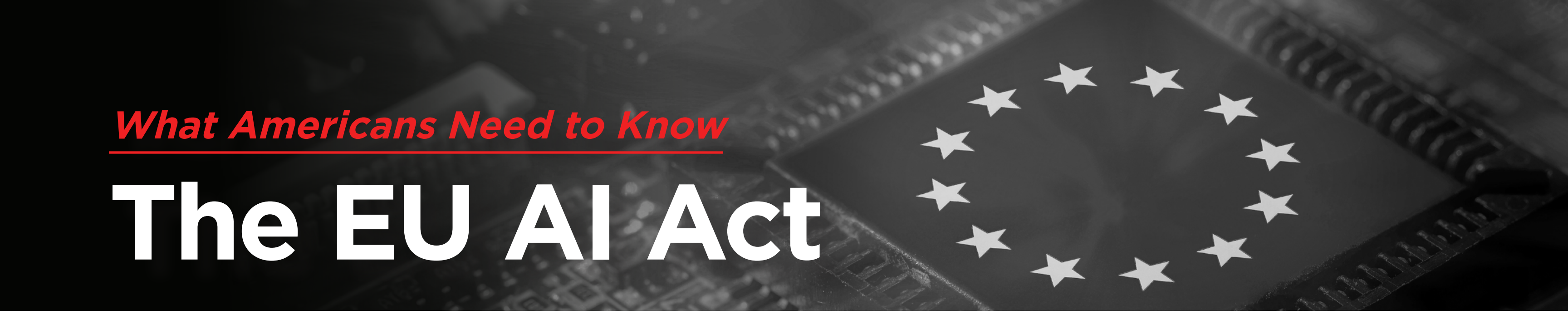

What Americans Need to Know

The EU AI Act

By Jack McPherrin

The European Union's Artificial Intelligence Act (AI Act) is the world's first comprehensive law governing artificial intelligence.[1] While framed as a consumer-safety measure, the Act's broad reach and extraterritorial design give European regulators authority over how AI is built and used worldwide, including by American companies.

This document answers key questions about the AI Act's scope, enforcement, and implications for U.S. sovereignty, free expression, innovation, and competitiveness. It is designed to help lawmakers and the general public quickly understand what the law does, why it matters, and what steps the United States can take in response.

1. What is the European Union's Artificial Intelligence Act?

The AI Act is a sweeping regulatory framework that governs the development, deployment, and use of artificial intelligence in the European Union. Enacted in 2024, it purports to promote "trustworthy" and "ethical" AI by imposing a risk-based set of rules on AI systems and the companies that build and use them.

In practice, the Act goes well beyond product safety. By asserting jurisdiction over any AI system whose outputs are "used in the Union," it allows European regulators to influence how AI is designed and operated worldwide, including in the United States. The Act's expansive definitions of risk and "fundamental rights" give Brussels broad discretion to decide which applications of AI are acceptable, which are "manipulative" or "exploitative," and which must be banned outright—decisions that can indirectly reshape American technologies and speech norms despite never passing through U.S. democratic processes.

2. Who and what does the AI Act apply to?

The AI Act applies not only to European entities but to any provider, deployer, importer, distributor, manufacturer, or authorized representative whose AI systems are placed on the EU market or whose outputs are used within the Union. It also covers "affected persons" located in the European Union.

This extraterritorial design means the law reaches American firms whose models or tools are accessed by European users, integrated into European products, or generate outputs consumed in Europe, even if the company has no physical presence in the EU and does not specifically target EU customers. In effect, Brussels uses access to its single market to export its standards globally, pulling non-European firms into its regulatory orbit whenever their systems are "used in the Union."

[1] This FAQ is a condensed version of a comprehensive *Policy Study* published by The Heartland Institute in November 2025. All information in this document is fully cited within the *Policy Study*. See: Jack McPherrin, "The European Union's Artificial Intelligence Act: An Extraterritorial Incursion on Americans' Inalienable Rights," *Policy Study*, The Heartland Institute, November 11, 2025, https://heartland.org/publications/the-european-unions-artificial-intelligence-act-an-extraterritorial-incursion-on-americans-inalienable-rights/

THE HEARTLAND INSTITUTE

3. How does the EU classify and regulate AI systems?

At the core of the AI Act is a tiered, risk-based framework. Systems deemed to present “unacceptable risk” are prohibited outright. These include tools that deploy manipulative techniques to distort behavior, exploit vulnerabilities, conduct social scoring, perform predictive policing based solely on profiling, scrape images to build large facial-recognition databases, infer emotions at work or in schools, or use biometric categorization to deduce sensitive traits such as race, political opinions, or sexual orientation (subject to narrow exceptions).

“High-risk” systems are not banned but are subject to stringent requirements. They include AI used as safety components in regulated products (such as medical devices or vehicles) and systems deployed in sensitive domains listed in Annex III, including biometrics, critical infrastructure, education, employment, access to essential services, law enforcement, migration and border control, and the administration of justice and democratic processes.

A third group of “limited-risk” systems face transparency obligations only, including disclosure that users are interacting with AI or viewing synthetic media. Remaining “minimal-risk” systems are effectively unregulated but encouraged to follow voluntary codes of conduct.

Finally, a separate cross-cutting regime governs general-purpose AI (GPAI) models, including large language models that can underpin any of these risk tiers.

4. What are the main obligations for companies under the Act?

The Act’s most consequential provisions and effects encompass the high-risk regime and the GPAI framework. Before a high-risk system can be placed on the EU market or used in the Union, it must satisfy baseline requirements for risk management, data governance, technical documentation, record-keeping, instructions for use, human oversight, accuracy, robustness, and cybersecurity.

Obligations are distributed across the AI value chain. Providers (who place the system on the market under their name) must conduct a conformity assessment, issue an EU “declaration of conformity,” and apply the CE mark, which functions as the system’s passport into the European Union. They must then monitor performance, correct problems, mitigate bias, and report serious incidents. Importers and distributors act as gatekeepers, verifying that CE-marked systems are compliant and suspending distribution if they detect non-compliance. Deployers—the banks, hospitals, schools, agencies, or firms that use the system—must follow the provider’s instructions, ensure human oversight, retain logs, and check key input data. In certain high-risk contexts, especially for public bodies or providers of public-facing services, deployers must also conduct a Fundamental Rights Impact Assessment before deployment.

GPAI providers face baseline duties to prepare technical documentation, inform downstream developers, adopt EU-compliant copyright policies, and publish a “sufficiently detailed” summary of training-data sources. Models designated as posing “systemic risk” must go further, performing standardized evaluations and adversarial testing, continuously assessing and mitigating risks, reporting serious incidents, and demonstrating compliance via standards or interim codes of practice.

5. How is the AI Act enforced, and what penalties can companies face for non-compliance?

Enforcement is split between national and EU-level authorities. Each member state must designate “national competent authorities,” including a notifying authority and a market-surveillance authority that are responsible for monitoring compliance, investigating violations, and maintaining an EU-wide database in which providers of high-risk systems must register their products. At the supranational level, the European Commission’s new EU AI Office oversees GPAI models, especially those deemed to pose systemic risk, and can request documentation, evaluate models directly, and coordinate enforcement across the Union.

The Act introduces substantial turnover-based fines. Prohibited AI practices can be punished with fines of up to €35 million or 7 percent of global annual turnover, whichever is higher. Violations of obligations for high-risk systems and GPAI can draw fines of up to €15 million or 3 percent of global turnover, while supplying incorrect, incomplete, or misleading information to regulators can be penalized up to €7.5 million or 1 percent of global turnover. Small and medium-sized entities (SMEs) face the same regime, but the lower total is assessed instead of the higher total.

Authorities may also order corrective actions, restrict or withdraw non-compliant systems, and impose disclosure requirements, which can be as burdensome as the fines themselves.

6. How does the AI Act extend European control beyond Europe’s borders—including over American companies?

The AI Act follows a well-established pattern of EU regulatory extraterritoriality often described as the “Brussels Effect.” Rather than regulating only European firms and activities inside the EU, the Act’s jurisdictional trigger is “use in the Union,” not corporate domicile. Any company whose AI outputs are used within the EU—whether it has a European presence or not—can be investigated, fined, or compelled to take remedial action.

Because penalties are pegged to global turnover and obligations are distributed across the value chain, global providers have strong incentives to align their products with the strictest plausible EU interpretation and then apply those constraints worldwide. Maintaining separate “EU” and “U.S.” versions of systems is costly and difficult to keep perfectly separate; one misrouted user or reseller can trigger EU exposure. As a result, many firms will standardize their design choices, content policies, and contracts to EU norms across all markets. In practice, this shifts key decisions—about what AI may generate, when persuasion becomes manipulation, and which inferences are “unacceptable”—from American institutions to European regulators and notified bodies, even when the systems are primarily used in the United States.

> Global providers have strong incentives to align their products with the strictest plausible EU interpretation and then apply those constraints worldwide.

7. How could the law affect free expression, innovation, and competition?

The AI Act effectively regulates speech by proxy. Providers and deployers are expected to prevent or mitigate outputs deemed "manipulative," "exploitative," or "biased," and can be held responsible even for user-generated content. Facing coordinated oversight and revenue-linked penalties, global platforms have strong incentives to calibrate their models and moderation systems to the most conservative European interpretation. Over time, this can narrow the range of permissible expression in AI-mediated communication—political commentary, journalism, art, education, humor, and everyday conversation—by discouraging controversial, value-laden, or unconventional ideas that could be alleged to distort behavior, exploit vulnerabilities, or perpetuate discrimination.

On the economic side, the Act's complexity and ongoing compliance burdens advantage the largest, best-connected firms with the resources to build dedicated departments for documentation, risk management, and conformity assessments. Startups and open research projects are more likely to delay releases, block European users, or abandon certain products entirely. Compliance costs therefore entrench incumbents, reduce competition, and slow innovation, shifting the AI ecosystem toward a more centralized, permission-based model shaped by bureaucratic politics rather than open experimentation and market entry.

> Providers and deployers are expected to prevent or mitigate outputs deemed "manipulative," "exploitative," or "biased," and can be held responsible even for user-generated content.

8. How might the AI Act's provisions affect Americans in practice?

In practice, the AI Act's extraterritorial reach and risk-mitigation duties can lead providers to implement global content restrictions and design choices that directly affect Americans' access to information and tools. One scenario could involve the climate and energy policy spectrum. After the Act takes effect, EU guidance could treat certain sustainability-related outputs as manipulation or exploitation, particularly when AI models influence consumption or investment decisions. To reduce regulatory exposure, providers may retrain systems to block or heavily qualify responses that question net-zero feasibility or renewable-energy mandates, effectively filtering what American policymakers, journalists, and citizens see on these topics, even though such views are fully protected under U.S. law.

Another scenario involves political-speech tools. A U.S. startup offering an AI writing assistant for political messaging could be classified as "high-risk" because its outputs may influence electoral outcomes in Europe. To satisfy high-risk obligations and avoid EU penalties, the company might impose global restrictions on election-related content and adjust contracts to prohibit political advocacy. These requirements would apply regardless of whether the users are in Europe or the United States, limiting how American campaigns, publishers, and nonprofits can use the technology. In both cases, European rules indirectly shape what Americans can say and hear through AI systems.

9. When do the law's key provisions take effect?

Although the AI Act entered into force on August 1, 2024, its obligations roll out in stages. Some provisions have already taken effect. Six months after entry into force, on February 2, 2025, the EU activated its ban on "unacceptable-risk" systems, including manipulative applications, social-scoring tools, and certain biometric-surveillance uses. One year after entry into force, on August 2, 2025, obligations for GPAI systems and related governance provisions began to apply and penalties for violating the prohibited practices ban became enforceable.

Two years after entry into force, on August 2, 2026, obligations and penalties for most Annex III high-risk systems—covering areas such as hiring, credit, education, health care, law enforcement, migration, critical infrastructure, and democratic processes—will take effect, as will penalties for non-compliant GPAI providers. By August 2, 2027, remaining high-risk systems used as safety components in regulated products, and all GPAI models placed on the market before August 2025, must be brought into full compliance. By 2026–2027, nearly every significant AI system operating in or affecting Europe will fall within the law's regulatory orbit.

10. What should the United States do in response?

The United States should respond on three main fronts. First, through trade negotiations and related instruments, the White House and Congress should make clear that the United States will not accept the extraterritorial application of EU law to American citizens, firms, or products.

Second, Congress should adopt federal legislation that prohibits foreign regulatory enforcement against U.S. entities operating solely within domestic borders and preempts state or corporate cooperation with such enforcement.

Third, states should follow Texas' lead by enacting laws that protect constitutional rights while setting narrow, clearly defined guardrails against genuinely harmful AI practices. Broad state-level adoption of such measures would help establish a coherent federal framework rooted in American principles of liberty, innovation, and accountability. Taken together, these steps would reassert American sovereignty in the digital sphere and ensure that AI governance reflects free expression, competitive enterprise, and democratic oversight rather than bureaucratic mandates from Brussels.

> Taken together, these steps would reassert American sovereignty in the digital sphere and ensure that AI governance reflects free expression, competitive enterprise, and democratic oversight rather than bureaucratic mandates from Brussels.