NO PREP

The EU AI Act, U.S. Executive Orders

How Governments Are Responding

Includes: Student reading, case study, differentiated questions, teacher key



Name: Period: Date:

The EU AI Act, U.S. Executive Orders: How Governments Are Responding

The Governance Gap

When a new technology emerges, there is typically a gap between the technology's capabilities and the legal

Name: **Period:** **Date:**

The EU AI Act, U.S. Executive Orders: How Governments Are Responding

The Governance Gap

When a new technology emerges, there is typically a gap between the technology's capabilities and the legal frameworks designed to govern it. Automobiles were invented before speed limits, seatbelt requirements, or drunk driving laws. Social media existed for over a decade before meaningful privacy legislation began to catch up. Artificial intelligence is now at the center of a similar governance gap, but the stakes are arguably higher, the technology is moving faster, and the international dimension is more complex than almost any previous regulatory challenge. The fundamental difficulty is that AI is not a single technology but an enormous category of technologies with vastly different capabilities, risks, and applications. Regulating AI requires governments to make decisions about which applications pose enough risk to require oversight, how to balance innovation with safety, who should be responsible when AI systems cause harm, and how to maintain regulatory coherence in a global technology landscape where rules in one country have limited effect on development in another.

The European Union's Approach: The AI Act

The European Union moved earliest and most comprehensively to regulate artificial intelligence. The EU AI Act, passed in 2024 and entering full force in phases through 2025 and 2026, is the world's first comprehensive legal framework for AI governance. Its central organizing principle is a risk-based tier system that classifies AI applications by the level of risk they pose and applies proportionally stricter requirements to higher-risk uses. The act establishes four risk tiers. At the top are prohibited applications: AI uses that pose unacceptable risks to

fundamental rights, including real-time biometric surveillance in public spaces, social scoring systems (AI systems that rate citizens and restrict their rights based on behavior), and manipulative AI that exploits psychological vulnerabilities. In the second tier are high-risk applications that are permitted but heavily regulated, including AI used in hiring decisions, credit scoring, medical devices, critical infrastructure, and law enforcement. In the third tier are limited-risk systems requiring disclosure. For example, chatbots must inform users they are interacting with AI. The fourth tier covers minimal-risk applications with no specific requirements. The enforcement mechanism is significant: non-compliance can trigger fines of up to 35 million euros or 7% of a company's global annual revenue, whichever is larger. For major technology companies, this represents a genuinely consequential penalty. The EU has also established an AI Office, a new regulatory body specifically responsible for overseeing compliance with the Act.

The United States Approach: Executive Action and Fragmentation

The United States has taken a markedly different approach. Rather than comprehensive legislation, the U.S. federal response has been primarily through executive orders, directives from the President that don't require congressional approval but are also more easily reversed by a subsequent administration. President Biden's Executive Order on Safe, Secure, and Trustworthy AI, issued in October 2023, was the most significant federal action: it directed federal agencies to develop AI standards, required companies developing the most powerful AI models to share safety test results with the government, and established voluntary commitments from major AI developers on safety practices. The Biden executive order was substantially revised by the Trump administration in early 2025, reflecting different priorities around innovation versus regulation. This instability underscores a fundamental weakness of the executive order approach: AI governance through presidential directive is subject to reversal with each administration change, making it difficult for companies to plan long-term or for the public to rely on consistent protections. In the absence of comprehensive federal legislation, individual U.S. states have moved to fill the gap. California, New York, Illinois, and Texas have all passed AI-related legislation covering areas including facial recognition, employment discrimination, and consumer disclosure requirements.

This has created a patchwork of state-level rules that apply differently depending on where a company operates or a consumer lives.

International Cooperation and Competition

AI regulation is complicated by the international dimension in ways that domestic consumer protection law never was. A country can regulate what AI companies do within its borders, but it has limited power over AI systems developed and operated elsewhere. The EU AI Act applies to AI systems used within the EU regardless of where they were developed — a principle called extraterritorial jurisdiction that has created significant compliance complexity for global technology companies. At the same time, governments are acutely aware that overly burdensome regulation could cause AI development to move to less-regulated jurisdictions, potentially resulting in less safe AI while also disadvantaging their own economies. The tension between maintaining safety standards and remaining competitive in a global AI race is a central challenge for every major government attempting to regulate this technology. The G7 countries (United States, United Kingdom, Canada, France, Germany, Italy, Japan) plus the EU have established the 'Hiroshima AI Process,' a framework for coordinating AI governance principles internationally. But coordination remains voluntary and the principles are high-level, leaving significant variation in how different governments actually implement AI oversight. Regulatory sandboxes — controlled environments where companies can test AI systems under regulatory supervision before full deployment — have emerged as a tool for balancing innovation with safety requirements. The EU AI Act establishes provisions for regulatory sandboxes, allowing companies to develop innovative AI applications with regulatory guidance rather than having to navigate uncertainty about compliance requirements. Several EU member states have launched national AI regulatory sandboxes, and the concept has been adopted in modified forms by regulators in the United Kingdom, Singapore, and several other countries. Civil society organizations have played an important role in shaping AI governance frameworks in both the EU and the United States. Groups including the Electronic Frontier Foundation, AlgorithmWatch, the AI Now Institute, and Access Now have documented harms from unregulated AI, proposed regulatory frameworks, and advocated for stronger enforcement of existing protections. Their input into legislative processes has been credited with strengthening several provisions of the

EU AI Act, particularly around facial recognition and employment AI. The involvement of civil society in AI governance represents an attempt to ensure that regulation reflects the interests of affected communities rather than only the interests of technology companies and governments. The EU AI Act's extraterritorial reach has created significant compliance challenges for global technology companies. A company headquartered in California that sells AI-powered services to European customers must comply with the Act's requirements regardless of where the AI was developed or where the company is based. This has driven significant investment in compliance infrastructure at major AI companies, including dedicated EU compliance teams, technical modifications to AI systems to meet the Act's requirements, and in some cases decisions not to offer certain AI services in the EU market at all.

Key Information: AI Governance Frameworks

Detail	Information
EU AI Act status	Passed 2024; full implementation through 2025-2026
EU organizing principle	Risk-based tier system: prohibited, high-risk, limited-risk, minimal-risk
EU prohibited AI uses	Real-time public biometric surveillance, social scoring, psychological manipulation
EU maximum fine	35 million euros or 7% of global annual revenue (whichever is larger)
U.S. federal approach	Executive orders (reversible) rather than comprehensive legislation
Biden AI Executive Order	October 2023 — safety testing requirements, agency standards, voluntary company commitments
U.S. state fragmentation	California, New York, Illinois, Texas all have separate AI laws
Hiroshima AI Process	G7 + EU voluntary framework for international AI governance coordination

Case Study: The Hiring Algorithm Under Review

TechCorp Europe uses an AI system to screen job applications. The system analyzes resumes and ranks candidates based on patterns in historical hiring data. When the EU AI Act's high-risk application requirements take effect, TechCorp discovers its hiring AI falls in the second tier — high-risk — because it makes consequential decisions about employment. This means TechCorp must document the system's design, conduct bias audits, register the system in an EU database, and allow human review of automated decisions. The process is expensive and time-consuming. But during the bias audit, TechCorp's compliance team discovers that the AI has been systematically ranking candidates from certain universities lower — not based on qualifications but based on a correlation in old hiring data. The system was perpetuating a bias that nobody had noticed because it was embedded in the algorithm. The EU Act's compliance requirements, which seemed like bureaucratic overhead, turned out to identify a real problem.

1. What unintended benefit did the EU AI Act's compliance requirements produce for TechCorp, and what does this suggest about the purpose of high-risk AI oversight?

2. How does this case illustrate the tension between the cost of AI regulation and its potential value?

Multiple Choice

1. What is the central organizing principle of the EU AI Act?

a) A risk-based tier system that applies proportional requirements to different AI applications

b) Requiring all AI companies to be headquartered within the European Union and its member states

c) A blanket ban on all AI use in public spaces as a comprehensive prohibition of this technology

d) Voluntary industry commitments supervised by the European Commission without legal authority

2. What is the primary weakness of the U.S. executive order approach to AI governance compared to legislation?

a) Executive orders cannot cover technology companies based outside the United States internationally

b) Executive orders are easily reversed by a subsequent administration, making governance unstable

c) Executive orders cannot impose financial penalties on non-compliant companies in most situations

d) Executive orders require a two-thirds majority in Congress before taking effect

3. Which of the following is an EXAMPLE of an AI application in the EU's prohibited tier?

a) A chatbot that must disclose it is not a human to users during chat

b) An AI medical device used for diagnostics in a hospital setting

c) A real-time facial recognition system in a public shopping mall

d) An AI system that screens job applications for employment purposes

Matching

Write the letter of the correct definition on the line next to each term.

Term	Definition
1. ___ Risk-based tier system	A) A law's application to companies or systems outside the regulating country's borders
2. ___ Extraterritorial jurisdiction	B) AI systems that rate citizens and restrict their rights based on behavior — prohibited under the EU AI Act
3. ___ Social scoring	C) EU AI Act framework classifying applications by risk level with proportional regulatory requirements
4. ___ Hiroshima AI Process	D) The period when a new technology's capabilities exceed existing legal frameworks designed to govern it
5. ___ Governance gap	E) G7 + EU voluntary framework for coordinating international AI governance principles

Fill-in-the-Blank

1. The EU AI Act can fine non-compliant companies up to 7% of their global annual _____ or 35 million euros, whichever is larger.

2. The Biden administration's Executive Order on AI was issued in _____ 2023 and directed agencies to develop AI safety standards.

3. Because the United States lacks comprehensive federal AI legislation, individual _____ have passed their own AI rules, creating a fragmented patchwork.

Short Answer

Answer each question in 2-4 complete sentences.

1. Explain why the EU AI Act's risk-based tier system is considered a more sophisticated approach than either banning all AI or allowing completely unregulated AI development.

2. What is the tension between innovation and regulation in global AI governance, and how does extraterritorial jurisdiction attempt to address it?

3. Do you think the U.S. should pass comprehensive AI legislation similar to the EU AI Act, or is the executive order / state-level approach sufficient? Defend your position.