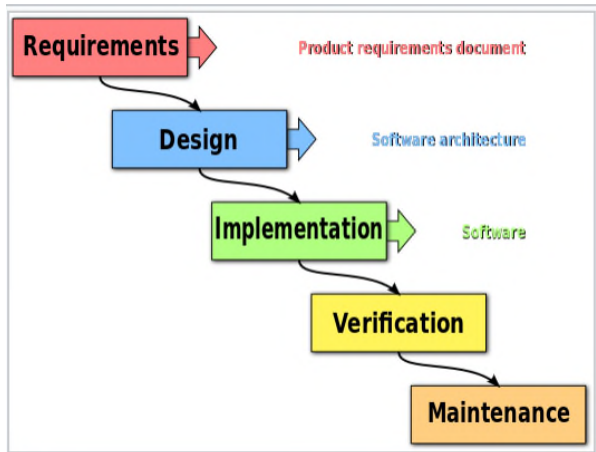
Complex Processing



- Potential for highly complex rules-based and expert system models, involving advanced math or computer concepts that are difficult to explain
- Cutting edge AI (e.g., deep neural networks) are least transparent. Surprising paths and approaches
- Model may be developed over time, and include many components and many authors over time, such that no one person knows all elements of model
- Individuals most knowledgeable about the model may no longer be available to explain it
- Model may be trade secret

Challenges: Changes over Time

Complex Development Over Time



- Customized for data sources, customers, marketing strategies, products, etc.
- Upgraded and amended model
- New, changed or different data sources
- Complex even for designers, in-house expert turnover
- System documentation vs. data scientist culture

Challenges: Explaining Decisions/Outputs

- Complex Outputs



- Outputs may be large and complex
- Outputs may not be user-friendly
- Outputs may be usable and comprehensible in-house, but hard to export and hard to use elsewhere
- Regulatory or business requirements may require explanation of decisions driven by models, which can be challenging

Challenges: Accusations of spoliation

Document Preservation and Spoliation



- The good
 - Rule 37(e) makes it hard to obtain spoliation sanctions.
- The bad
 - Plaintiffs' lawyers still seek to build record of knowing, unreasonable mishandling of relevant evidence.
- The ugly
 - State courts may have stricter rules.

Challenges: Accusations of spoliation

Document Preservation and Spoliation



- Sending unreasonable retention of evidence letters
- Using discovery to test feasibility of preservation
- Using “experts” to take unreasonable positions about what is feasible
- Arguing that preservation is easy
- Asking for inferences that failure to preserve was intentional

Challenges: Document demands

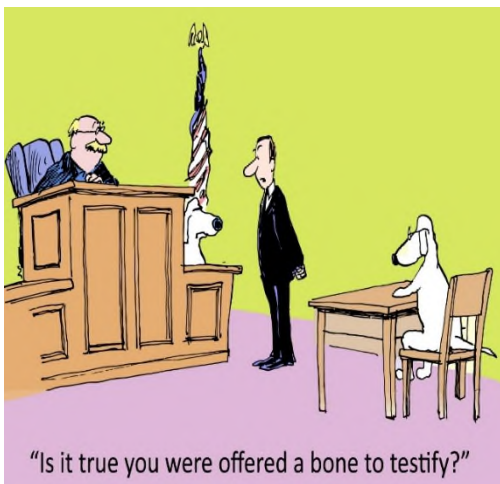
Document Production



- Unduly broad discovery demands and motions to compel.
- Seeking sensitive customer information
- Seeking trade secret model details
- Seeking information that third party vendors may not wish to share
- Challenging productions as inadequate
- Asking for direct, onsite access to models
- Seeking sanctions

Challenges: Rejection of evidence

Admissibility of Evidence: Must “authenticate” model and output. Are the computer, software, data and users reliable? How complex is the algorithm and problem?



- Discovery of all factors bearing on authentication
- Retaining experts to challenge authenticity
- Filing motions *in limine* to exclude evidence

Possible solutions: A bolt-on solution, after litigation commences, does not exist.



- Need to anticipate potential issues before litigation
 - Govern model
 - Explain model
 - Validate model

Possible solutions: Strong model governance

- **What is it?** Model governance is comprised of the policies, procedures and actions an organization takes to help ensure that models achieve their intended purpose.
 - “Regulators have put increasing pressure on financial institutions to make sure they adopt an enterprise framework for model governance.”
 - Foundation for litigation, regulatory, and public relations defense.
- Typically has layers, e.g., model users ensure model works as intended (level 1), supported by validators/testers (level 2), checked by audit (level 3), all guided by an internal management-led governance process.



Possible solutions: Strong model governance

- From a litigation defense perspective
 - Can help address model risks before disputes or issues arise, and thereby help to avoid disputes
 - Demonstrate to judge and jury that model was well-controlled and tested, and that any issues with model were not result of inadequate care
 - Ensure that models that may be subject to dispute are well-described and explainable
 - Helps to trace model changes to isolate relevant version of models and factors leading to any changes
 - Demonstrates that model has sound, defensible theory underpinning model insights

Possible solutions: Strong model governance

- **Oversight Structure**

- Establish key committees
- Reporting responsibilities
- Escalation process/expectations
- Set authorities by group

- **Requirements for Models**

- Model inventory, classification
- KPIs and KRIs for models
- Documentation required (including model descriptions)
- Performance monitoring
- Address third-party tools

- **Requirements for Data**

- Data inventory sources (incl. third-party)
- Documentation of data used
- Testing requirements for data used
- Data Privacy/Access restrictions

- **Model and Data Validation**

- Independence/capabilities of team
- Validation policy/Procedures
- Frequency of testing
- Testing standards
- Sensitivity testing
- Adherence to SR 11-7-like standards

Possible solution: Explain model

Elements of Model to Explain and Document

Purpose/ Design

- What is goal/task model is designed to achieve
- Theories (Actuarial principal/rationale underlying model)
- Describe basic function (steps performed) by model, and process map if helpful
- Key global variables driving model decisions
- People involved over time in development

Data

- Identify specific data sources used
- Where data obtained from and steps to ensure reliability of data
- Identify data used to develop model, and consistency with how model is operated
- Data variables, ranges, outliers, and correlations

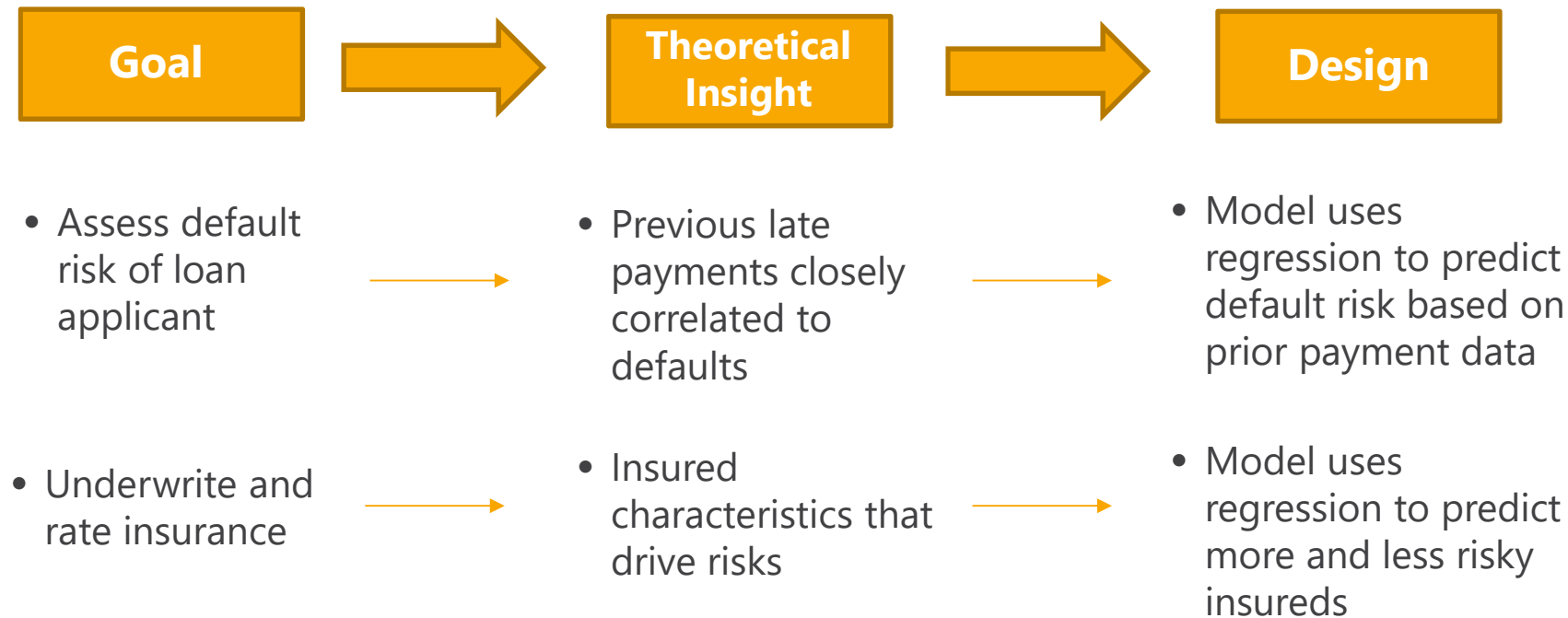
Testing

- Validation and testing team and their independence
- Describe tests performed and results of tests
- Identify data parameters for which model tested (e.g., sensitivity tests)
- Change control process and frequency of validation

Output

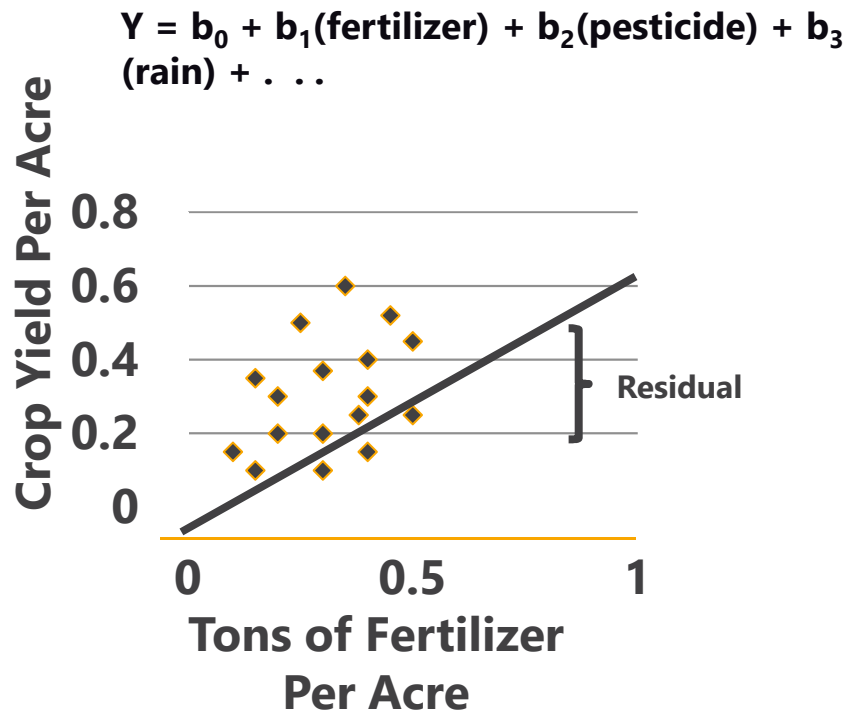
- Expected model output and interpretation of output
- Reason codes/Local variables of importance
- Role of humans in ultimate decisions

Possible solution: Explain model



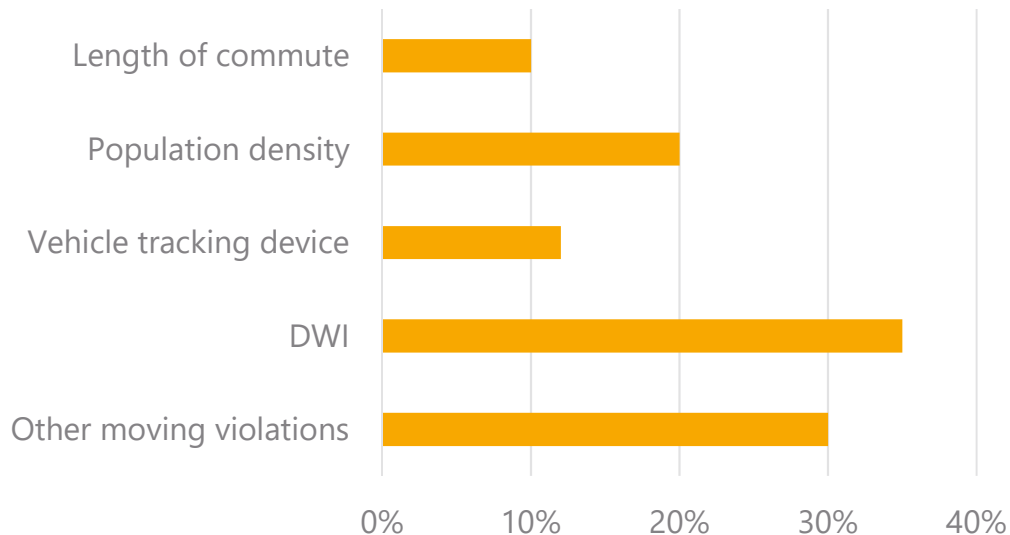
Possible solution: Explain model

- AI Models frequently use various statistical analyses to identify relationships between independent and dependent variables
 - Multiple Bayesian models
 - Regression
 - Decision trees
 - Discriminant analysis
- Key to describing the model is to describe (or present a picture) of the statistical methodology



Possible solution: Explain model

Global Variable Importance Chart



- Many AI tools now will generate data to explain the variables that tend to drive decisions across the model
- Some also create partial dependence charts, which provide the average prediction of the model for different input variables
- These are useful to assess reasonableness of model decisions and explain generally how model works

Possible solution: Explain model

Many Tools Used to Identify Import of Variables to a specific Decision

- **Shapley Value** (estimates import of each variable by changing/removing variable from equation)
- **Decision Tree** (Reflects decision path for particular decision, showing the key variables that guide the path)
- **LIME** (Local, Interpretable, Model Agnostic, Explanations) (uses data near the point estimate, and uses simpler model to estimate the key factors)
-

- Each method has its own benefits and drawbacks
- Will need to work with model developers to identify best tool
- But with those tools, the user can often generate reason codes for declination, limitation or rate differentials

Possible solution: Validate model

Independence

- Independence of model validators from developers?
- Reporting through Risk/compliance function?

Completeness

- Cover both in-house and third party tools
- Inventory of models, with risk assessment by model

Reporting

- Validation results reviewed within governance process
- Audit of validation team
- Key risks (legal, business, reputational) identified

Change Management

- Change logs should be maintained; Significance of changes identified
- Validation re-performed on significant modifications to model



11:55a.m.-1:25p.m.

Lunch and Presentation by Gabriel Morgan
Asaftei, Partner at McKinsey & Company

Perspectives on Artificial Intelligence Risk Management



Gabriel Morgan Asaftei
Partner
McKinsey & Company

Discussion topics for today



Artificial Intelligence and Machine Learning (AI/ML) Models and AI Risks in Financial Services

- What constitutes as an AI Model and AI Application?
- Why are AI Models and AI Applications different than existing models / applications?
- What are AI Models and AI Applications used for?
- Which governance mechanism should we apply?

The risks from AI/ML models are complex and require a redesign of the governance and oversight of model risk management and IT risks

Context

- **AI/ML** are **increasingly used across** the finance value chain and they have the **potential to amplify the risk** for financial institutions
- There is a **lack of common definitions** of what is considered AI/ML and what needs to be governed
- **Vendors often market directly to the business**, IT gets engaged late in the process
- **Traditional IT sourcing processes are not designed** to identify the **presence of AI / ML models** within business applications

Current framework

- Financial Institutions have **robust enterprise governance frameworks** that set and oversee standards across data, model, and technology:
 - » Model Risk Management
 - » Enterprise Architecture
 - » Data Governance & Management
- One of the **key challenges** has been to define **who drives and coordinates the discussion of a framework** that can respond to requirements from different stakeholders

Key strategic questions

- Given the **challenges of AI/ML** financial institutions need to answer the **following questions**:
- How can the bank oversee and mitigate the risks from AI/ML without creating a new roadblock for innovation?
 - How can the AI/ML risks materialize? How can the bank identify those risks early on and mitigate them?
 - How can these risks be measured and monitored across the AI development lifecycle?
 - How should the oversight function be structured? Who should be the owner of AI risks governance?

AI/ML models are now common at financial institutions, with wide adoption across the value chain...

Domains

Revenue Acceleration

- **Retention (Churn Modelling):** Save customers at risk of significantly shifting share of wallet, churning and switching
- **Next best action:** Advanced segmentation leads to effective next-best-action campaigns
- **Multi-channel customer journey:** Help identify opportunities for digital acquisition
- **Marketing and Targeting:** Expand customer base
- **1-2-1 pricing:** Identify optimal price for every single client/transaction, based on sensitivity

Risk Reduction

- **Underwriting:** Make better underwriting decisions To reduce risk by using deep-learning algorithms
- **Line optimization:** Reduce charge-off losses by offering an optimal line to each client
- **Collections:** Increase recoveries by making the right offer, at the right time, through the right channel
- **Payments fraud:** Identify and review high risk payments before they are executed
- **Anti-money Laundering:** Quickly suspend money laundering operations using a longitudinal view of payments pathway
- **Conduct risk:** Leverage NLP to identify emerging risks using customer complaints

Smart Operations

- **Contract compliance:** Automatically capture and validate data contained within written contracts
- **Data quality assurance:** Automatically flag data quality issues that affect decision-making
- **People analytics/sales force effectiveness:** Enhance workforce productivity and employee retention
- **Branch operations optimization:** Improve customer experience and decrease costs
- **Complaints redesign:** Monitor customer complaints to improve customer experience and decrease costs
- **Call volume analytics:** Identify key drivers to reduce call volumes in call centers

Customer Excellence

- **Customer service:** Analytics to improve CSAT with NLP
- **Call routing:** Intelligent routing in contact center to reduce wait times and improve satisfaction
- **Front line dashboards:** Actionable front-line digital dashboards to drive call interactions

... but AI/ML models can lead to unintended results that cause bad public and regulatory reaction

Artificial Intelligence and Machine Learning models led to bad reputational and customer outcomes...

Credit card issuer	“'sexist' credit card” : Credit approval process seems to be gender biased, providing significant lower limits to women
Delivery service	Delivery company excluded minority neighborhoods while extending it to mostly white neighborhoods
Social app	“Racist face-aging app” : viral app whitened the skin colour when aging African descendent people ³
Chat bot	Chatbot turned from a teenage girl into a “feminist-bashing troll”



... even from unintended causes

Observable issues:

1. Unintended biases creep into models
2. Overfitting models that do not perform outside of training set
3. Using training data that is not representative of the population to be predicted on
4. Model is not sufficiently tested in extreme situations – lack of fail-safes
5. Unstable learning systems can be manipulated by exposing them to manufactured training data

Regulators, such as the OCC in the US, are requesting information about their supervisory approach and requirements towards these complex models

Assessing the risk from AI/ML models is complex and require assessing multiple dimensions



Context of use and autonomy

Assessment of context and objective of the AI solution (e.g., prediction, recommendation, decision) and level of autonomy (e.g., full automation, "human in the loop")



Impact to stakeholder

Assessment of impact including type of adverse impact for the stakeholder (e.g., credit denial vs. bad product advice), size of the potentially affected population, adverse impact for the bank (e.g., reputational and regulatory fines/litigation)



Regulatory Requirements

Assessment of regulatory requirements for use case in question (e.g., US consumer credit related purposes, whereby the requirements of the US Fair Housing Act and Equal Credit Opportunity Act must be met)



Algorithmic complexity

Assessment of complexity and explainability of the AI solution (e.g., simple logistic regression with few parameters vs. "black-box" deep learning algorithm which requires techniques such as LIME / SHAP)



Data used

Assessment of the data used in the model considering the type of data used (e.g., personal data protected under GDPR) and its source (e.g., bank proprietary vs. third party)

Regulators in financial services have issued limited formal guidance thus far, but are increasingly paying attention to this topic

Federal Reserve Board (FRB) scrutiny of AI-ML models under existing guidelines

- In a recent public statement,¹ FRB Governor Brainard explicitly indicated that existing model risk guidelines extend to AI-ML models:
 - SR Letter 11-7: governs model risk management for all bank models, “which include complex algorithms like AI”
 - SR 13-19/CA 13-21 guidance on vendor risk management equally applies to “AI-based tools or services that are externally sourced”

New York Department of Financial Services (NY-DFS) Circular Letter No. 1 for insurance underwriting

- Highlights statutory obligations regarding use of external consumer information (including modeled output) in life insurance underwriting, focusing on:
 - Potential negative impact on life insurance decisioning that could result from using algorithms and predictive models
 - Lack of transparency for consumers stemming from use of algorithms and predictive models

Proposed Bill - U.S. Senate Algorithmic Accountability Act of 2019 (for companies making >\$50M a year)

- Designed to address biases in model assumptions or data that can result in discrimination or increased privacy risk
- Directs the Federal Trade Commission to require entities that use personal information to routinely conduct automated system and data impact assessments

Expected increase in European Commission (EC) supervision over the use of AI-ML models

- In an April 2018 directive (“Communication on Artificial Intelligence”),² the EC set out plans for increased scrutiny of AI-ML, including:
 - formation of working groups to consider whether existing regulations are fit for purpose
 - Planned report on “the broader implications for, potential gaps in and orientations for the liability and safety frameworks for AI”
 - pledge to draft AI ethics guidelines for the protection of “privacy, dignity, consumer, protection and non-discrimination”

Monetary Authority of Singapore’s (MAS) F.E.A.T. Principles

- MAS released a new set of principles designed to foster greater confidence and trust in the use of AI and data analytics, by ensuring that data and models are accurate and minimize unintentional bias

- **Attention from regulators to handling/mitigation of AI-ML risk is increasing** - at the same time, there isn't a yet a fully formed regulatory framework for AI
- In most cases, **regulators or supervisory authorities are at the level of design principles** and this has not yet transformed into detailed requirements or rules
- Regulators are in general, evolving their thinking and in instances, **engaging the industry to ascertain what the guidelines may look like**

¹ <https://www.federalreserve.gov/newsevents/speech/brainard20181113a.htm>

² https://ec.europa.eu/knowledge4policy/publication/communication-artificial-intelligence-europe_en

Banks are getting organized around governance and oversight of AI/ML risk: approaches and roles vary

Top US Bank

- **Head of Operational Risk** mandated by the CRO to develop “overarching framework for AI/ML governance”, given MRM perspective on the issue deemed too technical / not broad enough
- Multidisciplinary group convened to **develop AI risk roadmap**, i.e.:
 - Ethical AI principles
 - AI risk taxonomy
 - Risk assessment and tiering of use cases
 - End-to-end control environment (including validation)
 - Capabilities required in control roles (both first and second line), i.e.: knowledge of AI/ML methodologies and controls, like bias testing, to effectively act as a “translator”
 - Tooling and platforms for AI risk management

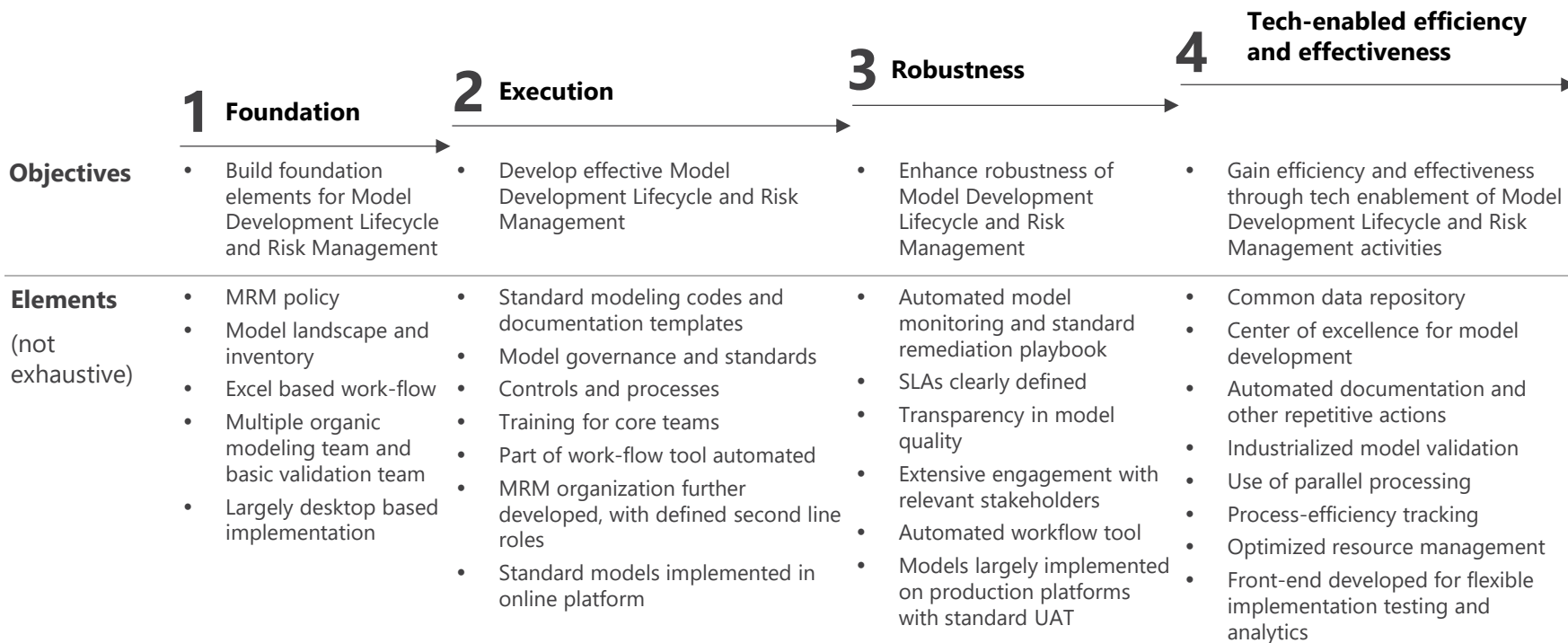
Top Canadian Bank

- **Multiple stakeholders developing framework** and requirements for AI in parallel (e.g., MRM, Compliance/Legal, Audit, Analytics CoE), including likely Canadian adoption of stronger regulatory rules from Europe and US
- **Expanding scope of MRM to address reputational and compliance risks:** e.g. marketing models, but lack of clarity on coordination in the second line and development of a unifying enterprise view
- Development under way for :
 - Structure of AI risk assessments for Compliance and Model risks
 - Aggregation of risks at the model level + assessment of the data science environment to define level of AI risk
 - “Compliance by design” approach to model control environment
 - New training paths to prepare control functions for AI

Top UK Bank

- **Chief Digital officer and Board** sponsored a process to update risk management frameworks and governance for AI, as well as the supporting capabilities required to operationalize it (critical pre-requisite for their **digital transformation**, which includes pervasive use of AI)
- Multidisciplinary group worked to:
 - Enhance risk governance to support broad use of AI including changes to the Risk Taxonomy, Risk Tiering and Risk appetite
 - Expand scope of MRM to address new categories of models (marketing) and address a greater rate of change.
 - Piloting new frameworks with current AI models in pipeline
 - Development of AI Risk KRIs

Banks' AI risk governance including model risk management and IT risk implementation is evolving across four stages



Most NA banks' level of maturity is at Stage 2-3

A comprehensive framework for AI/ML risk management and oversight can help to evaluate enhancements needed for target state

Not exhaustive

AI needs and business value	Business use case	<ul style="list-style-type: none">Complete set of AI capabilities aligned with BU vision and strategyAssessment of business function/ domain, value at stake (e.g., financial impact), customer exposure, beneficiaries and dependencies	Use case roadmap	<ul style="list-style-type: none">Prioritization of AI capabilities balancing feasibility, quick-win, long-term impact, and detailed roll-out plan of AI capabilities at the enterprise levelRoadmap with use case execution or high priority use cases		
Technology	Data	<ul style="list-style-type: none">Data architectureData quality principles and data management programs/policies	Infrastructure and platforms	<ul style="list-style-type: none">Supporting data and modeling capability infrastructure and platformsArchitecture integration guidelines		
	AI modeling capabilities	<ul style="list-style-type: none">Inventory of AI capabilities, AI modeling enablers (built or sourced)Sandboxes for data science development	Development and delivery	<ul style="list-style-type: none">Operating model for developing, delivering and maintaining use cases/applications over the algorithm/model lifecycle (e.g., Analytics Ops, DevOps, DataOps)		
AI Risk Management	Foundational elements	Definitions	<ul style="list-style-type: none">Definition of AI and AI capabilitiesDefinition of Statistical model, AI model, and model for MRM purposes	Risk oversight framework	Categories of AI Risks	<ul style="list-style-type: none">Classification of AI risks emerging through the use of algorithms/models (e.g., discrimination,)
		Taxonomy of AI	<ul style="list-style-type: none">Classification of AI methods/techniques from a use case/application perspective		Assessment of AI Risk	<ul style="list-style-type: none">Dimensions to assess risk from AI and quantification (e.g., AI risk index)
	Operating model	Process	<ul style="list-style-type: none">End-to-end AI Risk Review process		Guardrails and risk appetite	<ul style="list-style-type: none">Principles/policies around limited or off-limits methods/techniques, algorithms/ models, and use cases (e.g., using deep learning for employee selection)
		Organizational model	<ul style="list-style-type: none">Roles, responsibilities/ accountabilities, and reporting structures needed to oversee the development, delivery, and use of AI		Controls over the lifecycle	<ul style="list-style-type: none">Processes and policies defined at each stage of the algorithm/model development lifecycle to ensure appropriate risk controls & oversight to mitigate AI risk (e.g., bias)
		Governance framework	<ul style="list-style-type: none">Set of decisions related to the oversight of the development, delivery, and use of AIDecisioning bodies (e.g., roles, committees)	Cap-abilities	Talent	<ul style="list-style-type: none">Talent need and skill matrixTalent development and sourcing strategy
			Tools		<ul style="list-style-type: none">Risk management tools	

What is a model and what is a tool?

Details follow

ILLUSTRATIVE

AI Risk Review process step

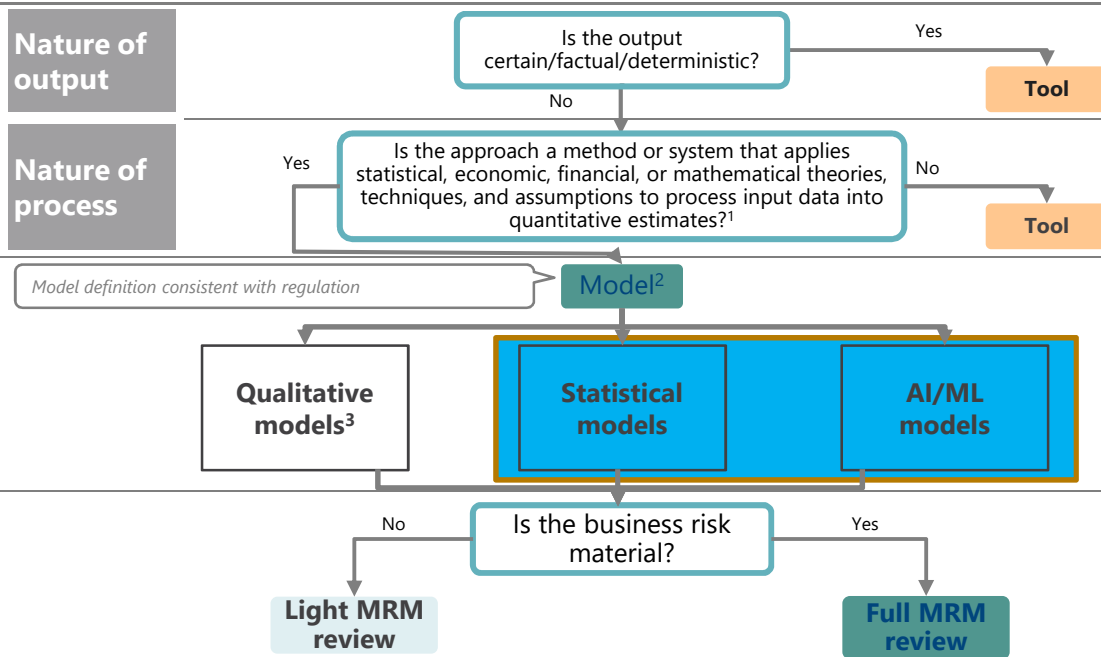
Evaluate model definition

Dimension

Nature of output

Nature of process

Decision tree for evaluating algorithms for MRM purposes



Model for MRM Review?²

Evaluate business use case risk

Examples

- Automation tools
- Applications Processing Data (e.g., ETL tools)
- Applications used solely to organize, or format data would typically not be classified as models e.g., business intelligence reporting such as Tableau

¹ Board of the Federal Reserve System, "Supervisory Guidance On Model Risk Management", SR 11-7, April 4, 2011. Document adopted by FHFA, AB 2013-07, November 20, 2013

² Other inputs may be needed to decide whether a model should go through MRM review e.g., evaluation of data integrity, restrictions, biases and misuse, evaluation of model impact on IT security, integration, integrity

³ Analytical/Statistical model approach with inputs which are wholly qualitative or based on expert judgement

To our knowledge, there is no specific definition of AI models from U.S. regulators. Industry leaders use model definitions in SR11-7/ AB 2013-07 and define AI models by exclusion

Definition of a model¹

- **“Model** refers to a **quantitative method, system, or approach** that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to **process input data into quantitative estimates**”
- A model consists of three components:
 - » **Information input**
 - » **Processing**
 - » **Output / Reporting**

		Typical technical features in a...	
		...traditional Statistical model	...AI/ML model
Model overview		<ul style="list-style-type: none"> ▪ Relies on defined rules or pre-defined equations/ logic with uncertainty (error component) but without autonomy or learning 	<ul style="list-style-type: none"> ▪ Contains a high degree of autonomy and feedback components, with ability to handle multiple types of data
Model component	Information input	<ul style="list-style-type: none"> ▪ Can ingest only structured data ▪ Can handle small or mid-sized data 	<ul style="list-style-type: none"> ▪ Can ingest structured, unstructured data or a combination of them ▪ Typically requires vast amounts of heterogeneous data
	Processing	<ul style="list-style-type: none"> ▪ High degree of explainability and a low degree of autonomy ▪ Relationships between variables are driven by formalized mathematic equations ▪ Trained models do not change functional form on their own during model lifecycle 	<ul style="list-style-type: none"> ▪ Low degree of explainability and a high degree of autonomy, often leading to reduced transparency and higher risk profile ▪ Learns from new data patterns and can change the applied functional form/hyper-parameters without modeler’s direct involvement
	Output / Reporting	<ul style="list-style-type: none"> ▪ Model output is specific to the types of model and assumptions used 	<ul style="list-style-type: none"> ▪ Model output can change based on interactions with users without being specifically pre-programmed for that scenario (feedback loop)
Not all features described above are present in every AI model			

¹ Board of the Federal Reserve System, “Supervisory Guidance On Model Risk Management”, SR 11-7, April 4, 2011. Document adopted by FHFA, AB 2013-07, November 20, 2013

Example of using AI/Natural Language Processing models in a chatbot and risks that may arise

EXAMPLE

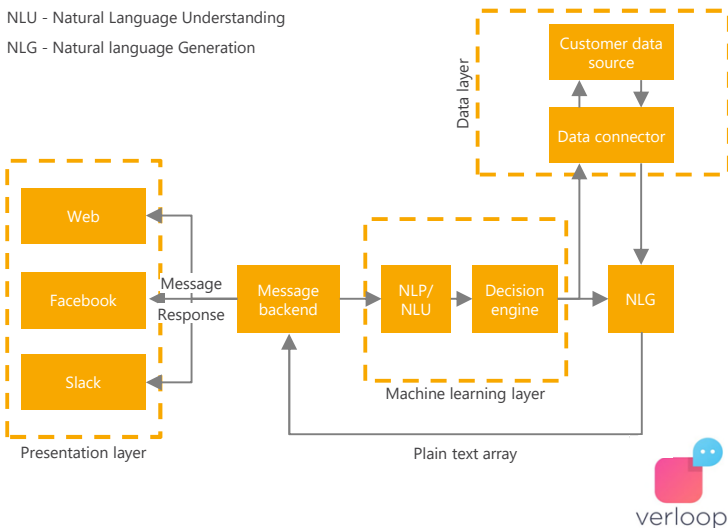
Chatbot functionality overview

Illustrative architecture diagram for a chatbot

NLP - Natural Language Processing

NLU - Natural Language Understanding

NLG - Natural language Generation



Model component

Risk evaluation can focus on

Input (data layer)

- **Syntax of the input** (e.g., ability to identify nouns, adjectives, verbs, etc.)
- **Realistic** (i.e., reflect what a customer might ask) – i.e., conversational reality
- Help the model learn to **distinguish actionable tasks** vs. **vague requests** (or bad English)

Processing (machine learning layer)

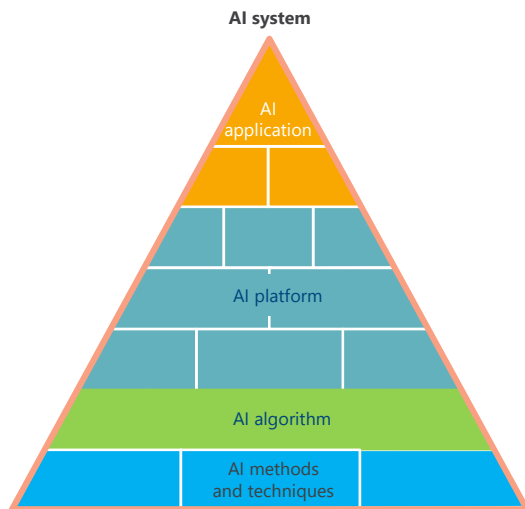
- **Accuracy and number of steps** needed to maintaining accuracy of responses
- **Performance of production model** vs. **challenger models** for individual components
- **Feedback mechanism** used to **maintain/improve performance** over time
- **Does not develop negative “biases”** when **input is outside of the trained dataset**

Reporting (presentation layer)

- Measure **information retrieval metrics** to measure accuracy of output
- **Multiclass classification** performance metrics
- **Risk assessment** of potential errors / unintended actions taken by the model (e.g., accessing wrong account information)
- **User satisfaction metrics:** task completion, user satisfaction, etc.

AI/ML is embedded throughout the enterprise tech stack

Hierarchy of AI capabilities



Description

AI system

Technology combining various internally developed or third-party Artificial Intelligence Software/Applications into a complex and integrated technology stack that interact directly with internal or external stakeholders and can make **unsupervised or semi-supervised decisions**.

AI application/ software/ hardware

Applications/Software/Hardware combining various **Artificial Intelligence Algorithms** that enable a non-human machine to solve a problem by analyzing its environment and taking actions that maximize its chance of success without being explicitly programmed by human intervention.

AI platform

Third party software or internally developed sandbox that **provides and facilitates the development and execution of AI algorithms** and can help automating the end-to-end process for building, deploying, and maintaining AI models at scale.



















AI algorithm

Algorithms are combinations of one or more AI methods and techniques to learn and act like humans do and improve their learning over time in autonomous fashion (i.e., without being explicitly programmed) by ingesting and processing data and information in the form of observation and real-world interactions.

AI methods and techniques

AI methods and techniques leverage mathematical formulae and computer programming techniques to **perform tasks that normally require human intelligence such as estimating correlations between variables, visual perception, speech recognition, translation between languages, and learn new patterns from data unseen previously**.

Who is responsible for overseeing AI/ML-embedded in third party tech platforms?

Types of AI Platforms		Example players	Description
Internal DIY	AI as a service	 	<ul style="list-style-type: none"> AI solution components offered as a service over cloud infrastructure (e.g. MSFT Cognitive Services)
	Vertical applications	    	<ul style="list-style-type: none"> Packaged solutions for specific use cases targeted at business owners & including core logic, UI elements, & APIs
	Commercial platforms + consulting services	 	<ul style="list-style-type: none"> Consulting services to develop bespoke AI solutions for specific vertical/use case contexts
	Commercial AI Enabling Platforms	  	<ul style="list-style-type: none"> Proprietary tools & environments for internal data science teams or system engineers to develop specific solutions
	Open source tools	  	<ul style="list-style-type: none"> Community developed libraries/ frameworks or solutions offered free, some with optional services (e.g., H2O.ai)
	On-prem hardware/ Cloud infrastructure	  	<ul style="list-style-type: none"> Purposefully built hardware for deep learning (e.g., GPUs, FPGAs, NVIDIA DGX-1 Deep Learning Server) Infrastructure platforms (e.g., AWS, MS Azure) providing GPUs, etc

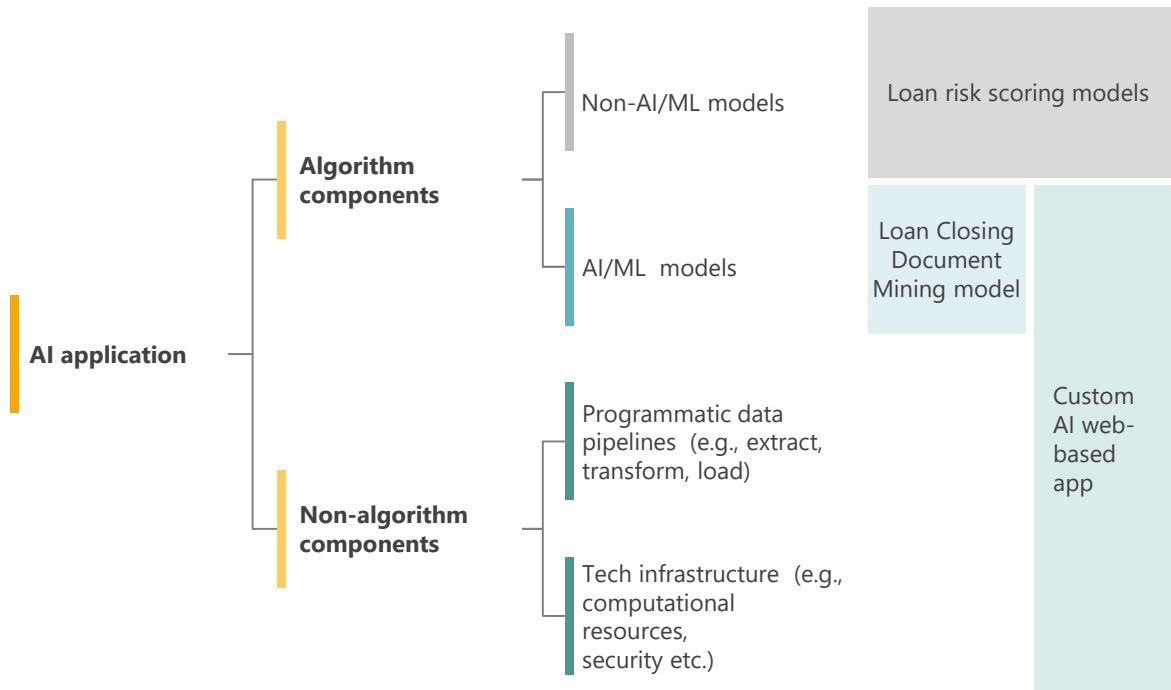
What needs to change in the existing governance to accommodate AI? – Model Risk Management (1/3)

Core process steps

- Model Risk management (MRM) is primarily responsible for **algorithms and for non-algorithm components** (e.g., data pipelines and technology infrastructure)
 - » For the algorithm components – MRM can determine the AI risks using AI taxonomy
 - » For non-algorithm components – MRM should engage IT Risk Review to determine risk associated with data and technology infrastructure
- There needs to be in place **processes and controls for handling components sent and received from IT Risk Review**

Examples

Categories



What needs to change in the existing governance to accommodate AI? – MRM (2/3)

MRM policy and governance	Model requirements	<ul style="list-style-type: none">▪ Validation activities for AI-ML models should thoroughly evaluate the technical environment in which the models are developed, and operated (e.g., platform, computational resources, data, security etc.)
	Development data set	<ul style="list-style-type: none">▪ Development data set created by partitioning should be free from any biases that may introduce discrimination in model outputs▪ Model validation activities for ML models should evaluate the data for partitioning in order to avoid biases
	Treatments & assumptions	<ul style="list-style-type: none">▪ Transformation techniques used in ML models to scale the data should be carefully evaluated to ensure they are appropriately applied to all the used data sets (training, validation, testing)
	Feature engineering	<ul style="list-style-type: none">▪ ML model validation activities should carefully evaluate the feature engineering process e.g., use of features as a data processing step only or as a core model component
	Modelling techniques	<ul style="list-style-type: none">▪ Parameter tuning / optimization is critical for ML models and therefore should be carefully assessed for its appropriateness and conceptual soundness
	Hyperparameters	<ul style="list-style-type: none">▪ In addition to the routine validation activities, ML validation activities require detailed assessment of the hyperparameters used (e.g., learning rate, number of trees etc.). Hyperparameter tuning / optimization is critical for ML models and therefore should be carefully assessed for its appropriateness and conceptual soundness
	Interpretability	<ul style="list-style-type: none">▪ Model validation for AI/ML should ensure that modelling techniques used are transparent and interpretable and not treated as “black box” while generating insights e.g., interaction effects between parameters should be clearly identified and assessed for unintended behavior.
	Bias	<ul style="list-style-type: none">▪ Given the nature of AI/ML models (uses of data and high complexity), model validation activities should carefully assess model outcomes for any form of bias introduced (e.g., through Lime or Shap) – e.g., bias can stem from training the learning algorithm on a sub-set of the data that is not fully representative of the dataset.

What needs to change in the existing governance to accommodate AI? – MRM (3/3)

MRM policy and governance	Production environment	<ul style="list-style-type: none"> ML validation activities should carefully evaluate the adequacy of the production environment in which the ML models operate Model validation activities for ML models should assess the scalability of these models as there is significant model risk in cases where the implementation scale is broader compared to the training set
	Tiering	<ul style="list-style-type: none"> Update based on model materiality, reputational risk, degree of customer facing, proximity to the decision activity
	Risk Appetite	<ul style="list-style-type: none"> Specify areas where not to deploy AI/ML models based on business risk and autonomy, restricted business usage based on explainability, and guidelines for gains from model complexity vs cost
	Roles and Responsibilities	<ul style="list-style-type: none"> Define accountability and responsibility of the key parties/stakeholders in relation to ML models (e.g., ML model developers, ML model outcome owners, and ML model oversight roles)
	Lifecycle Controls	<ul style="list-style-type: none"> Establish controls to ensure, e.g., <ul style="list-style-type: none"> » Data being sourced effectively & used in compliance with the group's regulatory requirements » Models being producing fair, safe and privacy compliant outcomes, with usable and reliable core performance of models » Ongoing monitoring activities of models in production and the recognition and action on changes of models in production » Regulatory compliance requirements and applicable risk profile across model lifecycle
Model validation function	Model review	<ul style="list-style-type: none"> Expand model review framework and process to address amplified risks from machine learning (e.g., explainability, bias, feature engineering, hyperparameter selection, production readiness, and dynamic model calibration)
	Capabilities, tools and infrastructure	<ul style="list-style-type: none"> Enhanced internal capabilities through recruitment (e.g., data engineers, data scientists and translators) and targeted upskilling/training Ensure access to systems, data and tools (e.g., cloud environment) used by developers

What needs to change in the existing governance to accommodate AI? – IT Risk Management (1/2)

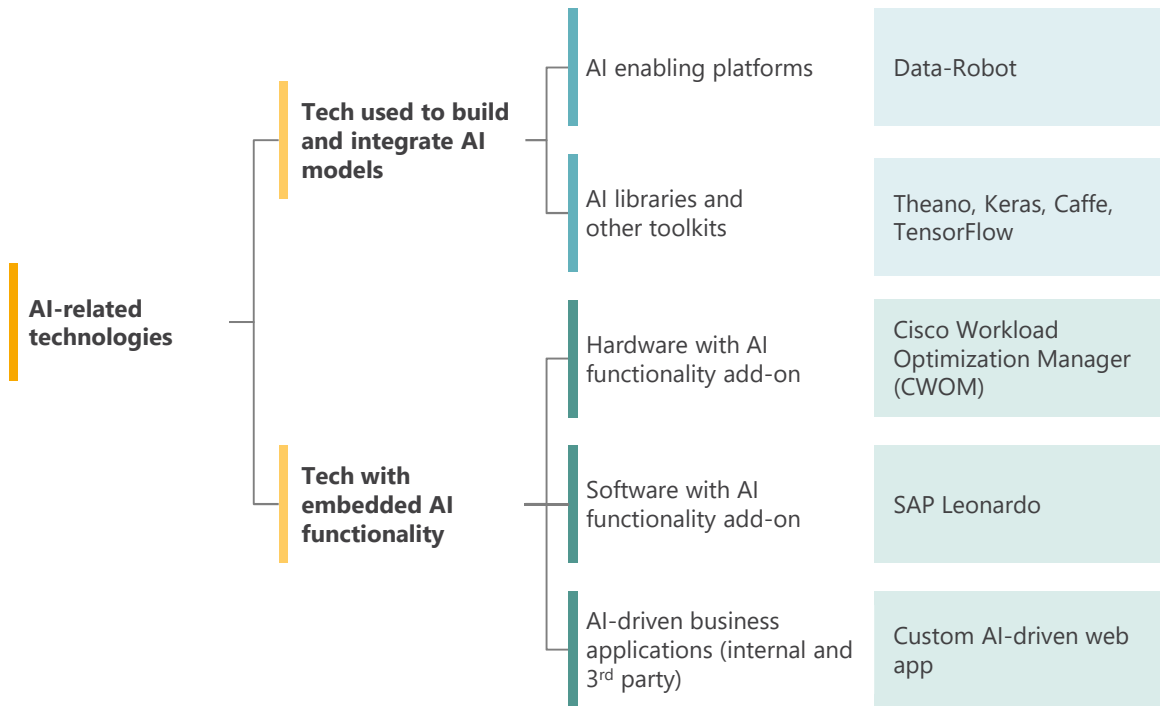
Core process steps

- IT Risk is responsible for reviewing **non-AI technology** (e.g., core tech) and **AI-related technology**
 - IT Risk is responsible for technologies used to build and integrate AI models
 - IT Risk is primarily responsible for technology with embedded AI functionality but engages MRM to review if the AI functionality qualifies as AI models
- There needs to be in place **processes and controls for handling components sent and received from MRM**

Examples

Categories

AI Applications

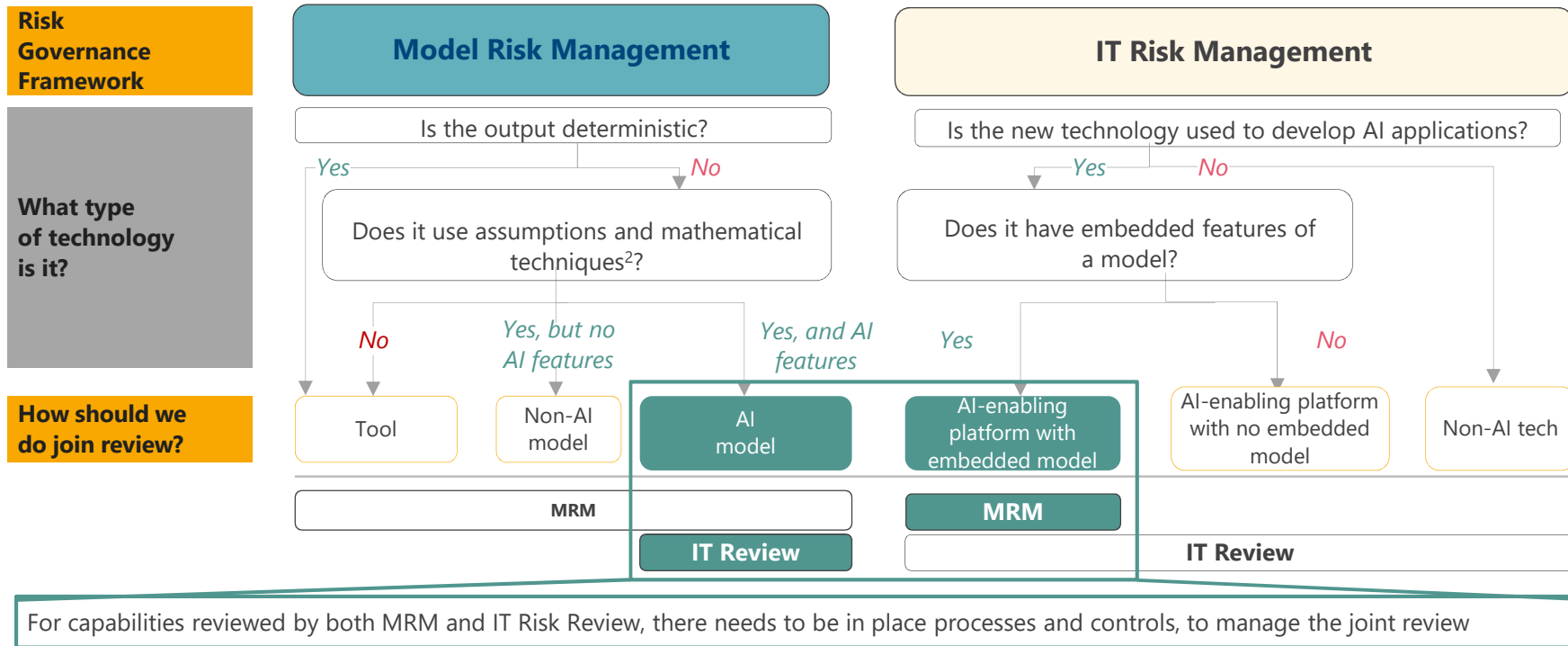


What needs to change in the existing governance to accommodate AI? – IT Risk Management (2/2)

IT policy and governance	Vendor frameworks	<ul style="list-style-type: none"> Ask vendors to explicitly identify presence of AI models in RFP/RFPs, and flag AI models to CIO / IT team Insert question(s) asking about presence of AI models in 3rd party risk assessment questionnaire Create standard template language covering AI, e.g., requiring vendor to disclose AI, provide documentation for validation, agree to specific clauses to protect the bank's interest & provide warranties, etc.
	Shared AI platforms across the bank	<ul style="list-style-type: none"> Maintain multiple AI technology platforms to cater to different needs across AI modeling teams Central management of tools available within platforms by enterprise AI tech team as part of reference catalog Enterprise AI tech team sets standards / guidelines to determine compute capacity allocation across applications
	Built-for-purpose AI platforms	<ul style="list-style-type: none"> AI modeling teams would be able to establish their own AI technology sandbox by provisioning their own infrastructure, with enterprise AI tech approval (on as-needed basis) Tools available will be a combination of AI modeling team-specific tools and common AI tools taken from reference image / catalog of tools managed by enterprise AI tech team Team specific tools can be requested by their IT lead; new tools must be reviewed by the enterprise AI tech team before adding to the catalog
	Languages & libraries	<ul style="list-style-type: none"> Enterprise AI tech team defines set of standard libraries as part of reference image / catalog of tools AI Tech team is responsible for evaluating of the risk of new version releases
	Collaboration & access tools	<ul style="list-style-type: none"> Enterprise AI tech team maintains standard set of approved tools that teams can download from the catalog of tools Tools should be standardized across shared AI platforms Enterprise AI tech team defines which of the standard tools are available in each shared AI platform
Embedded AI Model Governance	Identify potential models	<ul style="list-style-type: none"> When possible, leverage skilled experts from MRM Train IT tech team about how to identify presence of AI models in new technologies/new releases Update the IT governance process (where needed), including checkpoints from sourcing, risk, and legal perspective)
	Integrated review and monitoring	<ul style="list-style-type: none"> Recruit specialized expertise for scaling AI Models and AI Applications (e.g., Scala experts, Cloud computing engineers) and run targeted upskilling/training Enable safe access to new and innovative systems, data. and tools used to develop new AI applications

What parts of the data & tech organizations are responsible for AI Risk management?

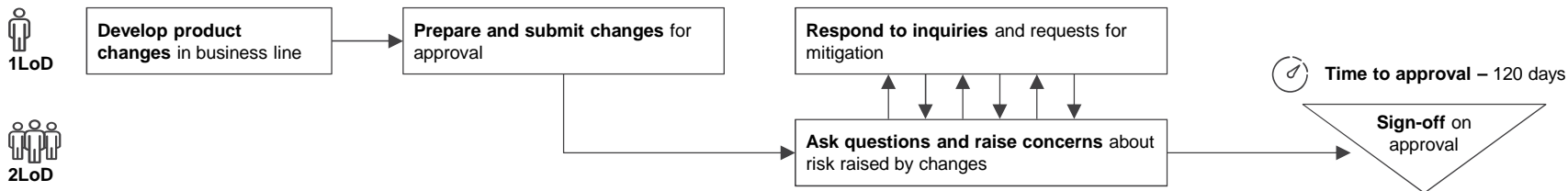
ILLUSTRATIVE; NOT EXHAUSTIVE



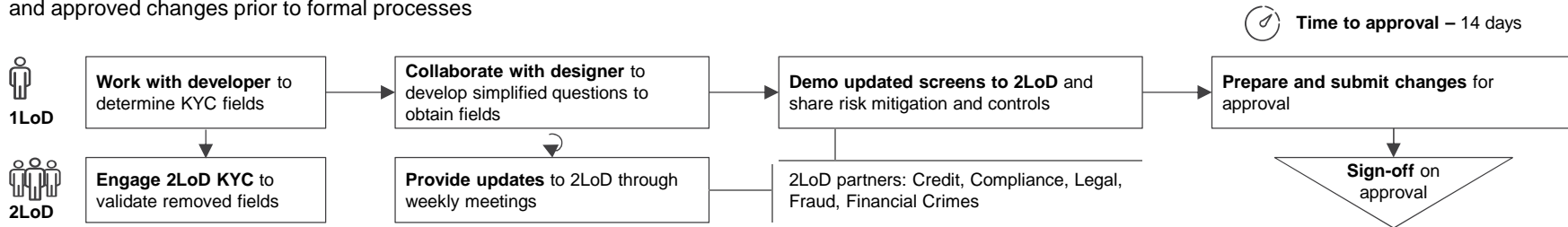
1 - "Does it have a processing component that applies mathematical techniques and assumptions to process input data into quantitative estimates?" FHFA, AB 2013-07, November 20, 2013

How could the AI Risk governance work for building an AI-embedded technology?

Silo approach: Changes to product developed in silo without engagement of 2LoD, leading to prolonged approval process



Coordinated approach: Early engagement and pre-socialization by risk SME accelerates approval process for streamlined loan application, as 2LoD have seen and approved changes prior to formal processes

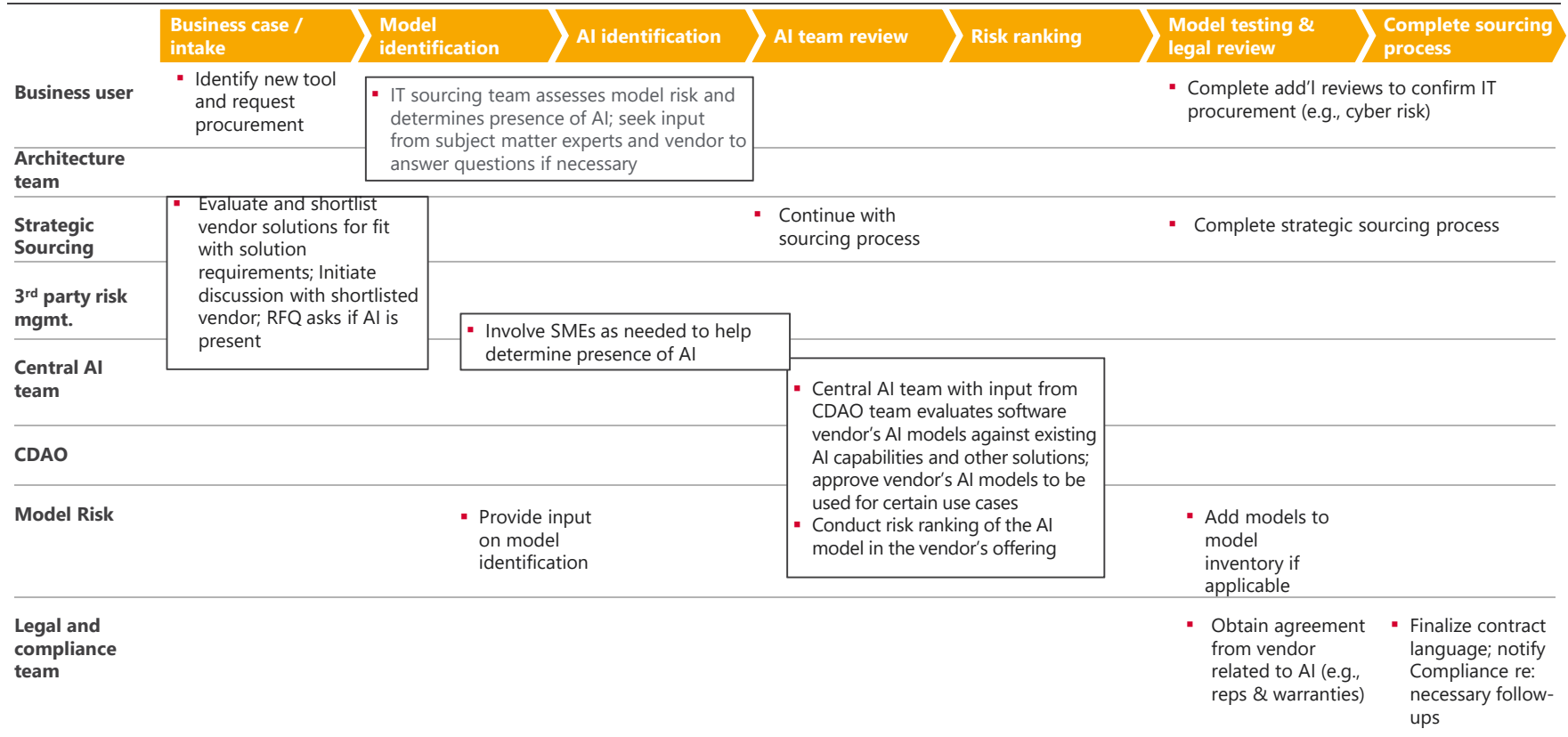


Single point of contact provided by 1LoD Risk SME coordinates **collaboration** with all risk functions

Regular touchpoints between 1LoD and 2LoD enable **transparency**

Accelerated approval process through **early engagement of 2LoD**

How could the AI Risk governance work for procuring 3rd party AI-embedded technology?



We see three broad governing archetypes for AI tech platforms across the industry

		Fully decentralized	Partially centralized	Largely centralized
Platform design		Low level of control / easy to experiment with new tools	Limited control on each environment; high level of flexibility to work with instance	Each zone is fully controlled by central team which alone has the flexibility to add newer tools
	Standards	Common standards and guidelines may be defined; Adoption is not mandatory	Common standards and guidelines defined; Adoption is not mandatory	Common standards and guidelines defined; adopted in all environments
	Level of platform consolidation (physical)	Lack of common or consolidated platform	Lack of common or consolidated platform; Enterprise IT to provision and manage infrastructure	Single consolidated platform managed centrally; zones for experimenting vs. production
	Environment design approach	Each AI team establishes its own image	Integrated image available implementing standards; full flexibility to modify to AI team needs	One enterprise image controlled centrally; Flex for AI teams to experiment with only AI functionality
Roles and responsibilities	Central AI Tech Team's role	Sets standards	Sets standards, builds and manages reference implementation / image	Develops and maintains the centralized ecosystem
	Business Unit IT Team's role	Responsible for AI technology and building functionality	Responsible for AI technology and building functionality	Building functionality only (e.g., build an AI based recommender using the platform tools)

Banks can develop an enterprise-level AI Risk Index to evaluate all AI/ML capabilities across categories of risk

ILLUSTRATIVE

AI models

- (9 points) - AI capabilities are leveraged directly for meeting regulatory needs (e.g., as part of a KYC/AML model)
- (3 points) - AI capabilities are indirectly supporting regulatory needs
- (1 point) - AI capabilities are not relevant to regulatory requirements



Client exposure

- (9 points) - AI capabilities are directly exposed to customers (e.g., model used by customers as part of digital apps) or involve processing of PII
- (3 points) - AI capabilities are indirectly exposed to customers (e.g., model used by organization internally for customer analytics)
- (1 point) - AI capabilities do not relate to customer (e.g., ML-based tool for employee retention)



Financial impact

- (9 points) - AI capabilities may lead to downside risk due to poor performance of the model
- (3 points) - AI capabilities helps create operational improvements (e.g., reduce time to market)
- (1 point) - AI capabilities do not directly map to financial or operational impact



Decision driver

- (9 points) - AI capabilities are used within 1 step away from making an actual business decision that has financial impact
- (3 points) - AI capabilities are used 2 or more steps away from making an actual business decision that has financial impact
- (1 point) - AI capabilities are not directly used for actual business decisions that have financial impact



Training data quality

- (9 points) - Quality of training data for AI capabilities is poor or cannot be validated
- (3 points) - Quality of training data is reasonably high and well documented
- (1 point) - Quality of training data is high, well documented and verifiable

AI Risk Index profile

- All AI tools and technologies can be classified across 3 risk tiers (High, Medium, Low) based on a total score across five key dimensions
 - » High risk: >27
 - » Medium risk: 15-27
 - » Low risk <15
- **Any AI tool / technology that has a high Regulatory impact (9) must be rated high risk** regardless of the overall score

A successful AI/ML risk governance could result in the following outcomes

- ❑ Every model / instance of **embedded AI is accounted for** and managed according to level of risk, providing transparency and facilitating risk mitigation
- ❑ There is a set of **operating principles for identifying, assessing and managing 3rd party tools with embedded AI** across the procurement and deployment lifecycle, clarifying responsibilities and streamlining processes
- ❑ There is a **single repository that catalogs and provides access to AI capabilities** available in the enterprise, reducing development time and time to market
- ❑ There is a **common set of technology platforms** for experimentation, training, testing and deployment of AI models used across the bank, driving operational efficiencies and cost savings

Three key messages to take away

1 **The increasing prevalence of AI/ML amplifies model risk for financial institutions**


- Complexity of this expanded class of models amplified model risk, e.g., through bias or unfair discrimination and lack of transparency of use

2 **Mitigating this risk requires enhancements to policy and governance as well the validation process and function**

- Policy and governance requires enhancements to, e.g., risk tiering, risk appetite, roles and responsibilities and lifecycle controls
- Model validation function requires enhancement to the independent review process as well as capabilities, tools and infrastructure

3 **Timely development and roll-out of these enhancements is critical for control functions not to become a bottleneck to bank innovation**

- Banks that do not have enhancements to its model risk management may result in delays or unnecessary obstacles to bank-wide innovation



1:25p.m.-2:20p.m.

Panel 4 - Contracting for AI in Financial Services

Speakers



Richard Assmus
Partner
Mayer Brown




Rohith George
Partner
Mayer Brown



Aviad Levin
*Senior Vice President,
Legal*
Socure



Sara Vero
*Emerging
Technologies Lawyer*
JP Morgan




2:20p.m.-2:40p.m.

Tech Talk: BaaS and Open Banking

Speaker



David Beam
Partner
Mayer Brown



2:40p.m.-3:30p.m.

Panel 5 - Insurtech

Speakers



Tara Bodden
*General Counsel and
Head of Claims
At-Bay*



Paul Chen
*Partner
Mayer Brown*



Shruthi Rao
*Co-Founder and CEO
Adapt Ready*



Vikram Sidhu
*Partner
Mayer Brown*

AI Opportunities in Insurance

AI Application

- Analyze and confirm consumer behavior and car/home/product performance
- Automatic or expedited emergency response if accident/loss is detected
- Customize information to educate customers on how to prevent losses and reduce premiums ("Predict and Prevent" methodology)
- Filter key data needed to expedite claims (human interaction, when needed, is focused on customer's needs rather than collecting data)



Potential Benefits

- More accurate risk assessment – AI algorithms can quickly develop risk profiles and help streamline underwriting process
- Risk prevention – alert drivers of unsafe driving behaviors and incentivize them to earn lower premiums by adopting safer practices
- More efficient claims process and greater customer satisfaction
- Usage based insurance (UBI)



Enabling Technologies

- Improved data analytics through use of machine learning (cognitive technologies)
- Interconnected devices (telematics, IoT, wearables)
- Interconnected data ecosystems (e.g., data aggregators, open source data, blockchain, etc.)
- Autonomous products and services (vehicles, drones, robotics, robo-advisers)
- Cybersecurity



AI Challenges in Insurance



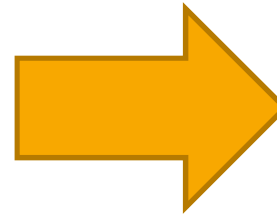
Data Collection

- How is data collected?
- How accurate is the data?
- What are the data privacy rules?

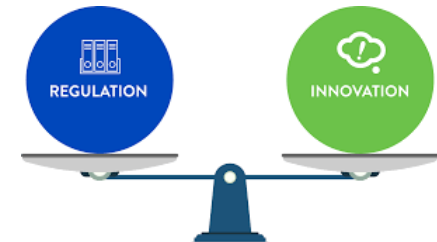


Data Use

- Inappropriate or incomplete data sets
- Algorithm bias
- Lack of transparency and explainability for underwriting and claim decisions



How to regulate while enabling innovation?



State Insurance Regulators and AI

- State insurance regulators want to enable (or at least not stifle) innovation
- But questions and concerns about use of AI in insurance in compliance with applicable insurance laws and regulations
- Efforts at the national (NAIC) level as well as by the states

NAIC

- National Association of Insurance Commissioners (NAIC) – association of the US insurance regulators from all 50 states, DC and the territories
- Considering AI usage in insurance to assess if current state laws and regulatory tools are sufficiently protecting buyers of insurance
- NAIC's Innovation, Cybersecurity, and Technology (H) Committee
 - Broad mandate with respect to innovation, cybersecurity, privacy, e-commerce and technology in insurance
 - One of its key working groups is the Big Data and Artificial Intelligence (H) Working Group

NAIC's Big Data and Artificial Intelligence (H) Working Group

- Researching use of big data and AI including ML in insurance
- Evaluating existing regulatory frameworks for overseeing and monitoring AI use
- Reviewing current audit and certification programs and/or frameworks that could be used to oversee insurers' use of consumer and non-insurance data and models using intelligent algorithms including AI
- Assessing data and regulatory tools needed for state insurance regulators to appropriately monitor the marketplace and evaluate the use of big data, algorithms, and AI/ML in underwriting, rating, claims and marketing practices

NAIC's Big Data and Artificial Intelligence (H) Working Group

- States' surveys of AI/ML use in private passenger auto, home and life insurance
- Third-Party Data and Model Vendors workstream
 - Considering several potential initial steps for enhanced regulatory oversight of third-party data and model vendors
 - Including requiring insurers to certify that the models that are being used comply with certain standards and developing a library of third-party vendors
- Potentially will lead to the development of or modifications to NAIC model laws, regulations, handbooks and regulatory guidance

NAIC's Collaboration Forum on Algorithmic Bias

- Forum to promote ongoing discussion among insurance industry stakeholders during regularly hosted events and presentations
- Issues such as:
 - What kinds of algorithms raise concerns for insurance regulators
 - How might bias arise in algorithms
 - Which tools might be effective in minimizing bias and detecting bias
 - What are potential regulatory frameworks for addressing algorithmic bias

NAIC's Collaboration Forum on Algorithmic Bias

- Themes raised at forum:
 - Risk management in use of AI
 - Ethical use of data and predictive models
 - Need for testing
 - Access to protected class data
 - Need for diversity
 - Model explainability

State-Specific Developments: New York

- NY DFS Circular Letter No. 1 (January 18, 2019)
- Resulted from investigation into New York life insurers' underwriting guidelines and practices
- To address concerns about potential unlawful discrimination, the circular letter set forth two guiding principles for New York insurers that use external data in underwriting:
 - Insurers using external data sources must independently confirm that the data sources do not collect or use prohibited criteria
 - Insurers should not use external data unless they can establish that it is not "unfairly discriminatory" in violation of applicable law

State-Specific Developments: California


- California Department of Insurance Bulletin 2022-5 – June 30, 2022
- Focus on allegations of racial bias and discrimination in marketing, rating, underwriting, and claims practices by insurers and other licensees
- Concerns about transparency, unfair discrimination (or discriminatory impact) and use of models and data without sufficient actuarial nexus to risk of loss
- Directed insurers and other licensees to:
 - “avoid both conscious and unconscious bias or discrimination” in use of AI
 - “before utilizing any data collection method, fraud algorithm, rating/underwriting or marketing tool, insurers and licensees must conduct their own due diligence to ensure full compliance with all applicable laws”

State-Specific Developments: Connecticut

- Connecticut Insurance Department April 20, 2022 bulletin – The Usage of Big Data and Avoidance of Discriminatory Practices
- Highlighted similar themes as California and New York
 - Insurers and other licensees must use technology and data in full compliance with anti-discrimination laws
- Began requiring a “data certification” that insurance licensees’ use of data complies with CID’s bulletin and applicable laws
 - First certification was due on September 1, 2022


State-Specific Developments: Colorado

- Enacted statute in July 2021
- Requires Colorado Insurance Commissioner to adopt rules prohibiting insurers from using any external consumer data, information sources, algorithms or predictive models that use external consumer data and information sources in a way that unfairly discriminates based on race, color, national or ethnic origin, religion, sex, sexual orientation, disability, gender identity or gender expression
- Colorado Division of Insurance has conducted several stakeholder meetings to discuss related issues before adopting rules on how insurers should test and demonstrate that their use of big data is not unfairly discriminating against consumers



3:30p.m.-3:40p.m.

Break



3:40p.m.-4:35p.m.

Panel 6 - Use of Digital Engagement Practices by Broker-Dealers and Investment Advisers

Speakers



Steffen Hemmerich
Partner
Mayer Brown



Jeffrey Lee
*Chief Technology
Officer*
The Motley Fool



Tram Nguyen
Partner
Mayer Brown



Bryan Weaver
VP, Associate General Counsel
Fidelity Investments
Chief Legal Officer
Digital Brokerage Services LLC

Scenario 1


Innovation Tech, a dually registered broker-dealer and investment adviser, serves a predominantly retail customer base and historically has focused on offering “traditional” investment products. To increase its market share of a younger, more tech-savvy, customer base, Innovation Tech has developed a mobile application or “App” that would simplify the on-boarding process, streamline the investment process, and allow customers to monitor their trading (and that of their “investment club”).

Scenario 2

One feature of the App, **Millionaire School**, is very popular with customers. This feature allows customers to complete three 5-minute “games” which mimic trading activities. Customers receive short infographics on investing fundamentals, can make “paper trades” (*i.e.*, simulation trades made without real currency) and then track the performance of these paper trades relative to the markets or their actual portfolios. These “games” include the ability to engage in paper trades with other App customers or a “bot,” with prizes awarded to the most successful investors at the end of each day.

Scenario 3

After 6 months, the App has drawn considerable attention from both customers and competitors. To stand out in a competitive market, and based on customer feedback, Innovation Tech believes that App 2.0 should enable customers to invest in digital assets and to track or “follow” investment activities of well-known investors, celebrities and/or “influencers.” The team is considering whether App 2.0 should allow celebrities/influencers to promote the App (for example, by including videos on the App, linking on the App to celebrities’/influencers’ social media sites and/or celebrities/influencers promoting App 2.0 on their social media sites).



3:40p.m.-4:35p.m.

Panel 7- Governance Issues for AI

Speakers



Esther Chang
Partner
Mayer Brown



Cameron Craig
*Deputy General Counsel
and Group
Head of Data Privacy
Group Legal*
HSBC Holdings




Chris Hetner
Member
Nasdaq Center for
Board Excellence's
Insights Council



**Dominique
Shelton Leipzig**
Partner
Mayer Brown



Oliver Yaros
Partner
Mayer Brown



5:30p.m.-5:45p.m.

Developing Your AI Mission

Speaker



Brad Peterson
Partner
Mayer Brown



5:45p.m.

Cocktail Reception

Disclaimer

- These materials are provided by Mayer Brown and reflect information as of the date of presentation.
- The contents are intended to provide a general guide to the subject matter only and should not be treated as a substitute for specific advice concerning individual situations.
- You may not copy or modify the materials or use them for any purpose without our express prior written permission.



[Americas](#) | [Asia](#) | [Europe](#) | [Middle East](#)

mayerbrown.com

Mayer Brown is a global services provider comprising associated legal practices that are separate entities, including Mayer Brown LLP (Illinois, USA), Mayer Brown International LLP (England), Mayer Brown (a Hong Kong partnership) and Taill & Chequer Advogados (a Brazilian law partnership) (collectively the "Mayer Brown Practices") and non-legal service providers, which provide consultancy services (the "Mayer Brown Consultancies"). The Mayer Brown Practices and Mayer Brown Consultancies are established in various jurisdictions and may be a legal person or a partnership. Details of the individual Mayer Brown Practices and Mayer Brown Consultancies can be found in the Legal Notices section of our website. "Mayer Brown" and the Mayer Brown logo are the trademarks of Mayer Brown. © Mayer Brown. All rights reserved.



Artificial Intelligence in Fintech

THE FUTURE OF FINANCIAL SERVICES: CORPORATE GOVERNANCE IN
A MODERN WORLD

Agenda

1. Artificial Intelligence in Fintech: How It Works
2. Regulatory Focus on the Board's Duty of Care and Oversight Has Heightened over the Past Year
3. How the Industry is Using AI
4. AI Regulatory Guide: The United States
5. California & Artificial Intelligence
6. AI Regulatory Guide: Europe
7. Algorithmic Bias
8. Questions?



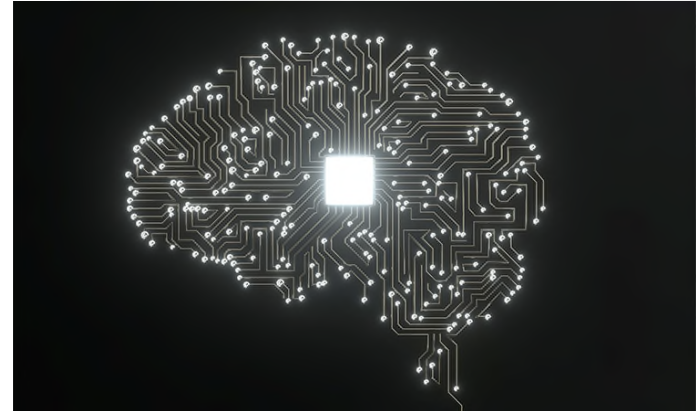


Artificial Intelligence in Fintech: How It Works

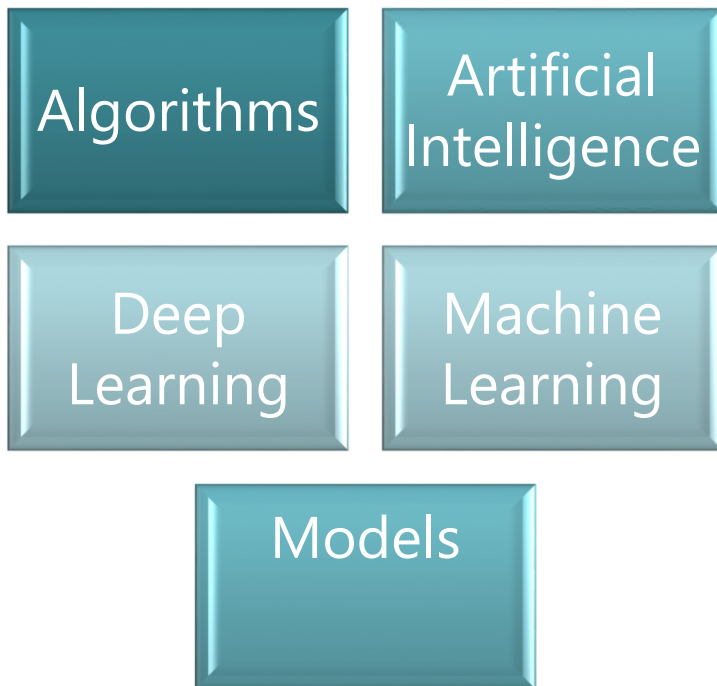


What is Artificial Intelligence (AI)?

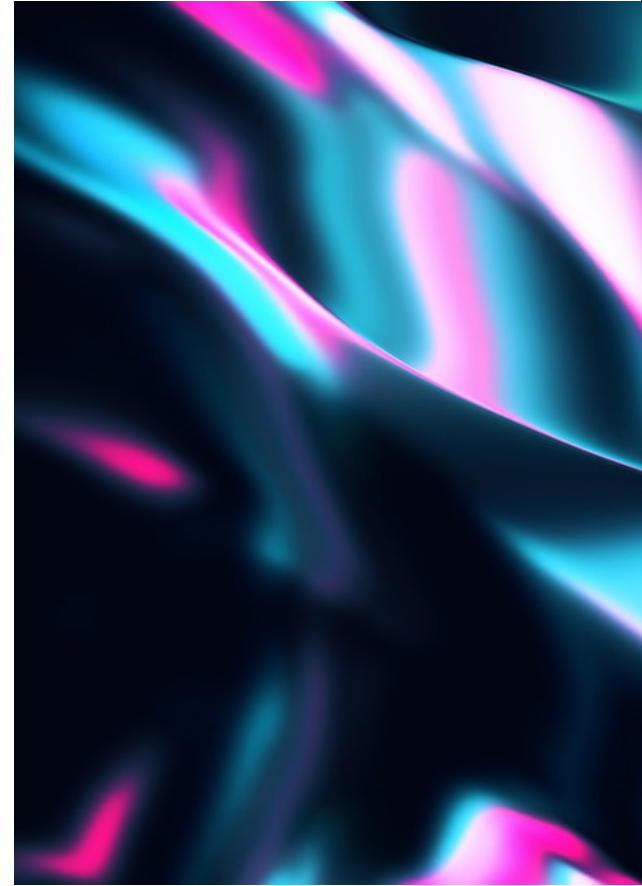
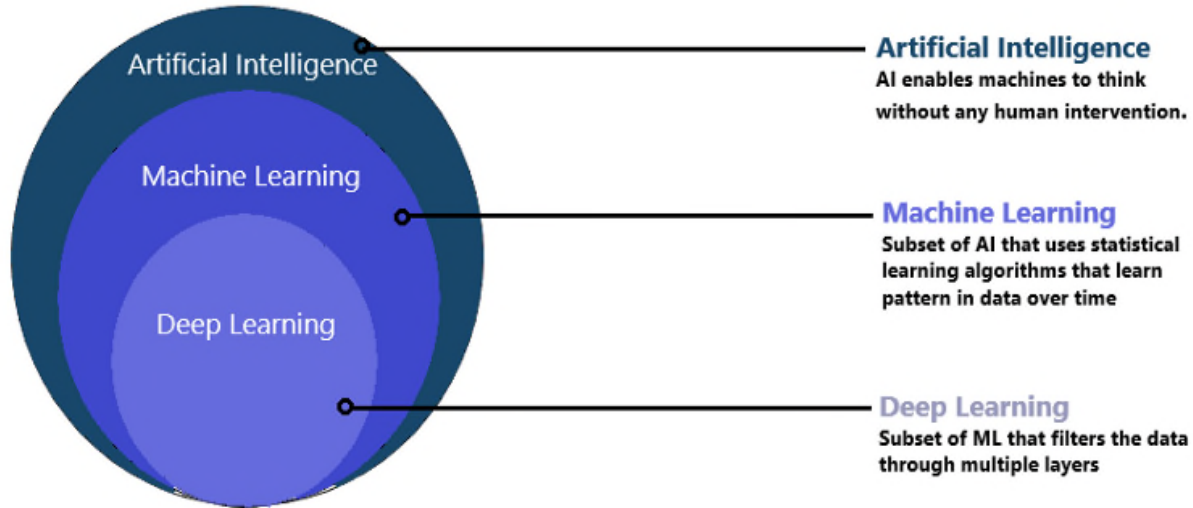
- AI is the basis for mimicking human intelligence processes through the creation and application of algorithms built into a dynamic computing environment.
- In its simplest form, artificial intelligence is a field that combines computer science and robust datasets to enable problem-solving.
- Has three key components:
 - Computational systems
 - Data and data management
 - Advanced AI algorithms (code)
- Institutions must be mindful of data privacy laws if AI is used to analyze data that is collected from its user base. Current state privacy laws have various definitions.



How do we define AI?



How do we define AI?



How Does AI Work in the Fintech Industry?


- **User Behavior Analysis** – institutions typically use AI APIs to help predict user behavior (e.g. the user requests data about their expenses in the last month – a single request. On the server-side, with the help of AI, the institution can predict their follow-up request)
- **Regulatory Technology (“RegTech”)** – institutions can use Regulatory Technology to manage regulatory compliance using AI algorithms. Includes client identification, transaction monitoring, regulatory analysis, and reporting. Typically seen in fraud detection
- **Risk Score Profiling** – institutions can also use Artificial Neural Networks (ANNs) to train technologies on the user’s historical data and classify whether they are a low or high risk borrower.
- **Improved Customer Service** – many financial institutions use AI-powered chatbots and personalized apps (e.g., banking apps)
- **Increased Security** – As the number and complexity of cyberattacks increase, artificial intelligence (AI) can assist under-resourced security management strategists with:
 - Diagnostic capabilities
 - Processing sensitive financial data



How Does AI Work in the Fintech Industry?

AI Tools in Fintech	Type of Data Involved
User Behavior Analysis	IP address, device ID, user behavior and activity on webpages
RegTech	Financial transactions, user information (i.e. name, account number)
Risk Score Profiling	Financial information, sensitive information (i.e. SSN)
Improved Customer Service	Customer information (i.e. name, address, account number)
Increased Security	Customer financial information





Regulatory Focus on the Board's Duty of Care and Oversight Has Heightened over the Past Year



DOJ's New Stance on Corporate Enforcement

DOJ Pushing Ahead With Corporate Settlement Policy That Could Make Execs Liable, Official Says

The U.S. Justice Department is charging ahead with a new policy that makes top executives certify the effectiveness of their compliance program as part of corporate resolutions



Why Cloud Investments May Not Be Living Up to the Hype

The COVID-19 pandemic accelerated many organizations' push to embrace the cloud. Now it's time to become more strategic, according to recent research.

The Emergence of Chief Controls Officers

TIAA's Pamela Feldstein leads a new team tasked with understanding and reviewing the firm's internal controls and processes as it aims to achieve operational excellence and hone customer experience.

Stanford's Chief Ethical Officer

- The DOJ will now have compliance officers sign off on the effectiveness of company programs as part of settlements.
- Alixandra Smith, the deputy chief of the criminal division at the Brooklyn U.S. attorney's office said recently:
 - "The certifications serve as a tool for the Justice Department as it tries to hold individuals accountable for their role in corporate wrongdoing"

Further Revisions to Corporate Criminal Enforcement Policies Following Discussions with Corporate Crime Advisory Group | Justice.gov

Recent Developments: SEC Feb. 9, 2022 Proposed Rule

Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies

- “Proposed rule 38a-2 would require a fund’s **board of directors**, including a majority of its independent directors, initially to **approve the fund’s cybersecurity policies and procedures**, as well as to review the written report on cybersecurity incidents and material changes to the fund’s cybersecurity policies and procedures that...would be required to be prepared at least annually”
- The required written reports... would provide fund directors with **information necessary to ask questions and seek relevant information regarding the effectiveness of the program and its implementation**, and whether the fund has adequate resources with respect to cybersecurity matters, including access to cybersecurity expertise. **We anticipate that a fund’s board’s review of the written reports would naturally involve inquiries about cybersecurity risks** arising from the program and any incidents that have occurred

“Board oversight should not be a passive activity”

SEC February 9, 2022 report

Recent Developments: SEC March 2022 Proposed Rule

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

- “Cybersecurity is already among the top priorities of many boards of directors [citation omitted] and cybersecurity incidents and other risks are considered one of the largest threats to companies.[Citation omitted] **Accordingly, investors may find disclosure of whether any board members have cybersecurity expertise to be important as they consider their investment in the registrant as well as their votes on the election of directors of the registrant.**”

For all public companies, the SEC describes its intention to require disclosure from public companies regarding whether their boards have members with cybersecurity experience.

Recent Developments: NY DFS July 29, 2022 Proposal

Cybersecurity Requirements for Financial Services Companies

- NY DFS' proposed rule would require board approval of cybersecurity policies that cover (at a minimum):
“(a) information **security**; (b) **data governance** and classification; and [] customer **privacy**.”
- “The board or an appropriate committee of **the board shall have sufficient expertise and knowledge, or be advised by persons with sufficient expertise and knowledge**, to exercise effective oversight of cyber risk and a committee or subcommittee assigned responsibility for cybersecurity.”

Regulators
Recommend
Third Party
Advisors to
Protect the
Board of
Directors.

Shareholder Derivative Actions Naming BoD Re Privacy & Cyber are on the Rise – 70+ Actions

CPO
MAGAZINE

HOME NEWS INSIGHTS RESOURCES



In recent months, a trend has begun to emerge among plaintiffs' lawyers seeking to file cybersecurity incident-related shareholder derivative lawsuits – attorneys are increasingly now filing claims specifically based on failures surrounding duty of oversight. In November of 2021, a shareholder derivative [lawsuit](#) was filed

Mayer Brown has identified 70+ shareholder derivative actions pertaining to privacy and cyber.

Overview of Lawsuits Against Officers and Directors

United States

1. Failure to Stay Informed
2. Lack of a Board Committee with Data Privacy and Security Oversight
3. Lack of Qualified Officers
4. Failure to Safeguard Personal Data
5. Failure to Respond to Known Cyber Threats
6. Failing to Conduct Adequate Due Diligence
7. False SEC Filings and Other Public Statements
8. Lack of Transparency
9. Insufficient Oversight of Vendors and Third Parties
10. Failure to Provide Timely and Adequate Notices
11. Compliance with Laws

DERIVATIVE ACTION



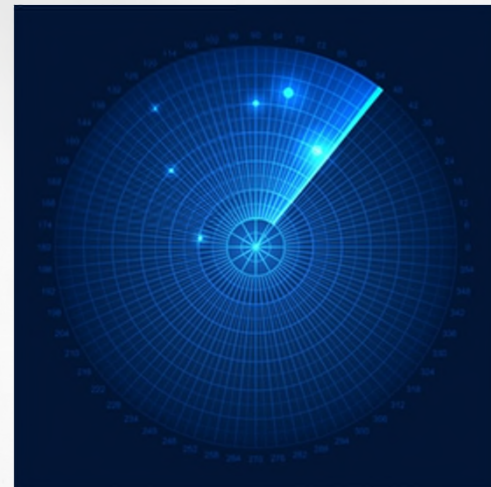
Focus on BoD Oversight of Privacy & Cyber is Global

- The **United Kingdom's** National Cyber Security Centre (NCSC) has a [Cyber Security Toolkit for Boards](#) website that contains "[r]esources designed to encourage essential cyber security discussions between the Board and their technical experts."
- **Denmark** guidance emphasizes BoD's oversight role when it comes to cyber [Centre for Cyber Security \(CFCS\) published a December 2019 cybersecurity guidance for boards of directors](#).
- **Australian Securities & Investment Commission** counseled board members to ask themselves: "**Does the board need further expertise to understand the risk?** Although boards may not require general technology expertise, for many companies it may be advisable to have one or more directors who have a strategic understanding of technology and its associated risks, or who have a background in cybersecurity. In some circumstances, *the board should consider the use of external cyber experts to review and challenge the information presented by senior management.*

BoD is the focus of regulators in the EU, MEA, and APEC

EU: Digital Operational Resilience Act (DORA)

- **EU** draft Digital Operational Resilience Act (DORA) covers “financial entities,” including crypto-asset service providers, as well as (critical) ICT {Information Communication Technology} third-party service providers. DORA states in Art. 4 (4): “Members of the management body of the financial entity shall actively keep up to date sufficient knowledge and skills to understand and assess ICT risks and their impact on the operations of the financial entity, including by following specific training on a regular basis, commensurate to the ICT risks being managed.”
- Art. 44 assigns the Member States the task of defining penalties for infringements. They shall, subject to the conditions provided for in national law, confer to the competent authorities the power to apply administrative sanctions and remedial measures to members of the management body.
- In Art. 28 et seqq., DORA introduces a targeted supervisory regime for the direct oversight of those ICT third-party service providers that are designated as “critical” by the competent “European Supervisory Authorities” (ESAs).

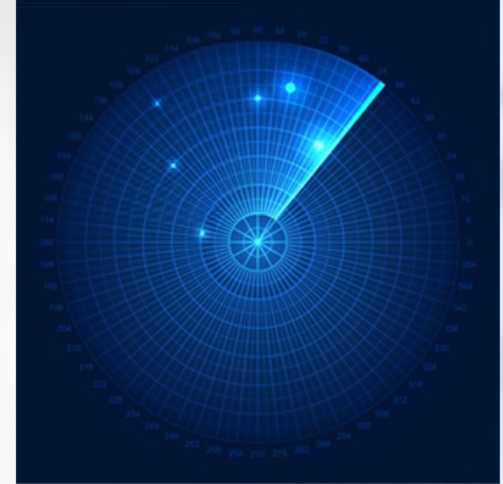


EU: Digital Operational Resilience Act (DORA)

Art. 4 (2): **The Management Body** shall define, approve, oversee and be accountable for the implementation of all arrangements related to the ICT risk management framework, which includes:

- Bearing the ultimate responsibility for managing the financial entity's ICT risks
- Setting clear roles and responsibilities for all ICT-related functions;
- determine the appropriate risk tolerance level of ICT risk of the financial entity;
- Approve, oversee and periodically review the implementation of the financial entity's ICT Business Continuity Policy and ICT Disaster Recovery Plan, ICT audit plans, audits, and material modifications thereto; arrangements regarding the use of ICT services provided by ICT third-party service providers

EU: Proposal for a Regulation on Digital Operational Resilience in the Financial Sector – what you need to know | [DataGuidance.com](https://www.dataguidance.com)





How the Industry is Using AI



Claims Management and Fraud Detection

- **How banks are doing it** – using Ayasdi (AI vendor) for anti-money laundering and reducing false positives in fraud detection processes
- **What the AI is doing** – identifying patterns within historical data that may point toward money laundering, which helps the bank stop payments before they violate regulations
- **Type of AI** – Ayasdi's solutions are primarily based on anomaly detection technology, which is helpful for recognizing deviations from a pre-established norm. AI software analyzes the sources and destinations of customer payments to make sure the funds are coming from legitimate sources.

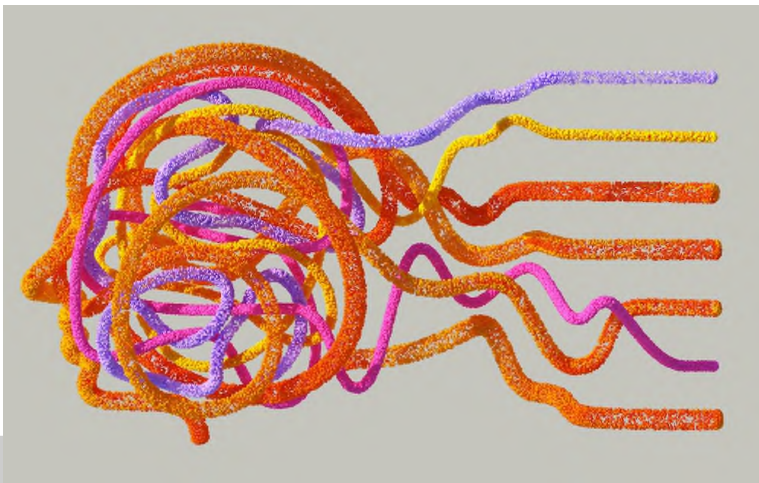


BOARD TIP:

Identify how personally identifiable information being collected, and how this process is disclosed.

Customer Service

- **How banks are doing it** – using AI-powered virtual agents (IVA) to assist with customer issues
- **What the AI is doing** – communicating with customers online
- **Type of AI** – The IVA solution uses advanced conversational AI to understand languages, accents, and dialects. It can also pinpoint the intent of a call by making sense of the customer's word's choices, meaning customers can speak using their own words and be their own words and be understood

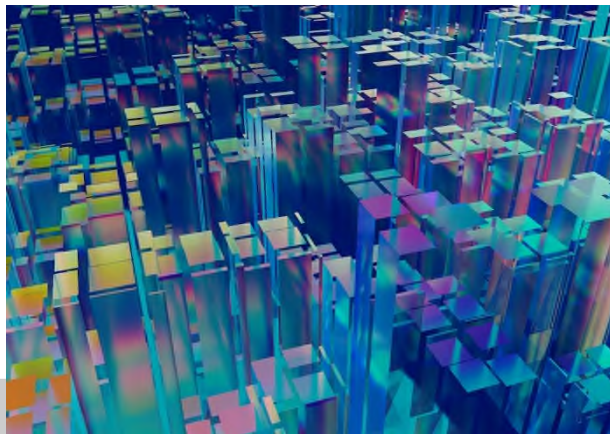


BOARD TIP:

Get management to present a briefing at board meetings about how AI is being used and what steps are being taken for privacy and data security compliance.

Quantitative Trading

- **How banks are doing it** – used experts to collect, clean, and organize more than 150 million data points — both publicly available data and proprietary data — to train the AI model, the Predictive Intelligence Analytics Machine (PRIAM).
- **What the AI is doing** – predicts the best investors for a deal based on the equity offering details, historical deal participation, trading and client touch point information, and market data.
- **Type of AI** – an AI deal prediction system that uses a network of supervised machine learning algorithms to understand relationship trends between ECM deals and investors



BOARD TIP:

Understand what controls are in place with all joint-strategic partners that your company is sharing data with.

Expert Matching

- **How banks are doing it** – entered into a strategic partnership with Lynk Global to help clients make better, more informed investment and business decisions. A bank-wide AI, Data and Analytics, team to use more artificial intelligence and data analytics to drive the bank's digitization.
- **What the AI is doing** – Lynk uses machine learning algorithms to match the investment clients with users with experts ranging from on its platform.
- **Type of AI** – AI data engine that indexes individuals based on their experience and expertise to match users with subject matter experts on its platform for a variety of engagement formats, from a quick conversation to consulting project, to make knowledge sharing faster and easier than ever.



Intelligently
Connected

BOARD TIP:

Sharing relationships are often scrutinized at the regulatory level. Understand what controls are in place with all third parties that are joint strategic partners.

Complaint Management

- **How banks are doing it** – incorporating AI and machine-learning initiatives to accelerate operations, streamline services, and enhance customer experiences.
- **What the AI is doing** – uses feedback connections to process data and extract intent from the phrasing pulled from the data to determine best course of action and move quickly on them
- **Type of AI** – long-short term memory in natural language processing and spoken language understanding



BOARD TIP:

Boards should be aware of how the company handles complaints, which could later turn into high-profile litigation if not properly handled.



US State Privacy Trends:

WHAT THE BOARD SHOULD KNOW



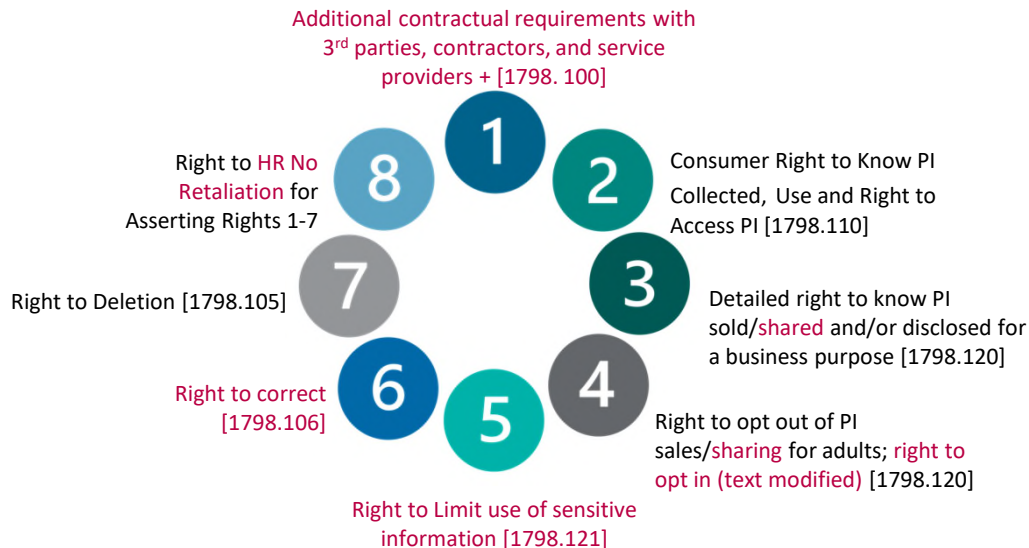
Definitions of Personal Information in State Data Privacy Laws

1. **California Consumer Privacy Act (CCPA)**
Effective January 1, 2020
2. **California Privacy Rights Act (CPRA)**
Effective January 1, 2023
3. **Virginia Consumer Data Protection Act (VCDPA)**
Effective January 1, 2023
4. **Colorado Privacy Act (CPA)**
Effective July 1, 2023
5. **Utah Consumer Privacy Act (UCPA)**
Effective December 31, 2023
6. **Connecticut Data Privacy Act (CTDPA)**
Effective July 1, 2023



Boards Should Ask How The Company Handles California's New Privacy Law

California Privacy Rights Act (CPRA)



Background

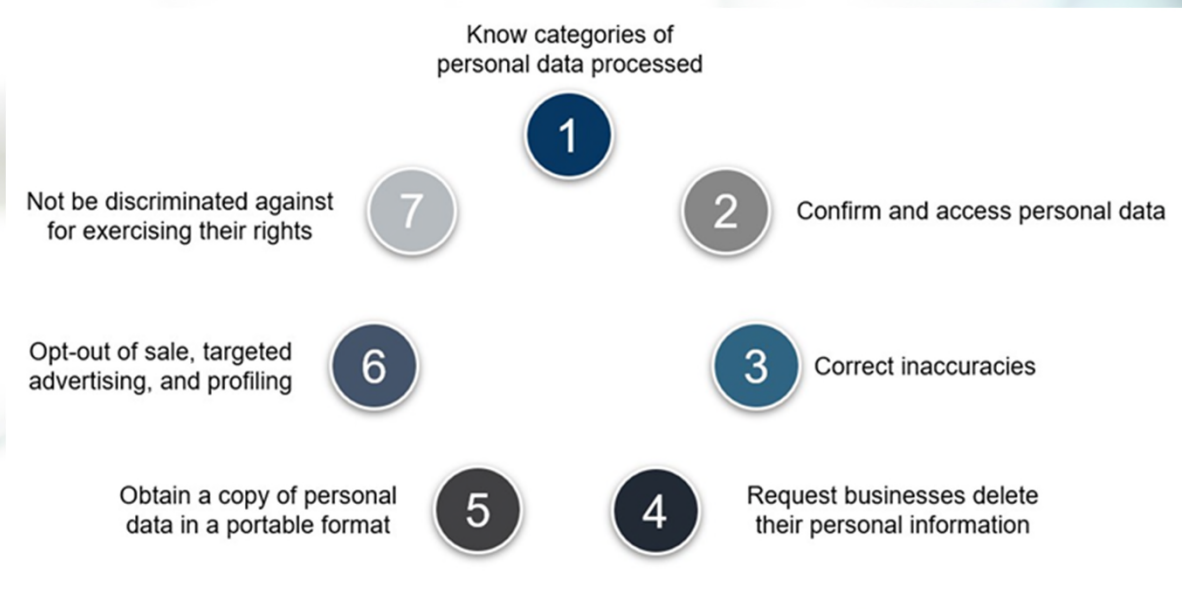
- CPRA amends the existing CCPA
- Becomes fully effective in 2023

New Legal Developments

- 30-day Cure Provision under CCPA will expire on January 1, 2023
- B2B and human resources data now within scope of legal regimes
- Contractual requirements with service providers, third parties and contractors now obligatory

Boards Should Ask How The Company Handles Colorado and Virginia's New Privacy Law

Colorado Privacy Act (2023) and Virginia Consumer Data Protection Act (2023)



Boards Should Ask The General Counsel To Report On The Company's Compliance

COMPARING CONSUMER RIGHTS UNDER STATE PRIVACY LAWS

Right	CTDPA	UCPA	CPA	VCDPA	CPRA	CCPA
Access	Yes	Yes	Yes	Yes	Yes	Yes
Correct	Yes	No	Yes	Yes	Yes	No
Delete	Yes (data provided by or obtained about consumer*)	Yes (data that consumer provided to controller)	Yes (personal data concerning consumer)	Yes (data provided by or obtained about consumer*)	Yes (data collected from consumer)	Yes (data collected from consumer)
Portability	Yes	Yes	Yes	Yes	Yes	Yes
Opt-out of sale	Yes	Yes	Yes	Yes	Yes	Yes
Non-discrimination	Yes	Yes	Yes	Yes	Yes	Yes
Appeals process	Yes	No	Yes	Yes	No	No

* The CTDPA authorizes businesses that collect data indirectly (about, rather than from, a consumer) to opt the consumer out of processing as an alternative or to retain (suppress) minimal data to ensure continued deletion. The VCDPA was amended on April 11, 2022, in like fashion.

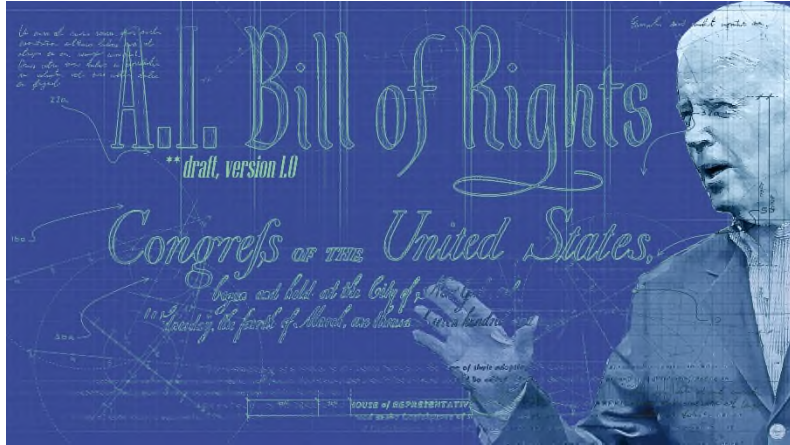


AI Regulatory Guide:

THE UNITED STATES



US Federal Guidance: The White House



- On October 4, 2022, President Biden issued the Blueprint for an AI Bill of Rights to ground federal principles in “an AI-powered world.” The pillars of this framework are are:
 - Safe and Effective Systems
 - Algorithmic Discrimination Protections
 - Data Privacy
 - Notice and Explanation
 - Human Alternatives, Consideration, and Fallback

BOARD TIP:

Boards should ensure its AI systems and use mirror White House guidelines.

US Federal Regulatory Guidance: The SEC

- In August 2022, the SEC issued its draft 2022-2026 fiscal plan. Among other initiatives, the agency aims to “build out its systemic risk identification abilities” and “ensure an ongoing proactive approach” which can be achieved by expanding disclosure and analytical tools, **broadening the use of machine learning and artificial intelligence**, developing long-term risk analysis directly connected to policy development, and focusing on more strategic and collaborative analysis across all regulated activities.



U.S. SECURITIES AND
EXCHANGE COMMISSION

Strategic Plan Fiscal Years 2022-2026 | SEC.gov

BOARD TIP:

It is important that boards pay attention to applicable regulators' actions and intentions with respect to AI oversight.

US Federal Regulatory Guidance: The SEC

- SEC Chair Gary Gensler **highlighted the important challenges that artificial intelligence** in robo-advisory services and cybersecurity disclosures **may bring**, namely, **conflict of interest, bias and systemic risks**.
- Chairman Gensler highlighted **one area that may require regulation to address is behavioral nudges**. When broker-dealers use these techniques to influence investors' behavior, "they may create gray areas between what is and isn't a recommendation — gradations that could be worth considering through rulemaking."



U.S. SECURITIES AND
EXCHANGE COMMISSION

**SEC Joins FTC in Voicing Concerns Over AI as
Risk of Regulation Looms | PYMNTS.com**

BOARD TIP:

Boards should take regulator signals of specific areas of concern as opportunities to assess gaps or weaknesses in company privacy and security policies.

US Federal Regulatory Guidance: The CFPB

- The Consumer Financial Protection Bureau (CFPB) confirmed in a circular published that **financial companies may violate federal consumer financial protection law when they fail to safeguard consumer data**. The circular provides guidance to consumer protection enforcers, including examples of when firms can be held liable for lax data security protocols.
- The circular provides examples of widely implemented data security practices and notes some examples where the failure to implement the following data security measures might increase the risk that a firm's conduct triggers liability under the Consumer Financial Protection Act, including:
 - Multifactor authentication;
 - Adequate password management;
 - Timely software updates



Consumer Financial
Protection Bureau

Consumer Financial Protection Circular 2022-04 | [ConsumerFinance.gov](https://www.consumerfinance.gov)

BOARD TIP:

Ensure your company's data security practices are regularly tested, updated, and secure to minimize regulator scrutiny.

US Federal Regulatory Guidance: The FTC

- On June 16, 2022, the FTC issued a report to Congress which warned about using AI to combat online problems, and urged policymakers to exercise caution about relying on it as a policy solution.
- In particular, **the FTC highlighted that AI cannot be seen as the solution to the spread of harmful online content**, which instead requires a broad societal effort.
- The FTC report warns against using AI as a policy solution for such online problems and noted that its adoption could introduce a range of additional harms.
- **Furthermore, the report outlines several problems related to the use of AI tools, including inherent design flaws and inaccuracy, bias and discrimination, and commercial surveillance incentives.**



**Combatting Online Harms
Through Innovation | [FTC.gov](https://www.ftc.gov)**

BOARD TIP:

Boards should make sure to properly assess the risks and benefits of AI use.



California & Artificial Intelligence

California – CPRA and AI

- No explicit guidance on artificial intelligence.
- Notably, in the May 2022 CPRA regulations, one of the most conspicuous omissions concerns the lack of parameters for automated decision-making.
- The CPRA defines “profiling” as “any form of automated processing of personal information, as further defined by regulations pursuant to paragraph (16) of subdivision (a) of Section 1798.185 [of the CCPA], to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements,” leaving the contours relatively amorphous in scope
- Contrary to the scope defined by other comprehensive state privacy laws and GDPR, the CPRA’s language casts an incredibly wide net that could be argued to cover everything from invasive facial recognition in public places to routine automated processes like calculators and spellcheckers that may process personal information.

BOARD TIP:

Boards should ensure that adequate privacy and cyber competence exists in the boardroom either through board appointments or third party advisors.



California – AI Pending Bills

- **CA A.B. 2273 (Pending)** – Enacts the California Age-Appropriate Design Code Act. Authorizes the Attorney General to seek an injunction or civil penalty against any business that violates its provisions. Holds violators liable for a civil penalty of not more than specified date per affected child for each negligent violation, or not more than specified date per affected child for each intentional violation
- **CA A.B. 2408 (Pending)** – Prohibits a social media platform, as defined, from using a design, feature, or affordance that the platform knew, or by the exercise of reasonable care should have known, causes a child user, as defined, to become addicted to the platform. Provides that a social media platform is not subject to a civil penalty if it demonstrates that it met certain requirements.
- **CA A.B. 1018 (Pending)** – Requires a social media platform to disclose to the public, on or before a specified date, and annually thereafter, statistics regarding the extent to which, in the preceding 12-month period, items of content that the platform determined violated its policies were recommended or otherwise amplified by platform algorithms, disaggregated by category of policy violated.

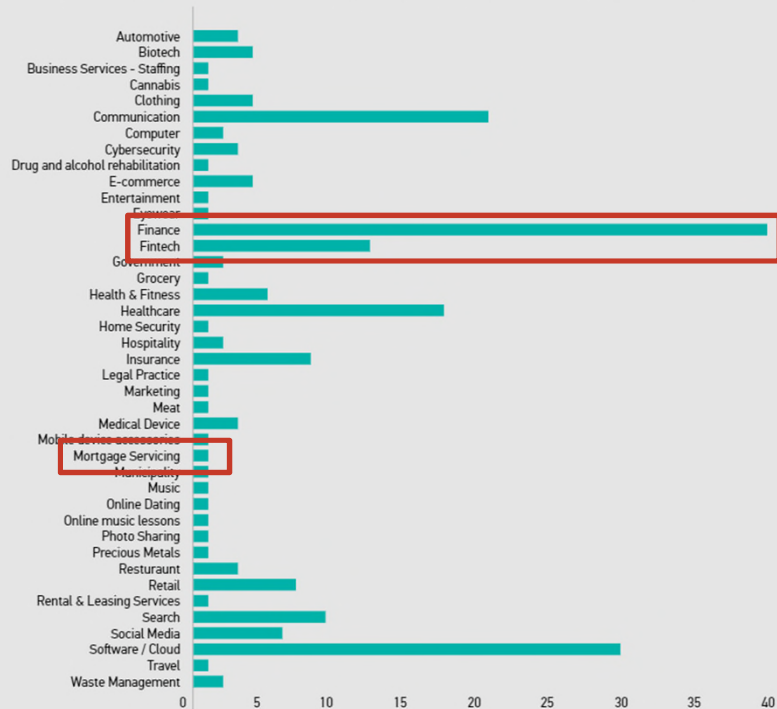


United States – Litigation Under CCPA

There has been an increase in the number of CCPA cases impacting the financial industry, notably in Finance, FinTech, and Mortgage Servicing.

Industry

Many of the CCPA cases focus on the technology sector with an emphasis on software. There has also been an increase in the number of cases impacting the financial industry and in turn, FinTech, followed by healthcare, search, and social media.



CCPA Litigation

- **McCoy v. Alphabet, Inc. et al., No. 5:20-cv-05427 (N.D. Cal.)**
 - **Allegations:** alleged Google violated the CCPA because the Defendant's failed to disclose that they collected data related to "non-Google apps, including the duration of time spent on non-Google apps and the frequency that non-Google apps are opened."
 - **Holding:** the court dismissed Plaintiff's CCPA claims, holding that the law does not provide a private right of action outside of the data breach context.
- **Gardiner v. Walmart Inc. et al., No. 4:20-cv-04618 (N.D. Cal.)**
 - **Allegations:** Alleged Walmart suffered a data breach it never disclosed; claimed that the personal information associated with his Walmart account had been discovered on the dark web and presented the results of security scans performed on Walmart's website, which allegedly show certain vulnerabilities.
 - **Holding:** the court dismissed plaintiff's CCPA claim on two grounds: (1) plaintiff needed to plead a breach occurring after January 1, 2020, and (2) plaintiff did not sufficiently allege disclosure of his personal information as defined in the CCPA. Cal. Civ. Code § 1798.81.5.

BOARD TIP:

It is important that boards contextualize cyber risk to financial exposure.





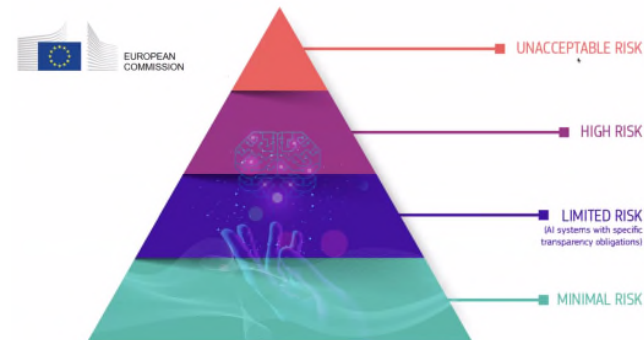
AI Regulatory Guide:

EUROPE



EU AI developments: The EU AI Act

- The European Commission submitted a proposal for an EU Artificial Intelligence Act in 2021. Requirements for AI systems divided into categories depending on risks:
 - Ban on AI systems with unacceptable risks. E.g. AI manipulation of vulnerable groups / evaluation of individuals to calculate "social score", real time biometric identification apart from in exceptional circumstances
 - Strict requirements for high risk AI systems - e.g. those related to critical infrastructure, educational training, and employee selection. Conformity assessment required before tech can enter EU market. E.g., providers must establish, maintain and document rigorous risk management systems, ensure an appropriate type and degree of transparency to users, gave effective oversight and control of AI by natural persons
 - Notice requirements for low risk AI systems – E.g. those that interact with humans, detect emotions, determine association with social categories based on biometric data, generate / manipulate content (deep fakes)
 - Penalties of up to €30,000,000 or 6% of total worldwide annual turnover (whichever is higher)



EU AI Developments: Liability Rules

- On 28 September 2022, the European Commission adopted proposals for two directives adapting non-contractual civil liability rules to AI. The proposed AI Liability Directive aims at targeted harmonization measures on civil liability for AI among the EU Member States. The revised Product Liability Directive proposes adaptations to the producer's strict liability (sometimes referred to as 'no fault liability') for defective products that have caused damage to private property or injury.
- Under the proposed Product Liability Directive, compensation is available when defective AI causes damage, without the injured person having to prove the manufacturer's fault. Not only hardware manufacturers but also software providers and providers of digital services that affect how the product works (such as a navigation service in an autonomous vehicle) can be held liable. Manufacturers can be held liable for changes they make to products they have already placed on the market, including when these changes are triggered by software updates or machine learning.
- The parallel proposal for an AI Liability Directive seeks to ensure that, where an injured person has to prove that an AI system caused damage in order to obtain compensation under national law (e.g. if someone failed a job interview because of discriminatory AI recruitment software), the burden of proof can be alleviated if certain conditions are met.
- The proposed liability rules for AI will complement other proposed laws such as the EU AI Act, the Digital Services Act and the Digital Resilience Act.

Other European AI developments

- UK published AI policy paper in July 2022. Six cross-sectoral principles regulators to apply in their sector or domain:
 - Sector-specific approach: Unlike the EU's AI Act proposal, the policy paper sets out a de-centralised approach to AI regulation. No new AI specific regulator with separate enforcement powers
 - No central list of prohibited or high-risk use cases: Sector regulators to decide if the use of AI in specific scenario should not be allowed or should be subject to higher regulatory burden

GDPR – Privacy Principles

Lawfulness, Fairness, and Transparency

There must be a legal justification for processing personal data and the reason for processing must be transparent to the Data Subject.

Purpose Limitation

Personal data must be collected for specified legitimate purposes, and not further processed in a way incompatible with those purposes.

Data Minimization

All personal data collected must be limited to what is necessary in connection with the purpose for which it is collected.

Accuracy

Personal data must be accurate and be kept up to date.

Storage Limitation

Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

Integrity and Confidentiality

Personal data must be processed in a way that ensures appropriate security (Technical and Organizational Measures, “TOMs”).

Accountability

The controller shall be responsible for, and be able to demonstrate, compliance with these principles.

EU Regulatory Guidance: EU Parliament

- On May 3, 2022, the EU Parliament adopted the final report of the Special Committee on Artificial Intelligence in a Digital Age
- The report aims to establish an artificial intelligence ('AI') roadmap for up to 2030, with more than 150 policy recommendations on governance, data sharing digital infrastructure, investment, e-health, e-governance, industry, and security.
- The report makes a number of recommendations for a legal framework for AI, which will feed into upcoming work on the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence ('the AI Act')



European Parliament

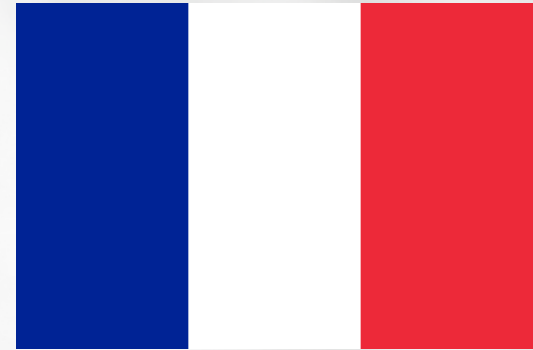
EU Regulatory Guidance: EU Parliament (Con't)

- Prior to the May 2022 guidance, the EU Parliament released a study on the Impact of GDPR on AI in June 2020. The report suggests that it is likely that GDPR 'will be interpreted in such a way as to reconcile both desiderata: protecting data subjects and enabling' useful applications of AI.
- Highlighted provisions where AI could fall under:
 - **Article 4(1):** Personal Data (identification, identifiability, re-identification)- In connection with the GDPR definition of GDPR definition of personal data, AI is raised in two key issues: i) the 're-personalisation' of anonymous data, namely the re-identification of the individuals to which such data are related; (ii) and the inference of further personal information from personal data that are already available.
 - **Article 4(2):** Profiling- Although GDPR does not explicitly refer to AI, it does address processing that is accomplished using AI technology. The process consists of using the data concerning a person to infer information on other aspects of that person.
 - **Article 4(11):** GDPR consent: According to GDPR, consent should be freely given specific, informed, and unambiguous. Consent plays a crucial role in the traditional understanding of data protection, based on the 'notice and consent model,' according to which data protection is aimed at protecting the right to 'informational self-determination.'



EU Regulatory Guidance: France Provides AI Recommendations

- On April 5, 2022, the French Data Protection Authority ('CNIL') released extensive publications concerning AI that restated GDPR's data protection principles, and applied them to AI specifically.
- CNIL recognized the tension between compliance with GDPR's data protection rules and AI, and that compliance would be difficult.
- CNIL noted that, depending on their exact role when processing personal data, AI providers and users can act as either data controllers or data processors.
- CNIL published recommendations and best practices to follow, which include:
 - identifying their role (i.e. data controllers vs. data processors) in the design, implementation, maintenance, and review of AI systems.
 - Ensure that data processing techniques are proportionate and necessary to achieve an explicit purpose.
 - Implementing appropriate security measures during the entire AI system lifecycle, starting from the training phase.
 - Detailing how they intend to comply with rights of data subjects



EU Regulatory Guidance: Spain Has Concerns About AI

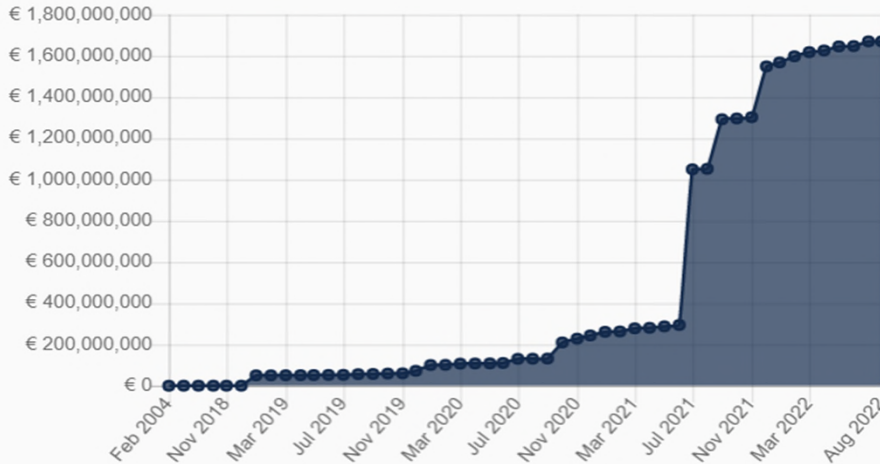
- On July 27, 2022, the Andalusian Council for Transparency and Data Protection ('CTPDA') issued a warning on the need to evaluate projects that massively process personal data or use Artificial Intelligence ('AI') to protect the rights of citizens.
- The CTPDA highlighted that the large scale processing of personal data and use of AI may constitute a threat to the rights and freedoms of citizens.
- It also noted that it was necessary to carry out a Data Protection Impact Assessment ('DPIA') prior to the processing of personal data through the use of AI
- The DPIAs required a systematic description of the planned treatment of operations, evaluating the need and proportionality of processing, alongside an assessment of the risks to the rights and freedoms of persons concerned.



GDPR Today – Increasing Fines

1. Course of overall sum and number of fines (cumulative):

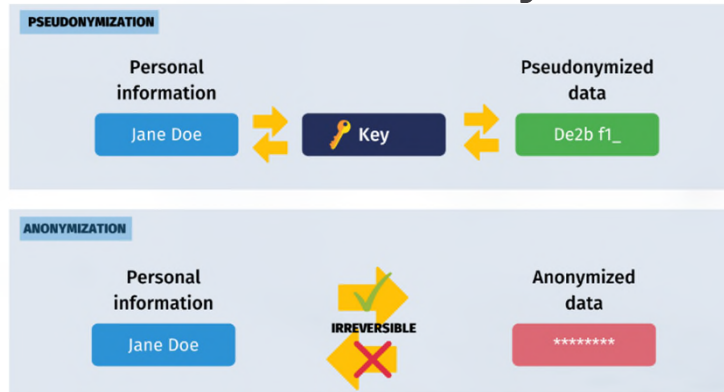
a) Course of overall sum of fines (cumulative):



- Greece's privacy authority fined facial recognition company Clearview AI fined €20 million for violating parts of Europe's General Data Protection Regulation (GDPR)
- Hungary's privacy authority fines Budapest Bank Zrt approx. €653,000 for violating GDPR by using AI with respect to audio recordings of customer service calls

Source: GDPR enforcement tracker (Aug. 17, 2022)
<https://www.enforcementtracker.com/?insights>

Algorithms Working With Pseudonymized Data Could Be Covered By GDPR





Algorithmic Bias



D.C. Attorney General introduces the “Stop Discrimination By Algorithms Act”

- On December 8, 2021, District of Columbia Attorney General Karl A. Racine introduced the “Stop Discrimination by Algorithms Act of 2021 (Act)” for consideration and enactment by the Council of the District of Columbia.
- If passed, the Act would prohibit **covered entities** from making an **algorithmic eligibility determination** or an **algorithmic information availability determination** on the basis of an individual’s or class of individuals’ actual or perceived race, color, religion, national origin, sex, gender identity or expression, sexual orientation, familial status, source of income, or disability in a manner that segregates, discriminates against, or otherwise makes **important life opportunities** unavailable to an individual or class of individuals.
- In addition, any practice that has the effect or consequence of violating the above prohibition would be deemed to be an unlawful discriminatory practice.
- The Act would apply to a broader range of industries; impose affirmative requirements, including an annual self-audit and reporting requirement; and provide enforcement authority to the Office of the Attorney General for the District of Columbia (AG).



[Source](#)

The SEC Has Also Signaled Concerns with AI Bias

- Another aspect of the use of artificial intelligence that concerns Chairman Gensler is **bias**. **Data used by platforms in their analytic models could reflect historical biases, and this could result in people not getting fair access and prices in the financial markets.**
- Chairman Gensler didn't suggest rulemaking may be the way forward in this area, but he instructed his staff to take a closer look.



U.S. SECURITIES AND
EXCHANGE COMMISSION

SEC Joins FTC in Voicing Concerns Over AI as Risk of Regulation Looms | pymnts.com

BOARD TIP:

Boards should ensure AI algorithmic testing is conducted to assess and mitigate potential biases.

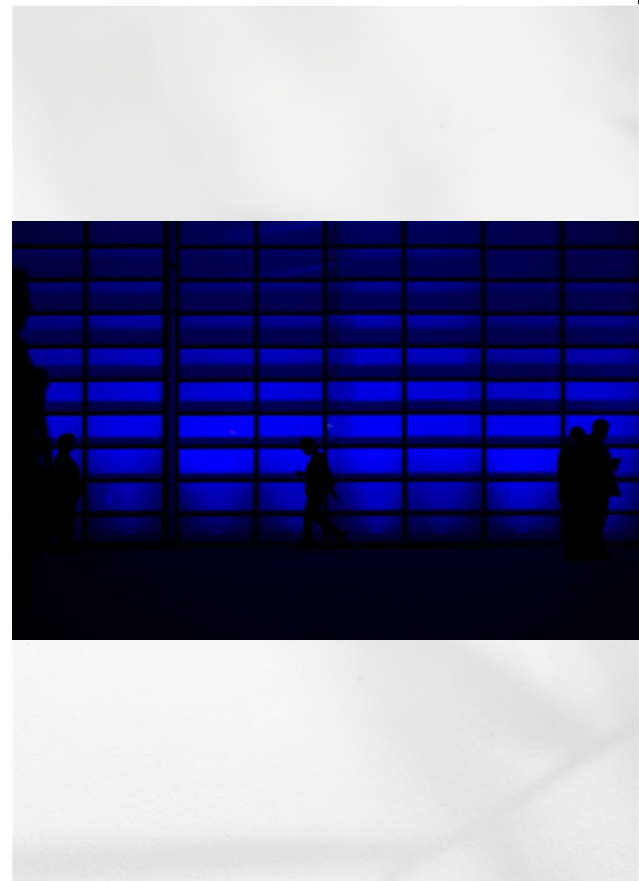
EU Digital Services Act (DSA)

- The EU AI Act will be accompanied by a Digital Services Package consisting of the Digital Markets Act (DMA) and the Digital Services Act (DSA), the latter will regulate the obligations and accountability of online intermediaries and platforms
- The DSA contains obligations for online providers regarding algorithmic transparency and accountability, for example:
 - Art. 12 (1) Providers of intermediary services shall include information on measures and tools used for the purpose of content moderation, including algorithmic decision-making in their terms and conditions
 - Art. 31 (1b) Upon request, providers of very large online platform shall explain the design, logic and functioning of their algorithmic systems, including their recommender systems, to the competent authority
 - Art. 26 • Providers of very large online platforms shall diligently identify, analyse and assess any systemic risks stemming from the design, including algorithmic systems, functioning and use made of their services in the EU
 - Art. 54 (3) The competent authorities may require the provider of very large online platforms and search engines to provide explanations on IT system, and algorithms, data-handling



AI Bias

- Machine learning bias, also known as algorithm bias or artificial intelligence bias, refers to the tendency of algorithms to reflect human biases.
- Ways AI Bias can play out:
 - Models may be trained on data from human choices or data from social or historical disparities.
 - Data may be biased by the way they are gathered or chosen for use
 - A machine learning system may potentially detect statistical connections that are considered socially inappropriate or unlawful
 - Making lender or banking decisions based on non-traditional financial data (*i.e.* social media, retail spending histories, residential stability, professional licensure)
 - Lack of diversity in AI development teams (*e.g.*, who creates the algorithms also plays a key role)



AI Bias – Algorithmic Testing

MIT researchers developed a technique that removes multiple types of bias from a mortgage lending dataset, which improves the accuracy and fairness of machine learning models that may help make fair predictions of whether borrowers receive a mortgage loan.

Using a system called DualFair, the researchers trained a machine-learning classifier that makes fair predictions of whether borrowers will receive a mortgage loan.

The researchers' technique is new in the mortgage lending domain because it can remove bias from a dataset that has multiple sensitive attributes, such as race and ethnicity, as well as several "sensitive" options for each attribute, such as Black or white, and Hispanic or Latino or non-Hispanic or Latino. Sensitive attributes and options are features that distinguish a privileged group from an underprivileged group.



Fighting discrimination in mortgage lending | MIT.edu

AI Bias – Recruiting

- Recruiting algorithms, which are typically trained using past resumes of successful candidates, can amplify bias.
- A major technology and e-commerce company used a recruiting algorithm that was trained largely on male resumes collected over a ten-year period.
- The algorithm viewed male candidates as preferable and discriminated against women.

Women's representation in the United States in ...



47%
Labor force*



24%
Technology
positions**



27%
Keynote or standalone
speakers at technology
conferences***

AI Bias – Credit Decision Making

- A male credit card user alleged he received a credit limit 20x higher than his wife despite his wife having a higher credit score.
- NY DFS examined 400,000 NY state applications to determine whether a “black box” algorithm used to make credit limit decisions violated state laws that prohibit discrimination on the basis of sex.



AI Bias – US Enforcement & Litigation

- FTC sued Social Media Platform for **failure to protect consumer privacy** and **misleading consumers** by telling them that they could opt in to using the AI algorithm when it was set on by default
 - \$5 billion settlement
- FTC sued Cloud Photo Storage App on similar grounds, where the company used the facial images it extracted for development of its facial recognition technology
 - Settlement required the company to obtain **express consent** from consumers
- **Class action lawsuits** brought by African American and LGBT content creators against an Online Video Sharing and Social Media Platform
 - Alleging that (1) the site's algorithm acts as an improper censor, and the system is rife with "digital racism" and (2) the site's algorithms discriminated by removing words commonly used in the LGBT community causing them to lose advertising revenue.



AI Bias – EU Developments

- The EU AI Act will be accompanied by a Digital Services Package consisting of the Digital Markets Act (DMA) and the Digital Services Act (DSA), the latter will regulate the obligations and accountability of online intermediaries and platforms
- The DSA contains obligations for online providers regarding algorithmic transparency and accountability, for example:
 - Art. 12 (1) Providers of intermediary services shall include information on measures and tools used for the purpose of content moderation, including algorithmic decision-making in their terms and conditions
 - Art. 31 (1b) Upon request, providers of very large online platform shall explain the design, logic and functioning of their algorithmic systems, including their recommender systems, to the competent authority
 - Art. 26 • Providers of very large online platforms shall diligently identify, analyse and assess any systemic risks stemming from the design, including algorithmic systems, functioning and use made of their services in the EU
 - Art. 54 (3) The competent authorities may require the provider of very large online platforms and search engines to provide explanations on IT system, and algorithms, data-handling





Questions?





Americas | Asia | Europe | Middle East

mayerbrown.com

Mayer Brown is a global services provider comprising associated legal practices that are separate entities, including Mayer Brown LLP (Illinois, USA), Mayer Brown International LLP (England), Mayer Brown (a Hong Kong partnership) and Tauil & Chequer Advogados (a Brazilian law partnership) (collectively the “Mayer Brown Practices”) and non-legal service providers, which provide consultancy services (the “Mayer Brown Consultancies”). The Mayer Brown Practices and Mayer Brown Consultancies are established in various jurisdictions and may be a legal person or a partnership. Details of the individual Mayer Brown Practices and Mayer Brown Consultancies can be found in the Legal Notices section of our website. “Mayer Brown” and the Mayer Brown logo are the trademarks of Mayer Brown. © Mayer Brown. All rights reserved.