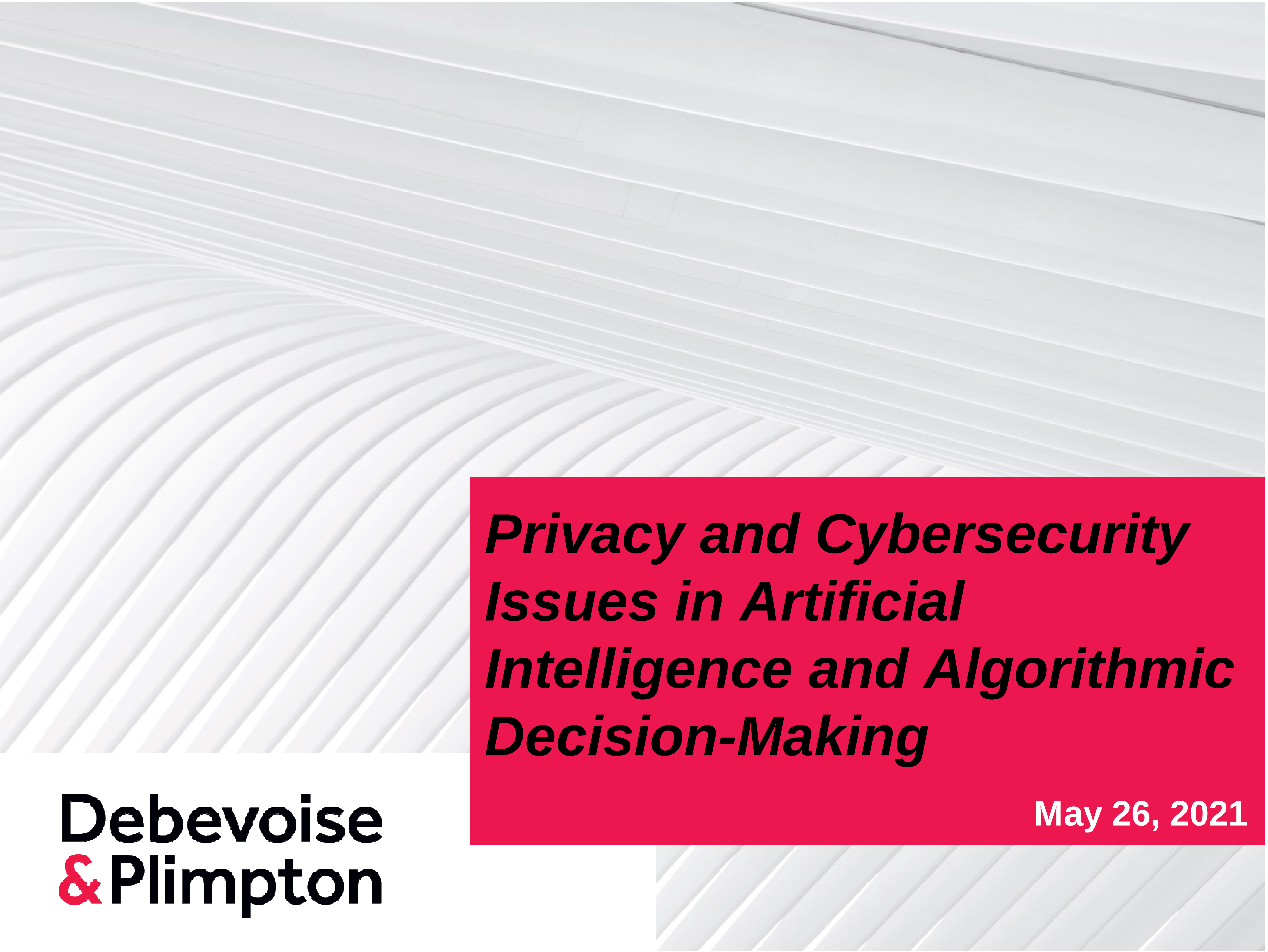

Privacy and Cybersecurity Issues in Artificial Intelligence and Algorithmic Decision-Making

May 26, 2021

Debevoise & Plimpton

Panelists

- **Avi Gesser**, Partner, Debevoise & Plimpton
- **Marina Kaganovich**, Director & Head of U.S. CIB Digital Compliance, BNP Paribas
- **Frances McLeod**, Founding Partner, Forensic Risk Alliance
- **Kaitlin Asrow**, Fintech Policy Advisor, Federal Reserve Bank of San Francisco

Overview of Topics

- AI in Use Today
- General Cybersecurity and Privacy Risks for AI
- High Risk AI
- Privacy Risks & Mitigation Strategies
- Cybersecurity Risks & Mitigations Strategies
- Challenges for AI Governance
- Recent Regulatory Guidance
- Training
- 9 Questions?

Examples of AI in Use Today

- Credit decisions – loans and credit cards
- Life / Health insurance coverage and claims
- Hiring and retention decisions
- Fraud detection
- Customer service
- Risk management/regulatory compliance (e.g. interdiction software)
- Cybersecurity
- Data and text analysis
- Biometric Identification & Monitoring

General Cybersecurity and Privacy Risks for AI

Cybersecurity

- Need to protect models, inputs, testing data, and outputs from unauthorized access by both insiders and third parties, and prevent hacking, ransomware, data poisoning, adversarial attacks, and other malicious training or use.

Data Rights

- Need to ensure that privacy obligations and other data rights have been respected for any data used for testing, validating, and operating an AI system.

Factors for Assessing High-Risk AI Use Cases

1. The AI system will involve the use of large volumes of sensitive personal information;
2. The AI system will perform important operations including with respect to key infrastructures or is critical to a core business function;
3. The failure of the AI system would endanger the company's key business lines, threaten the stability of financial markets and carry significant reputational risk.
4. The vulnerability of the AI system to compromise.

Examples of Privacy Risks Associated with AI

- Use of personal data for purposes beyond the authority
- Sharing of data with third parties without proper notices or consents
- Accuracy of personal information, especially with data from unverified and multiple sources
- Inclusion of PII in data that is supposed to be anonymized
- Skewed or non-representative data that results in bias
- Changes to low-risk use cases that makes them higher risk without revisiting privacy considerations

Mitigation Strategies against Privacy Risks

- Data discipline for what goes into data lakes, what comes out and who has access to that data.
- Anonymized/Synthetic Data
- Testing data sets for completeness and accuracy.
- Ensuring applicable disclosures and consents relating to data use
- Maintaining proper documentation of privacy measures
- Limitations on third-party and/or cross-border data sharing
- Data minimization
- Third-party vendor management
  - Risk-based approach
  - Contractual protections

Examples of Cybersecurity Risks Associated with AI

- Theft of training or the model itself
- Ransomware locking up the model
- Adverse training of the model
- Data poisoning and model tampering
- Compromise and control of the model

Mitigation Strategies against Cybersecurity Risks

- Anonymization
- Data minimization
- In-house development
- Penetration testing aimed at the model and the associate data
- Stress testing for adversarial training of AI models
- Parallel and dynamic monitoring
- Tabletop exercises
- Insurance
- Third-party vendor management
  - Risk assessment, questionnaires, testing, policies & procedures
  - Contractual (breach notification, indemnification, right to audit)

Challenges for Governance of AI

1. Who is responsible?
2. Board and senior management oversight
3. Multi-stakeholder consultation in the design, implementation, and continued oversight of high-risk AI
4. Vendor Management
5. Whether to use existing frameworks or build new ones
6. Budget and resources for AI compliance and regulatory compliance
7. Benchmarking, standards and certifications
8. Managing reputational risk
9. Understanding the evolving regulatory requirements
10. Documentation

Why Act Now? Why Not Wait for New Legislation?

1. Creating new and complicated governance structures will take time.
2. Chance to innovate and experiment with what might work for your organization.
3. Regulators are using existing regulations to investigate and bring enforcement actions
4. Don’t want AI models being built today to have to be decommissioned when new regulations come into force
5. Chance to shape the evolving regulatory framework

Existing and Evolving Regulation

1. Existing cyber and privacy laws that apply to AI
   - CCPA, GDPR, State data laws
2. European Commission’s Draft AI Legislation
   - Application to U.S. Companies
   - Banned AI Systems
   - “High Risk” AI Systems
   - Other Obligations
3. U.S. Banking Regulators Joint Request for Information on AI
4. Federal Trade Commission Guidance
5. State regulators
6. Model Risk Management Guidance

The Need for Training

- Provide training for employees who develop, approve, or use AI applications, including boards and management.
- Provide special training for certain employees relating to bias and model validation.
- These teams need to be mindful of implementing appropriate controls (including those available from cloud providers) for accessing and transferring data used to train models, especially when that data may contain PII.

Questions?

For additional thought leadership on AI-related topics, please visit:

https://www.debevoisedatablog.com/category/artificial-intelligence/