IDSS PAPER

17 March 2026

The Logic of Access in US Digital Policy and Diplomacy

Jose Miguelito Enriquez and Kevin Chen Xian An

RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSiS 30

RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore
Ponder the Improbable since 1996
IDSS Paper
Ponder. Analyse. Prepare. Engage. Refresh.
www.rsis.edu.sg
No.044– 17 March 2026

The authors' views are their own and do not represent the official position of the Institute of Defence and Strategic Studies of the S. Rajaratnam School of International Studies, NTU. These commentaries may be reproduced with prior permission from RSIS and due recognition to the authors and RSIS. Please email to Editor IDSS Paper at RSISPublications@ntu.edu.sg.

The Logic of Access in US Digital Policy and Diplomacy

Jose Miguelito Enriquez and Kevin Chen Xian An

KEY TAKEAWAYS

- *The US approach to digital issues used to be described as laissez-faire, but that characterisation is no longer accurate.*

- *Recent developments surrounding AI company Anthropic and a diplomatic push against foreign tech regulations point to a security-centric approach.*

- *Washington wants to bind US tech companies to its will domestically while unshackling them abroad.*

COMMENTARY

Compared with the stringency of Europe and China's digital regulatory regimes, the United States' approach to digital issues has typically been characterised as laissez-faire. Successive administrations since the advent of the internet in the 1990s were seen to retain a general preference for "letting the market work" to protect civil liberties and maximise incentives for private innovation.

The rapid development of Artificial Intelligence (AI) tools, however, has made the relationship between the government and tech companies more complex, and has also exposed the limits of an absolutist free-market framing of US policy. AI developers are becoming integral to government agency functions in a way that goes beyond simply supplying hardware. Both OpenAI and xAI, for example, signed separate US$200 million contracts with the Pentagon in June and July 2025.

Claude, the AI tool made by Anthropic, was arguably one of the most valuable models employed by the US military, playing a key role in planning both the Venezuelan raid that captured then-President Nicolás Maduro and the initial strikes on Iran. As such, it came as a shock when a dispute between Anthropic and the Pentagon spilled into the open, resulting in the company being declared a "supply-chain risk". This development marks a crucial milestone in America's accelerationist orientation in AI development, but it is important to qualify the scope and limits of this trend of digital governance.

The rapid development of AI tools complicates the relationship between the US government and tech companies, highlighting the limits of a free-market approach. *Image source: Unsplash*

This action by the Pentagon is not entirely inconsistent with the historically laissez-faire approach to US digital governance. However, seen in conjunction with developments such as stronger US opposition to foreign digital regulations, it reflects a broader logic of US digital policy and diplomacy, one that involves unrestricted access to technology for the US government coupled with unrestricted overseas market access for the diffusion of US technology.

This is not simply a question of the Trump administration making an ad hoc political decision against an American AI firm, or of US diplomats lobbying against a foreign regulation perceived to be hostile to American interests. It is part of a broader, longer-term trend that also raises questions about US cyber power and leadership in the global digital space.

US Government Access to Technologies

In her 2023 book, *Digital Empires*, Anu Bradford illustrates how the US government has intervened to urgently protect US national security interests in cyberspace since the events of September 11. By the time of the 2016 landmark case, when the Justice Department attempted to force Apple to hack into an iPhone belonging to one of the perpetrators of the San Bernardino mass shooting incident, the government had already waged similar efforts 63 times.

In all these cases, the government was driven by a need to ensure national security and law enforcement, while tech companies were hesitant to grant the government access to their devices that could be exploited by criminal parties.

This dilemma is closely linked with the Anthropic–Department of War (DOW) dispute. The heart of the disagreement is that Anthropic has insisted on preventing the use of its AI models for mass domestic surveillance and in fully autonomous weapons, while the Pentagon believes that it should have the leeway to use AI in any manner it considers legal. Defence officials bristled at the idea of a "vendor [inserting] itself into the chain of command".

The fallout of this confrontation is still unfolding. Most reportage suggests the Pentagon's labelling of Anthropic as a supply-chain risk effectively prevents government contractors from using its models. Anthropic, however, argues that the wording of the Pentagon's announcement was narrower than initially feared. Neither side seems ready to back down.

Nonetheless, the use of the "supply chain risk" label, usually reserved for organisations from adversary countries, shows the extent of the Anthropic–DOW dispute. This unprecedented action has pushed Anthropic to bring the Pentagon to court, setting up yet another fierce legal battle over the government's access to sophisticated technologies.

Overseas Market Access for US Tech Diffusion

Yet, even as the US government tightens its demands on tech companies at home, it has demanded looser access regulations for those same companies to operate overseas.

In February, a leaked State Department cable revealed orders for US diplomats to lobby against attempts to regulate US tech companies' handling of foreign data. The cable reportedly cited the General Data Protection Regulation (GDPR) in the European Union as an example of "unnecessarily burdensome data processing restrictions and cross-border data flow requirements", while accusing China of building tech infrastructure with "restrictive data policies that expand its global influence and access to international data".

On the surface, this cable appears to be a continuation of the US government's techno-libertarian approach towards digital regulations overseas. In 2025, for example, US Secretary of State Marco Rubio ordered diplomats to whip up opposition to the European Union's Digital Services Act, which sought to compel social media firms to remove illegal content.

Such antipathy towards foreign regulations is certainly not new. In *Digital Empires*, Bradford wrote about how American officials and tech lobbyists opposed the EU Digital Markets Act, Europe's digital antitrust law aimed at five American tech giants. However, the Biden administration's efforts to lobby against "digital protectionism" abroad stalled when it also began fighting Silicon Valley's alleged anticompetitive practices at home.

The leaked cable points to an intensification of earlier trends. The United States does not just want to ensure free data flows for its tech companies; it also wants to do so explicitly to compete with burgeoning Chinese developers. The same spirit extends to the recent trade deals that the United States signed separately with Cambodia, Malaysia and Indonesia, calling for refraining from "measures that discriminate against US digital services or … products" and for the countries to "consult" or "communicate" with Washington before signing digital trade agreements that "[jeopardise] essential US interests".

Conclusion

In essence, Washington wants to bind US tech companies to its will domestically while unshackling them abroad. While these objectives seem dramatically different at first glance, they are both driven by the mantra of national security, albeit in different domains. The US security apparatus wants to retain control of and access to frontier technologies such as AI in the hopes of reinforcing American tech leadership.

If the lobbying efforts are successful, American AI companies will benefit from uninterrupted cross-border flows of data. However, they will also find it increasingly difficult to draw a balance between honouring safety principles, including data privacy and transparency, while working on US government contracts.

More broadly, these developments underscore that AI is one of the biggest arenas for US-China competition. As the AI race heats up, we may see more policy departures from a strictly laissez-faire approach to digital policy in favour of prioritising US AI dominance in military and consumer applications. For Washington, there is no other option but to win this race.

Jose Miguelito Enriquez *is an Associate Research Fellow in the Centre for Multilateralism Studies at the S. Rajaratnam School of International Studies (RSIS).* ***Kevin Chen Xian An*** *is an Associate Research Fellow in the US Programme at the Institute of Defence and Strategic Studies (IDSS), S. Rajaratnam School of International Studies (RSIS).*

Please share this publication with your friends. They can subscribe to RSIS publications by scanning the QR Code below.