BIPSS Commentary
www.bipss.org.bd September-2025
BIPSS Towards a Secure World

AI Rivalries: Contesting U.S. and Chinese Approaches to Artificial Intelligence Regulation

Mohosina Mostofa Mity[1]

Introduction

Unlike earlier technology races—such as the space race of the Cold War—the AI rivalry is less about spectacle and more about subtle yet profound control. The debate is no longer confined to who builds the most advanced algorithms or trains the largest language models. Instead, it revolves around who gets to shape the rules of the game: who sets the standards, defines responsible use, protects—or exploits—data, and ultimately determines how AI aligns with human values. In this sense, AI regulation is emerging as the new battleground where national interests, security imperatives, and ideological differences converge.

Source: An Article by the Yale Law School

[1]Mohosina Mostofa Mity is a Research Associate at the Bangladesh Institute of Peace and Security Studies (BIPSS). She completed her BSS & MSS in International Relations from the Bangladesh University of Professionals (BUP).

For the United States, the approach to AI regulation has been guided by a mixture of democratic values, market-driven innovation, and a strong concern over security risks. Washington has sought to balance encouraging innovation with preventing misuse—whether in surveillance, disinformation, or autonomous weaponry. Yet, in an age where private corporations often move faster than governments, U.S. regulatory efforts face the constant challenge of catching up with Silicon Valley's speed.

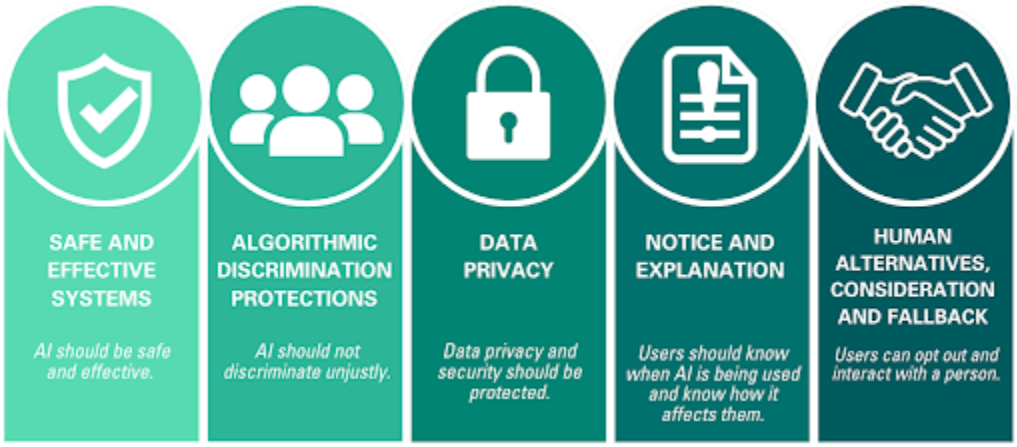
China, by contrast, views AI through the prism of state authority, societal control, and strategic dominance. Its regulatory approach emphasizes central oversight, data sovereignty, and alignment with broader national goals. Beijing sees AI not only as a tool for global competitiveness but also as a means to strengthen governance at home. Its policies reflect a model where regulation is intertwined with political control, offering both efficiency and concerns about repression.

At present, these rival approaches are no longer confined within national borders. They ripple outward, influencing international organizations, shaping global standards, and compelling smaller states to navigate a world where choosing between Washington's open-market vision and Beijing's state-centric model may define their digital futures.

AI Regulation as a Reflection of Political Systems

The United States operates within a liberal democratic system where regulation tends to emerge through open debate, institutional checks and balances, and a strong reliance on private sector innovation. This results in a patchwork style of governance, where different agencies and stakeholders—ranging from Congress and the White House to technology companies and civil society groups—play significant roles in shaping the rules. For instance, the Blueprint for an AI Bill of Rights introduced in 2022 by the White House emphasized protecting citizens from algorithmic discrimination, ensuring transparency in automated decision-making, and defending privacy rights.[2] The framework reflected core democratic principles, such as individual freedoms and accountability, even though it was non-binding and left much to the interpretation of companies and regulators.

[2]The White House. 2023. "Blueprint for an AI Bill of Rights | OSTP | the White House." The White House. November 22, 2023. https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/.



Source: US AI Act

China, on the other hand, is governed by a centralized, authoritarian political system where the state holds primacy over both markets and civil society. This allows Beijing to impose uniform regulations across industries swiftly and with little opposition. Its regulatory approach is rooted in a belief that AI should serve national priorities, strengthen social governance, and enhance state security. For example, China's Generative AI Regulation (2023) required companies deploying AI tools to align outputs with "socialist values" and prohibited content deemed politically sensitive.[3] Unlike the U.S. model, where citizens and advocacy groups push for rights-based safeguards, China's framework prioritizes political stability and control, embedding censorship and surveillance into the fabric of regulation.

A striking example of these contrasting philosophies can be seen in the regulation of generative AI platforms. In the U.S., tools like ChatGPT were released openly, with guardrails gradually added through public debate and user feedback. Regulatory oversight lagged behind innovation, reflecting a willingness to tolerate risks in favor of market dynamism. In China, however, platforms like Baidu's Ernie Bot were subject to strict pre-launch compliance checks to ensure alignment

[3]Sheehan, Matt. 2023. "China's AI Regulations and How They Get Made." Carnegie Endowment for International Peace. 2023. https://carnegieendowment.org/research/2023/07/chinas-ai-regulations-and-how-they-get-made?lang=en.

with state-approved narratives.[4] This revealed a system where control and oversight precede innovation.

Ultimately, AI regulation in both countries is not just about managing algorithms—it is an extension of their political DNA. While the U.S. model emphasizes rights and innovation, the Chinese model reflects control and state authority, setting the stage for a broader clash over which governance framework will shape the global AI order.

Data Governance and Sovereignty Battles

In the U.S., data governance discourse emphasizes privacy rights, transparency, and corporate accountability, albeit within a fragmented legal landscape. There is no single overarching federal privacy law; instead, states like California have led with statutes such as the California Consumer Privacy Act (CCPA).[5] Critics argue that the absence of a unified national framework weakens the country's capacity to regulate large-scale data collection effectively. Embedded in U.S. approaches are concerns about foreign access to citizen data, especially via Chinese-owned platforms. The case of TikTok is illustrative: U.S. authorities contend that data collected by TikTok could be accessed by the Chinese government, prompting debates about forced divestment or bans.[6]

China, by contrast, treats data as a national strategic asset under strong state control. With enactment of the Personal Information Protection Law (PIPL) and the Data Security Law, Beijing asserts regulatory authority over cross-border data flows and mandates that technology firms—both domestic and foreign—align their practices with national interests.[7] Under PIPL, for example,

---

[4]Ye, Josh, and Urvi Dugar. 2023. "China Lets Baidu, Others Launch ChatGPT-like Bots to Public, Tech Shares Jump." Reuters. August 30, 2023. https://www.reuters.com/technology/baidu-among-first-win-china-approval-ai-models-bloomberg-news-2023-08-30/.

[5] State of California Department of Justice. 2024. "California Consumer Privacy Act (CCPA)." State of California - Department of Justice - Office of the Attorney General. 2024. https://oag.ca.gov/privacy/ccpa.

[6] Minges, Madison. 2025. "National Security and the TikTok Ban." American University. January 23, 2025. https://www.american.edu/sis/news/20250123-national-security-and-the-tik-tok-ban.cfm.

[7]Minges, Madison. 2025. "National Security and the TikTok Ban." American University. January 23, 2025. https://www.american.edu/sis/news/20250123-national-security-and-the-tik-tok-ban.cfm.

transferring certain personal data abroad requires explicit separate consent and must satisfy strict auditing and regulatory approval. The Chinese model frames data sovereignty as inseparable from national security and regime stability.

A compelling example is the U.S. campaign against TikTok. Washington's critics argue that TikTok, owned by ByteDance in China, poses a risk because China's National Intelligence Law (2017) compels Chinese firms to cooperate with state security agencies. In response, the U.S. Congress passed the Protecting Americans from Foreign Adversary Controlled Applications Act (PAFACA) in April 2024, mandating divestiture or ban of "foreign adversary controlled" apps (explicitly targeting TikTok).[8] In short, the U.S. sees access to its citizens' data by a foreign regime as a national security threat, and has legislated accordingly.

Source: CNBC

This clash—U.S. emphasis on rights plus regulation, versus China's assertion of sovereignty and centralized control—fragments the global data ecosystem. Smaller states increasingly face pressure to choose between these paradigms. Will they adopt regulatory regimes favoring openness, or align with more controlled, sovereignty-driven models? The outcome of this battle may well define the architecture of global AI and data governance for decades to come.

[8] Liu, Han, and Ji Li. 2025. "TikTok versus United States." Cambridge University Press EBooks, February, 113–30. https://doi.org/10.1017/9781009457859.008.

Innovation vs. Regulation: The Pace Dilemma

In the United States, AI innovation is largely market-driven, powered by private technology companies such as OpenAI, Google DeepMind, and Anthropic. The U.S. regulatory approach tends to be reactive rather than proactive, allowing companies to deploy new technologies quickly while regulators catch up through guidelines, oversight committees, and ethical frameworks. For example, the launch of ChatGPT in 2022 occurred with minimal prior federal regulation. Ethical and safety guardrails were added incrementally in response to public and governmental scrutiny. This approach fosters rapid advancement, giving the U.S. a competitive edge in AI capabilities, but it also raises concerns about bias, misinformation, and misuse in critical sectors.

China, by contrast, enforces strict pre-approval regulations for AI deployment. Companies must comply with guidelines set by central authorities, ensuring that products align with political, ethical, and social norms before launch. The rollout of generative AI tools like Baidu's Ernie Bot was closely monitored by regulatory agencies, emphasizing alignment with state priorities and "socialist values." While this approach may slow deployment compared to the U.S., it reduces risks associated with misuse, disinformation, or politically sensitive content.

This divergence in regulatory pace creates a strategic dilemma. U.S. companies can innovate faster, attracting talent, investment, and global market share. However, gaps in regulation can allow harmful uses to proliferate, potentially inviting stricter retroactive policies. China's approach reduces such risks, but tightly controlled innovation may limit creativity and entrepreneurial flexibility, slowing technological leadership in emerging AI fields.

A notable example is AI in financial services. U.S. firms have rapidly adopted AI for credit scoring, fraud detection, and trading algorithms, sometimes outpacing regulatory clarity. In China, all AI-driven financial products undergo pre-approval to ensure compliance with state rules, preventing rapid experimentation but safeguarding systemic stability. [9]

Ultimately, the pace dilemma illustrates the trade-off between innovation and control. U.S. openness accelerates discovery but risks ethical and security breaches. China's regulatory rigor

[9] Yang, Samuel. 2025. "AI Ethics: Overview (China)." China Law Vision. January 20, 2025. https://www.chinalawvision.com/2025/01/digital-economy-ai/ai-ethics-overview-china/.

mitigates risk but may constrain disruptive innovation. This tension is central to understanding global AI rivalry and the future trajectories of AI governance.

AI in Security and Military Domains

In the United States, AI development for defense is framed around ethics, accountability, and interoperability with allied forces. The Department of Defense's *Responsible AI Strategy* emphasizes human oversight, transparency, and compliance with international humanitarian law. AI is deployed in areas such as predictive maintenance, logistics optimization, and decision-support systems, while autonomous weapon systems remain heavily regulated. This approach reflects the U.S. balance between technological superiority and ethical responsibility, acknowledging both military advantage and reputational risk.[10]

China, however, integrates AI into a broader military–civil fusion strategy, blending commercial innovations with defense applications. Algorithms are employed for battlefield simulations, surveillance, cyber operations, and autonomous systems, with less public debate about ethical constraints. The People's Liberation Army reportedly leverages AI to enhance situational awareness, optimize logistics, and manage advanced drone systems. Beijing's approach prioritizes speed, state control, and strategic dominance, viewing AI as both a force multiplier and a tool for domestic governance.

A compelling example of divergence is surveillance and facial recognition technology. In the U.S., its military applications are restricted by ethical guidelines, while private AI companies face strong scrutiny. In China, AI-driven surveillance in Xinjiang and border regions illustrates the state's prioritization of security and control over privacy, with technologies simultaneously advancing military and domestic intelligence capabilities.[11]

[10] "Utilization of Artificial Intelligence (AI) to Illuminate Supply Chain Risk." 2025. Defense Logistics Agency. May 2025. https://www.dla.mil/About-DLA/News/News-Article-View/Article/4186367/utilization-of-artificial-intelligence-ai-to-illuminate-supply-chain-risk/.

[11] "China's AI-Powered Surveillance State | Journal of Democracy." 2025. Journal of Democracy. 2025. https://www.journalofdemocracy.org/articles/chinas-ai-powered-surveillance-state/.

Ultimately, AI in security and military domains demonstrates how governance philosophy shapes technological adoption. The U.S. emphasizes ethical safeguards and coalition interoperability, whereas China emphasizes speed, state oversight, and strategic advantage. These competing models not only drive the bilateral AI rivalry but also influence global norms in military AI deployment.

Global Influence and Standard-Setting

Beyond domestic regulation, the U.S.-China AI rivalry increasingly plays out on the global stage, as both powers seek to shape the rules, standards, and norms that govern AI worldwide. AI governance is no longer merely a national concern; it has become a tool of geopolitical influence.

The United States has historically promoted multilateral, open-standard approaches, reflecting democratic and market-oriented principles. Initiatives such as the G7 Hiroshima AI Process aim to establish shared standards on AI safety, ethics, and transparency, emphasizing human-centric AI and responsible innovation.[12] By coordinating with allies, Washington seeks to extend its regulatory philosophy globally, ensuring that AI development aligns with democratic values.

China, in contrast, actively exports its state-centric AI governance model through partnerships in the Global South, digital infrastructure projects, and forums like the Digital Silk Road. Beijing promotes standards emphasizing central oversight, data sovereignty, and state control, often framing them as efficiency-oriented and security-conscious alternatives to Western frameworks. (

A concrete example is Africa and Southeast Asia, where U.S. and Chinese influence compete over AI infrastructure, smart-city projects, and regulatory guidance. While Washington often encourages private-sector-led innovation and ethical safeguards, Chinese companies implement AI solutions aligned with Beijing's centralized standards. Countries adopting one model over the other are effectively choosing between different approaches to sovereignty, privacy, and market control. (cfr.org)

[12]"Microsoft: G7 Hiroshima AI Process (HAIP) Transparency Report | OECD.AI | HAIP Reporting Framework." 2025. Oecd.ai. 2025. https://transparency.oecd.ai/reports/68e6cacb-5496-4487-8793-de3e70080b27.

Conclusion

The contest over AI regulation between the United States and China is far more than a technical or bureaucratic debate—it is a battle over the very frameworks that will define the future of technology, governance, and global order. In 2025, AI has evolved into a dual-use force: a driver of economic prosperity and a lever of state power. The U.S. approach, emphasizing democratic values, innovation, and ethical safeguards, contrasts sharply with China's state-centric model, which prioritizes control, strategic advantage, and societal alignment. These differences are not trivial; they shape how algorithms are designed, how data is governed, and how AI is deployed in both civilian and military spheres.

Source: Medium

Yet the rivalry is not a zero-sum game. Rather, it is a complex negotiation of risk, ambition, and ideology. U.S. openness accelerates discovery and global adoption but risks misuse, inequity, and security vulnerabilities. China's centralized approach mitigates risk and strengthens state oversight, but may constrain innovation and limit cross-border collaboration. In this interplay, smaller states and emerging economies are caught in the crosscurrents, forced to align with one model or navigate a hybrid path that balances access, control, and sovereignty.

Looking forward, the next decade of AI governance will hinge on which paradigm can scale effectively, adapt to unforeseen challenges, and persuade other nations to adopt its standards. The

U.S. model may appeal to markets and democratic coalitions, while China's model offers speed, control, and security assurances. The real stakes are global: AI standards and norms will shape not just economic and technological landscapes, but ethical boundaries, civil liberties, and even the conduct of war.

Ultimately, understanding AI regulation as a reflection of political philosophy, strategic priority, and global influence is critical. As AI moves from tools to infrastructure, and from innovation to governance, the U.S.-China rivalry is defining a new bipolar order in the digital era—one in which the rules, risks, and rewards of intelligence itself are contested. How the world navigates this competition will determine whether AI becomes a unifying force for progress or a vector of division and strategic tension.