Risk Management in the Dynamic Global Regulatory Landscape for AI Products and Services

Artificial Intelligence and Data-Driven Business Models 2022
Meet Today’s Presenters

Benjamin Glatstein
Assistant General Counsel (Cloud + AI)
Microsoft

Charlyn L. Ho
Partner
Perkins Coie

Arjun Rangarajan
Sr. Counsel – SW Products (AI/ML)
Apple
Agenda for Today

Topics for Discussion

1) The Big Picture: Overview of AI Regulatory Landscape
2) Deep Dive on the EU AI Act
3) Recommendations and Best Practices
4) Questions and Concerns Going Forward
Overview of the Global Regulatory Landscape
Polling Question #1

In the U.S., where do you think primary AI regulation would come from in the immediate future?

A. New AI Legislation

B. FTC Enforcement
Regulating AI – Innovation v Safety?

• Challenge for regulators is balancing the tension between protecting the public from potential unintended harmful effects of AI while encouraging positive innovation and competitiveness

• It seems that U.S. federal government is continuing a “light-touch” approach to regulation, focusing currently on competition issues

• It will be interesting to follow US state and city regulations, some of which seem to have taken a more comprehensive approach to AI

• EU has taken a more cautious approach focused on risk and ethical principles through the EU AI Act (draft)

• Many issues are intertwined with regulatory developments relating to data privacy
Overview of the Global Regulatory Landscape

AI-Focused Regulatory Developments

- **United States Developments**
  - U.S. National Policy and Key Legislative Efforts
  - Enforcement Updates
  - State Legislative Efforts

- **International Policy Developments**
  - International Organizations Developments
  - EU Policy and Regulatory Developments
  - China Developments

- **Sector-Specific Developments**
Overview of the Global Regulatory Landscape

U.S. National Policy & Legislative Efforts

- Legislative Updates
  - Algorithmic Justice and Online Transparency Act
  - Data Protection Act of 2021
  - Consumer Safety Technology Act
  - Innovation and Competition Act
    - $200B investment over 5 years — focus areas AI, ML & autonomy

- National Security Commission on AI Final Report
  - AI can enrich the human experience, the expansion of AI usage also increases the vulnerability of US national security

- NIST Developments: two publications
  - Framework for Reducing Risk of Bias in AI
  - Identifying and Managing Bias in AI
Overview of the Global Regulatory Landscape

Enforcement in the US

• **Federal**
  • Enforcement at FTC
    • Guidance emphasizing transparency and fairness; blog post by Comm. Slaughter
  • Consumer Finance Protection Bureau (CFPB) by using the Fair Credit Reporting Act (FCRA)
  • Enforcement via the US Equal Employment Opportunity Commission (EEOC)

• **State**
  • Washington State Bill to Regulate AI (SB 5116)
    • New regulations for departments that use “automated decision systems”
  • AZ Bill HB2685
    • Provides requirements for algorithms that implement decisions without human intervention
Overview of the Global Regulatory Landscape

International Regulatory Developments

• International Organization Work on AI
  • UN Developments (UNHCR Moratorium and UNESCO Global Standard of Ethics)
  • Implementation of Organization for Economic Cooperation and Development (OECD) AI
  • World Health Organization (WHO) global report on AI: Ethics and Governance of AI for Health

• EU AI Act
  • Slovenian Compromise
  • French Compromise

• EU Council ePrivacy Regulation
  • Watch for restrictions on use of data by companies doing AI technology

• China Policy Initiatives
  • Cyberspace Administration of China (CAC) draft administrative measures on Deep Synthesis Technology
Overview of the Global Regulatory Landscape

Sector Specific Developments - I

- **Autonomous Vehicles**
  - SELF DRIVE Act HR 3711
    - Reintroduced in June 2021 to establish a U.S. federal framework
  - Iowa’s AV Legislation
  - EU Report
    - European Union Agency for Cybersecurity (ENISA) and the Joint Research Centre (JRC) issued a report concluding that a host of cybersecurity risks are present in CAVs and proposed a series of recommendations to mitigate these vulnerabilities.
  - Germany
    - German Bundestag passed a draft law designed to amend the Road Traffic Act and the Compulsory Insurance Act on Autonomous Driving

- **Financial Services**
  - Federal financial institutions (FDIC, Fed Reserve, Comptroller of Currency) and regulatory agencies collectively issued an RFI
  - New cybersecurity reporting rule
Overview of the Global Regulatory Landscape

Sector Specific Developments - II

- **Medical Devices and Healthcare**
  - FDA Action Plan for AI Medical Devices: FDA launched list of AI and ML enabled medical devices (Software as Medical Device)
  - Increase transparency and access to information on AI/ML-based SaMDs, and to act as a resource to the public regarding these devices

- **Facial Recognition**
  - Facial Recognition and Biometric Technology Moratorium Act
    - Impose limits on the use of biometric surveillance systems, such as facial recognition systems, by federal and state government entities
  - Deepfake Taskforce Act
    - Task force within the Department of Homeland Security (DHS) tasked with producing a plan to reduce the spread and impact of deepfakes, digitally manipulated images and video nearly indistinguishable from authentic footage

- Continuing U.S. State and City Developments
Deep dive – EU AI Act
Overview

- Proposed Regulation on Artificial Intelligence
- European Commission published in April 2021 after multi-year consultation process
- Still subject to proposed amendments
Overview

- **First comprehensive regulatory framework** for AI
- **Risk-based proposal** prohibiting certain ‘unacceptable risk’ systems (e.g., social scoring) and focusing regulation on ‘high-risk’ systems
- Regulation currently **focuses requirements on “provider”** of high-risk system
- **Testing requirements** to help identify and address risk
- Proposed regulation of biometric identification (facial recognition, limiting use to serious crimes and exigent circumstances)
- Very significant fines (2-6% of annual worldwide turnover)
Risk-based approach

Risk-based approach: Unacceptable risks

- Unacceptable risks are prohibited
- Example: Social scoring
- From the Commission:
  “All AI systems considered a clear threat to the safety, livelihoods and rights of people will be banned, from social scoring by governments to toys using voice assistance that encourages dangerous behaviour.”
Risk-based approach: High risk

- Examples: critical infrastructure; safety components of products; essential private / public services (e.g., credit scoring); law enforcement; administration of justice
- Permitted, but with required mitigation measures:
  - adequate risk assessment and mitigation systems;
  - high-quality datasets;
  - logging / traceability of results;
  - detailed documentation;
  - clear and adequate information to the user;
  - appropriate human oversight measures;
  - high level of robustness, security and accuracy.
EU AI Act

Risk-based approach: High risk AI systems / Risk management life cycle

1. Identify known / foreseeable risks
2. Estimate risks when used / reasonably foreseeable misuse
3. Evaluate risks based on post-sale monitoring of data
4. Adopt suitable risk mitigation measures
5. Adequate: design and development; mitigation and control measures; information and training
6. Testing to ensure compliance with requirements for intended purpose
Risk-based approach: Limited risk

- Example: Chat bots
- **Permitted**, but with transparency obligations (e.g., users need to be aware that they are engaging with an AI system)
Risk-based approach: Minimal / no risk

- Examples: video games; spam filters
- **Permitted**, with no mitigation measures:
- From the Commission: “The vast majority of AI systems currently used in the EU fall into this category.”
Recommendations and Best Practices
Governance

• **Organization Governance** - Create governance mechanism for ensuring compliance

• **System Governance** - Engage stakeholders and provide transparency

• **Risk Management** - Think about the risk categories for your services and identify the related compliance obligations
Data

- **Data Inventory** - Create an inventory of data assets and flows
- **Performance Metrics** - Define performance metrics for each component of the AI system
- **Bias** - Identify potential biases in the data that may affect how the AI performs
- **Expertise** – Consider what expertise is needed for testing the AI system and for documentation
Performance and Monitoring

- **Staying Current** - Monitor developments and changes in AI regulation
- **Performance** - Continuous and sustained oversight on performance
Questions?