DATA+AI SUMMIT
BY databricks

AI REGULATORY LANDSCAPE

June 12, 2024

Aaron Cooper: SVP, Global Policy - BSA | The Software Alliance

Scott Starbird: Chief Public Affairs Officer, Databricks

AGENDA

1) Brief overview of key AI regulations

2) Fireside chat - the evolving landscape of AI regulation, with Aaron Cooper

SVP, Global Policy - BSA | The Software Alliance
The leading enterprise software trade & advocacy organization

REMINDER:

Pre-existing laws apply to AI

- Privacy (GDPR, state laws, etc.)
- Anti-discrimination
- Consumer protection
- Criminal laws
- Copyright
- Antitrust / unfair competition

WHAT IS IN PLACE SO FAR?

EU AI Act	1ST comprehensive AI regulation with global reach
Biden Executive Order	Impacts federal use of AI; agency enforcement of existing laws; oversight of frontier models; IaaS large training run reporting
Federal Agency Actions	Under OMB guidance, agencies are implementing AI risk management programs, designating Chief AI Officers, etc.
Colorado AI Act	1st state regulation broadly focused on risky uses of AI
Various states	Narrow-focus AI bills, targeting biometrics, hiring, etc.
China & other countries	AI laws with limited global impact so far

AI REGULATION LANDSCAPE: COMMON THEMES

At all stages, protect:

- Data security
- Privacy
- IP rights

At all stages, focus on preventing:

- Algorithmic discrimination in hiring, school admissions, etc.
- Generation of harmful content

Pre-release, implement:

- Risk planning
- Modifications to mitigate risk
- Guardrails
- Documentation

Post-release, maintain:

- Guardrails
- Transparency (letting users know they are dealing with AI)

Post-release, actively:

- Monitor
- Perform risk mitigation

BIDEN EXECUTIVE ORDER ON AI

Numerous responsive actions taken by federal agencies

- Guidelines for AI use in Federal Government, Critical Infrastructure, etc.
- Implementing AI risk management programs
- Guidance for reporting by IaaS providers & frontier model developers
- Furthering research
- Designating Chief AI Officers
- Federal AI hiring spree

WHY FOCUS ON THE EU AI ACT?

- ➢ 1st comprehensive AI regulation with global impact
- ➢ Likely precedent for AI regulation elsewhere
- ➢ Pressure to pre-commit (e.g., AI Pact)
- ➢ Several leading emerging AI regulations largely lie within its framework

  (risk-based, focused on consequential decision-making, impact assessments)

However:

- It’s likely some AI regulation will go further in certain areas
- It’s important to monitor for the outliers & potential impact

EU AI ACT: RISK-BASED FRAMEWORK*

Category	Unacceptable Risk	High Risk (Focus of the Act)	Limited Risk	Minimal Risk
Description	**Manipulate or monitor behavior; certain biometric ID apps**	**Adverse impact on fundamental rights,** or **harm to health or safety**	Not high risk, but **interacts with humans**	Remainder / **no interaction with humans**
Requirements	**Prohibited** ☠	**Extensive requirements** (see later slide)	**Notice of interaction with AI** (unless reasonably apparent)	**No obligations** (but adoption of AI code of conduct encouraged)

* *The Act also regulates general purpose AI (GPAI) and frontier models regardless of use case*

WHAT IS ‘HIGH-RISK’? (& EXEMPTIONS)

Annex I Of The Act	**High-risk product already covered by specific EU legislation & the existing law requires 3rd party conformity assessment *(e.g., AI in medical devices)***
Annex III Of The Act	**Listing of high-risk categories** ***(e.g., AI used in healthcare, education, employment, critical infrastructure, law enforcement, biometrics, etc.)***
Annex III Exemptions	**If covered by Annex III, not deemed high-risk IF the AI System is intended to:** • Perform a narrow procedural task, • Improve the result of a previously completed human activity, • Detect decision-making patterns or deviations from prior patterns and is not meant to replace or influence the previous human assessment, without proper human review, **OR** • Perform a preparatory task to an assessment relevant to the use cases listed in Annex III ➢ **However, if it performs profiling of humans, always considered high-risk**

EU AI ACT – OBLIGATIONS RE: HIGH-RISK SYSTEMS

Prior to Launch

- Risk planning, identification & mitigation
- Set up risk & quality management systems
- Proper data selection, security & governance
- Technical documentation, instruction, auto logging in place
- Focus on accuracy, robustness & cybersecurity
- Design for proper human oversight

As of Launch Date

- Conduct and maintain:
  - – Conformity Assessment
  - – Fundamental Rights Impact Assessment (if impacted)
  - – GDPR Data Protection Impact Assessment (if PII present)
- Mark system with “CE” to indicate conformity with Act
- Register in EU high-risk AI system database

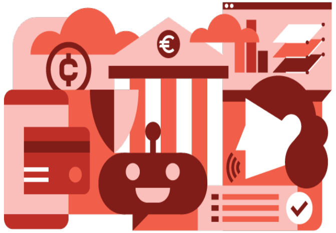
Post Launch

- Monitoring & risk mitigation
- Incident response & reporting
- Transparency & provision of information to users, including awareness AI is in use
- Apply appropriate human oversight based on risk
- Operate quality management system
- Maintain & update documentation

EU AI ACT: CONFORMITY ASSESSMENT KEY ELEMENTS

- Identification & assessment of reasonably foreseeable risks
- Description / confirmation of:
  - Risk management system
  - Testing & risk mitigation measures
  - Data sets used to train & test
  - Technical documentation
  - Reporting & auto-logging functionality
  - Human oversight & AI transparency where appropriate
  - Accuracy, robustness, cybersecurity

EU AI ACT PENALTIES



Infraction:	Penalties up to greater of* (% of global turnover OR X million Euros)
Violation of prohibition against **unacceptable systems**	7% or € 35 million
Non-compliance with AI **use obligations**	3% or € 15 million
Incomplete or faulty **information provided** to regulators	1% or € 7.5 million

** It's the "lesser of" for small and medium sized businesses (< 250 employees <u>and</u> annual turnover < €50 million)*

THE EU AI ACT - IMPLEMENTATION TIMELINE

June 2024

Entry Into Force

6 Months after entry into force

Prohibitions on Unacceptable AI go into effect

9 months after entry into force

EU AI Office must present AI Code of Practice for General Purpose AI

12 months after entry into force

Obligations on General Purpose AI go into effect

24 months after entry into force

All other provisions go into effect

(exception: provisions on AI integrated into certain products go into effect 36 months after entry into force)

AI REGULATORY COMPLIANCE ON DATABRICKS

Functionality to assist with AI compliance is available across the Data Intelligence Platform

databricks

Databricks is an optimal platform for AI regulatory compliance, with extensive functionality and expertise in:

- Data security / governance / AI security
- Model design, development, and tuning
- Model monitoring and lineage
- Data and model resting, modification and audit

To learn more, attend session today at 5:10pm:

Responsible AI on the Databricks Data Intelligence Platform

PREPARING FOR AI REGULATION

If your AI app is “high-risk” – start early

- Build into your process: risk management, planning & documentation
- Focus on data security now more than ever
- Conduct an assessment to understand how your company uses AI
- If your AI app interacts with humans, make sure either:
  - Notice is built in, OR
  - It’s obvious to a reasonable person it’s AI
- Evaluate points where a human in the loop is needed
- Work closely with your AI platform vendor

DISCUSSION WITH AARON COOPER

- SVP, Global Policy - BSA | The Software Alliance
  - The leading trade & advocacy organization for the enterprise software industry
- Background:
  - Has led BSA’s global policy team since 2015
  - Served as Chief Counsel for IP and Antitrust on the US Senate Judiciary Committee (2006-2013)
  - Clerked on the U.S. Court of Appeals for the 11th Circuit
  - Practiced at Covington & Burling for 6 years

FIRESIDE CHAT:

THE EVOLVING LANDSCAPE OF AI REGULATION