Cooley

AI Talks: AI Governance & Financial Services

Michelle Rogers

Chris Chynoweth

Mike Egan

May 8, 2025

Agenda

- Overview
- Regulatory Climate
- Keys to AI Governance
  - Governance Structure
  - Risk Assessment
  - Implementation of AI Governance
  - Data Licensing and Governance

Regulatory Climate

Cooley

Federal Regulatory Climate

- Jan. 23, 2025 Executive Order
  - U.S. policy is to sustain and enhance America's global AI dominance to promote human flourishing, economic competitiveness and national security
  - Directs a review to rescind policies, directives and regulations that might be impediments to AI innovation
- Apr. 3, 2025 OMB Memo: Accelerating Federal Use of AI through Innovation, Governance and Public Trust
  - Speedy deployment
  - Investment in US-developed AI products and services
  - Training and recruitment of AI-knowledgeable employees
  - Governance structures to carry out purpose

State Regulatory Climate

- Colorado Artificial Intelligence Act—effective Feb. 1, 2026
  - Focus on AI systems making “consequential decisions,” such as those involving education, employment, financial services, housing, health care or legal services
  - Aims to protect against “algorithmic discrimination”
  - Imposes obligations on both developers and deployers of AI: documentation, disclosure, risk analysis, governance
  - Requires disclosures to consumers so consumers are aware when interacting with AI system
- Two state legislatures have enacted comprehensive laws only to see them vetoed
  - Virginia legislation regulating risk management and algorithmic discrimination
  - California legislation governing AI model providers and assigning liability
- State legislatures considering numerous bills to protect consumers from AI, although bills tend to target criminal conduct, physical harm and various frauds
  - Regulation of the use of AI in financial services will undoubtedly be a focus as states come to understand deployment

Preventing Access to US Sensitive Personal Data and Government-Related Data by Countries of Concern (including China) or Covered Persons

- Applies to transfers of “bulk sensitive personal data” belonging to U.S. persons to countries of concern or covered persons
- Prohibited:
  - Data brokerage of bulk U.S. sensitive personal data
  - Access to any covered government-related data
  - Transfers of bulk human “-omic” data
- Restricted:
  - Transactions involving vendor, employment or investment agreements with a covered person

Implications for AI and Financial Institutions

- Threshold for restricted transfers: personal financial data on over 10,000 U.S. persons
- If using an AI vendor to process sensitive data (e.g., financial data, precise geolocation data), financial institutions need to do diligence to determine if the vendor could be considered a "covered person"
  - Remember, thresholds apply regardless of whether the data is anonymized, key-coded, pseudonymized, de-identified or encrypted!

Keys to AI Governance

Cooley

Governance Structure

Intake process

Initial review of tool and use case

Committee review

Identify stakeholders

Broad SME participation

Risk assessment

Ongoing monitoring

Enterprise-wide tracking

Oversight and testing

Policies, procedures, training

Bias/UDAAP Risk Assessment

- Aspects of risk
  - Hallucination
  - Accuracy
  - Steering
  - Reliance on prohibited basis or proxy
  - Decisioning and pricing disparities
- Risk mitigant: April 23, 2025, EO indicating federal policy will shift away from disparate impact liability

Risk Assessments: Privacy

Will any personal data or NPI be fed into the model?

Does the Company have all rights and consents to use the personal data in this way?

Has the Company considered applicable laws (e.g., BIPA, CIPA, GLBA) that may impact use of the model with respect to personal data and/or automated decision-making?

Does the Company have any contractual limitations on what data it can or can't provide to a third party?

Risk Assessments: Security / Confidentiality

- Has the model provider experienced a security incident?
- Does the Company have insight into the model provider's security practices and controls?
- What threats does a model present (hacking, viruses, and malware, adversarial attacks etc.)?
- Can the model be easily manipulated into hallucinations?
- Is the model susceptible to poisoning?
- Can the model be manipulated to provide outputs with Company confidential information or other valuable information to the Company?

Implementation of AI Governance

Intake Questionnaire

- Enable employees to propose AI use cases with sufficient detail for evaluation against risk assessment and AI governance policies
- Scope of use case, proposed AI vendor(s), details on proposed inputs and outputs to AI models, estimated processing/inference costs
- Pointed questions to highlight risks or concerns

AI Vendor Due Diligence

- Security practices (NY DFS minimums, GLBA safeguards, SOC-2, NIST)
- Adverse events (infringement litigation, data breaches, consent)
- Sources of training data and model training practices
- Contractual posture (retention of data, retained training rights, confidentiality commitments, ownership of outputs)

Implementation of AI Governance

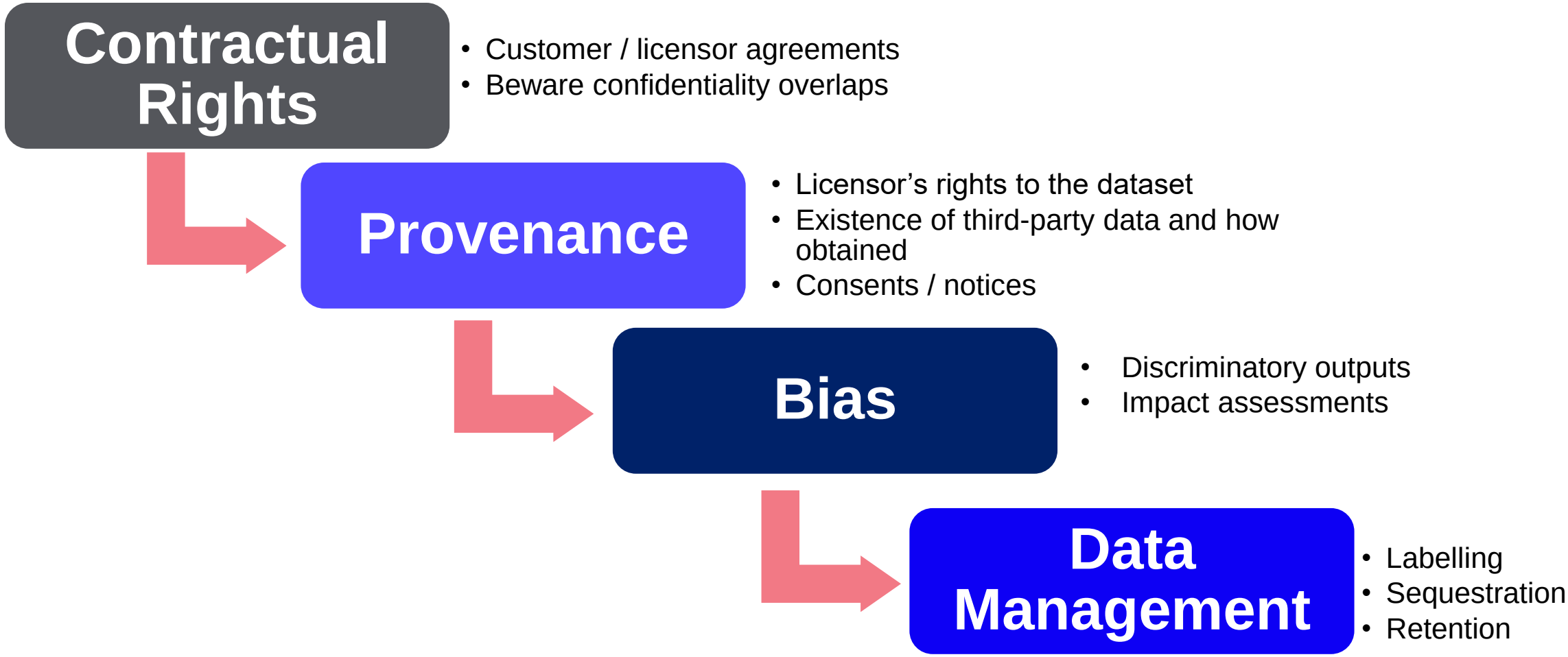
Contract Negotiation

- Diligence different contractual terms available (enterprise vs individual)
- Execute enterprise terms (including DPAs) where available
- Consider “walled garden” or “fine tuning” environments or use of own dataset
- Protection for security failures, unauthorized use of data, infringement
- Regulatory cooperation and transparency

AI Usage Policy

- Written policies (prohibited, permitted, and required activities)
- Clear compliance guidelines (e.g., opt-outs, sandboxing, etc.)
- Clear identification of governance process
- Mechanisms to ensure appropriate compliance by employees
- Risk management processes

Data Licensing and Governance



Financial Services Forecast: Five in Five Series

Register using the link in the chat.

Session 3 – May 15, 2025

Rulemaking Rundown: What's In and What's Out in Federal Financial Regulation

In this session, attendees will gain insights into navigating compliance considerations during this period of uncertainty, with practical strategies for adapting to evolving regulatory frameworks.

Session 4 – May 22, 2025

Filling the Gap! State Enforcement and Regulation Priorities

During this session we will explore issues top of mind for state attorneys general and state banking departments, including bank partnerships, payment processing, fair lending (yes, it's still a thing), and unfair and deceptive practices.

Session 5 – May 29, 2025

The 119th Congress: Investigative and Legislative Priorities

Join us for our final session, where we will provide a comprehensive analysis of the critical priorities shaping the 2025 congressional calendar and their potential impact on the financial services sector, and will share practical strategies for navigating the political risks associated with congressional investigations.

Questions?

For questions, comments, or additional information, please contact the team.

Michelle L. Rogers
Partner
mrogers@cooley.com
+1 202 776 2227

Chris Chynoweth
Special Counsel
cchynoweth@cooley.com
+1 650 843 5372

Mike Egan
Partner
megan@cooley.com
+1 202 776 2249