

Recent Developments in AI Policy & Governance

Presentation to CT AI WG

November 15, 2023

Chloe Autio

Independent AI Advisor

chloe@chloeautio.com

[linkedin.com/in/chloe.autio](https://www.linkedin.com/in/chloe.autio)

Agenda

1. Level Set on Policy Landscape

- A. Demystifying / ways to organize*
- B. Global – EU AI Act, UK, G7*
- C. US – AI EO*

2. Broadening the Aperture: Implications of EO & Policy Activity

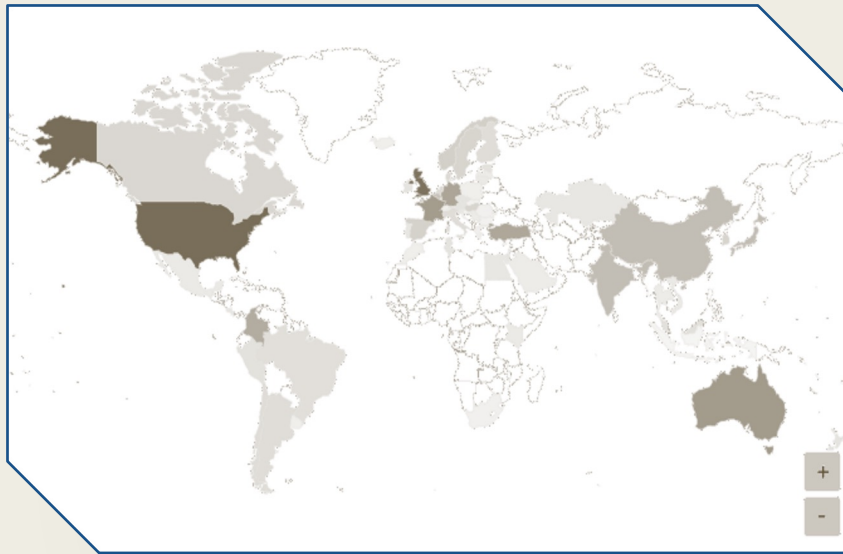
- A. For states*
- B. For industry*
- C. Key Takeaways*

3. Q&A

The AI & Data Policy landscape is increasingly complex – and maturing.

In addition to new regulatory standards, societal, corporate and market expectations all call for thoughtful engagement and communications regarding AI development and use.

Global Snapshot of Government AI Initiatives



Graphic: OECD.AI (2021), powered by EC/OECD (2021), database of national AI policies

- **Policy and regulatory initiatives**, which are shifting from Strategy & Investment to Governance of AI
- **Work in global standards bodies** (IEEE, ISO) and certification regimes are coordinating development of voluntary frameworks
- **New legal precedent:** Regulators are examining how to combat AI harms through the courts and enforcement of existing law (i.e., broad antidiscrimination and civil rights laws, sector specific privacy laws)

Global AI Policy Developments

- **UK AI Safety Summit**, creation of Institute and Bletchley Declaration among 29 countries
- **EU AI Act** – Trilogues continue, with some new additions and sticking points:
 - **Generative AI:**
 - Latest text includes a requirement for red teaming for general purpose AI systems (potentially “through vetted red-testers” from the AI Office).
 - Definitions and how to treat generative AI / foundation models (“high-impact foundation models” vs. general purpose AI)
 - Debates about enforcement i.e., how centralized it should be within EU vs. Member States
 - Negotiations will continue, with “50-50” chance the Act passes before Parliament elections in June 2024
 - After passage, AI Act will only come into force after two years.
- **G7 code of conduct** for companies, focused on risk mitigation, tracking issues and misuse, and transparency via public reporting on capabilities.

AI EO Summary

- Longest and most comprehensive EO of the Biden Admin to date
- Perhaps the most comprehensive related to tech / digital policy ever
- Activates 50 different entities, with Commerce Dept taking on many new responsibilities
 - *Establishment of AI Safety Institute at NIST*
- Over 150 new directives (actions, reports, guidance, rules, and policies) to be implemented or initiated within 30 – 365 days

LOTS of work to do!

Pre-EO, the USG was already very active on AI regulation, as are state governments and legislatures.

Congressional, federal and executive agencies, military and intelligence agencies, and state and local governments are all working to carve out their own frameworks for AI regulation.

Administration, Regulatory & Defense

- **White House OSTP** Bill of Rights and **AI Commitments**
- **NIST**-Supported initiatives
 - NAIAC
 - NAIRR
 - AI RMF
- **Agency-specific** activities and rulemaking
 - EEOC – Algorithmic Fairness Initiative; Guidance on ADA Compliance
 - CFPB – Report and guidance on ECOA compliance when using black box models
 - HHS – Trustworthy AI Playbook
 - FTC – Report on AI for online harms; rulings on data disgorgement; warnings RE behavioral advertising
 - NTIA RFCs on Privacy, Equity & Civil Rights AND AI Assurance
- Joint statement from **DOJ, CFPB, EEOC** on Enforcement Efforts Against Discrimination and Bias in Automated Systems



Congressional

- **AI-specific legislation** (NO FAKES Act, Algorithmic Accountability Act, licensing bill)
- **Privacy and Competition legislation** with AI provisions
 - Section 207 of the ADPPA
 - Provisions in CHIPS and Science



State & Local

- **NYC** AI Hiring law, **CO** big data insurance law
- **IL** Biometric Protection Law
- **CT** AI work & cross-state collaborations
- **CA** AB 331 and SB 294
- **DC** Stop Discrimination by Algorithms Act
- **State privacy laws** with AI provisions
- **DOD** RAI Initiatives – Principles, Just-released toolkit.



Breaking it Down: Six Core Categories

National Security

- Reporting (of foundation model development and of Cloud customer use)
- Protections against AI-enabled bio engineering
- National Security Memo

Privacy, Consumer Protection, IP

- **Research, evaluation and uptake of PETs (NSF)**
- **Evaluation of how agencies buy and use commercially available data (i.e. from data brokers)**
- HHS to develop responsible AI in drug discovery and create reporting mechanism unsafe AI in healthcare
- **USPTO guidance on AI inventorship and proposed actions from copyright office**

Equity & Nondiscrimination

- DOJ to coordinate enforcement and guidelines RE AI discrimination
- Develop best practices for AI used in criminal justice system (DOJ, DHS, OSTP)
- Agency civil rights and liberties offices consulted RE AI use
- Guidance from FHFA, CFPB on loan and tenant screening
- Guidance on AI use in benefits administration, including human review and redress

Labor and Worker Rights

- **DOL to issue guidance RE AI use in hiring for federal contractors**
- Report on labor market effects of AI (CEA)
- Assess viability of safety nets and consult with unions (DOL)
- Guidance to ensure AI augmented or tracked work is compensated fairly (DOL)

Security of AI Systems

- NIST AI Safety Institute, **developing test beds and standards for red teaming**
- DHS AI Safety & Security Board (DHS) to apply standards to critical infrastructure & evaluate other risks
- Standards for **authenticating AI-generated content**
- Defining **open source risks (NTIA)**

Bolstering AI in USG

- **Immigration provisions**
- Boost hiring of AI talent via fellowships and new hiring authorities
- Provide AI training to public servants
- NAIRR Pilot
- **Responsible Use via OMB guidance**
 - Agencies to appoint chief AI officer, AI review board
 - Implement risk management protocols and procurement guidance

Implications and Engagement Points for States

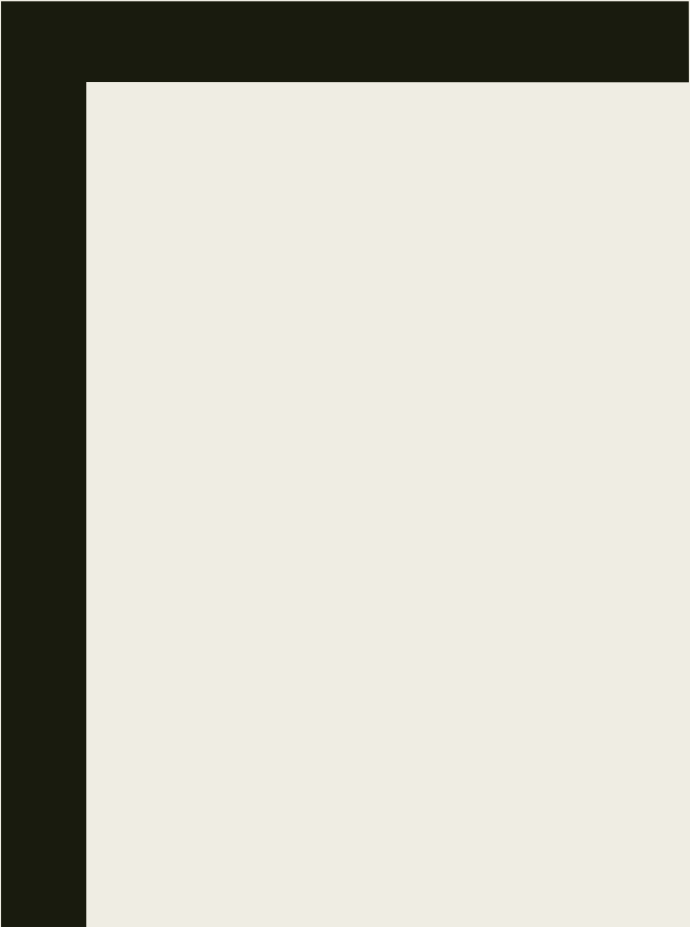
- **Draft OMB Guidance:** Organizational structure and processes for AI governance
 - *AI Officers and councils, minimum risk management processes*
- **Investment and Innovation:** Coordination with Regional Innovation Cluster program funding to establish Small Business AI Innovation and Commercialization Institutes via Commerce Dept
- **Review, guidance and technical assistance from DOJ on use of AI in criminal justice settings**
 - *Also training and guidance for AI use by law enforcement professionals*
- **Guidance for State / local benefits administration:** HHS guidance and coordination to address use of automated or algorithmic systems, and mechanisms for human oversight, redress, audits (Sec 7.2)
 - *Also examining AI use for benefits with Dept of Agriculture, DOT*

[Top of Mind] Implications for Industry

- **Reporting requirements** for entities developing “**dual use foundation models**” which meet computing threshold or are used for use cases with biosecurity implications: results of red team testing (including discriminatory outputs)
- **Compute monitoring and reporting** for **cloud service providers** to share information about compute used by foreign entities that could enable malicious cyber activity
- **Procurement considerations** for organizations contracting with the federal government regarding risk management of AI systems (auditability, documentation, accountability)
- **Civil rights** and **nondiscrimination enforcement warnings**, particularly for employers

Key Takeaways

- #1: Regulation has moved from abstractions around high level principles to more tangible/actionable guidelines or third party access (via things like red teaming).**
- #2: However, proposals are not self-executing and often present unclear and differing requirements for fairness, transparency, safety and accountability.**
- Framing for transparency or accountability is probably the easiest and most effective way to regulate, via required disclosures like process documentation and risk assessments for select use cases, or the mandated allocation of resources towards governance activities.
- #3: Focus on generative AI and existential / future risks has pulled focus from traditional GRC approaches to AI.**
- Discussions about AI safety and model governance are distinct from governing AI use cases and data on a more practical and tangible level. Non-advanced / “traditional” AI can create risks which should be managed today.
- #4: Leading industrialized nations (UK, EU, US) are competing to demonstrate who is the leader in AI regulation.**
- Companies using AI are working to balance requests and prioritize time / initiatives with geopolitical considerations top of mind.
- #5: Industry self-regulation has a role to play beyond technical compliance, but it won't be a complete solution.**
- Risk assessments – which are context and sector specific – need to be worked out in context of regulator with sector jurisdiction.
 - These technologies are constantly evolving – need standards that can be flexible and adapt to technological change. Setting standards around performance or other metrics will become mostly irrelevant (as we have seen with generative AI).



Thank you!
Questions