The Need for Tech Regulation Beyond U.S.-China Rivalry

Kenton Thibaut

U.S. policymaking circles increasingly frame the topic of technology regulation in terms of a "race" with China for global supremacy, with critical national security implications. Tech executives have warned that regulatory and antitrust measures targeting Big Tech would impede artificial intelligence (AI) companies from out-innovating China, thus undermining U.S. national security[1]; the Trump administration scrapped the Biden administration's recently released national security-focused AI executive order in large part due to this same argument[2]. And officials in both the Trump and Biden administrations and Congress have drafted and passed measures to ensure that U.S. technology is developed and governed with national security objectives front and center.[3] These objectives have been served in the form of export controls,[4] investment restrictions,[5] and efforts to ban Chinese technologies from the U.S. market.[6]

There are justifiable national security arguments for these measures. People's Republic of China (PRC) actors do, indeed, weaponize the U.S. technology ecosystem in ways that undermine American interests, values, and national security. This includes the use of U.S. venture capital to fund technology companies with ties to China's surveillance and repression regime, the application of U.S. cloud infrastructure to evade export restrictions and

Kenton Thibaut is a senior resident China fellow at the Atlantic Council's Digital Forensic Research Lab (DFRLab), where she leads China programming for the Democracy + Tech Initiative, and a resident senior fellow at the Atlantic Council's Indo-Pacific Security Initiative (IPSI) at the Scowcroft Center for Strategy and Security.

train AI models that undermine U.S. interests, and the potential for social media platforms like TikTok to exploit the market openness of the United States to gather sensitive data on Americans. These are real security risks that need to be addressed.

However, absent a complementary approach that considers what Americans want their broader technology ecosystem to look like, these measures—which are narrowly crafted to address specific national security concerns largely limited to one problematic end user—will fail to adequately address systemic national security problems. The U.S. is long overdue for a conversation about what a more comprehensive and proactive tech strategy should look like. This should include an emphasis on transparency, disaggregating monolithic terms like "AI," safeguarding Americans' domestic data privacy and security, multistakeholder collaboration, and a clear articulation of what the U.S. can offer the world in AI technologies rather than what it aims to prevent. Such a strategy would enhance resilience against exploitation not just from China, but from a range of threat actors, strengthening U.S. security in the long term.

Silicon Valley and China's Military-Civil Fusion Strategy

In recent years, Silicon Valley investment firms have come under fire for funding PRC companies that advance China's technical military capabilities and aid in perpetuating human rights abuses within the country.[7] One report released by the House select committee on the Chinese Communist Party (CCP) detailed how billions of dollars of U.S. venture capital financing have flowed into Chinese companies that had previously been blacklisted by the U.S. government for enabling human rights abuses—for example, in the Uyghur autonomous region of Xinjiang.[8] Facing backlash, several high-profile U.S.-based firms divested from their China operations, with Sequoia Capital being one of the most notable cases.[9]

However, despite the chill in outbound U.S. venture capital investment to China in recent years,[10] U.S. companies are still providing funding to Chinese startups with close links to China's military-industrial complex. Indeed, even with the best of intentions, these connections can be difficult to escape in China. For example, U.S.-based venture capital firms Matrix Partners and BlueRun Ventures were early shareholders in the AI and robotics startup AgiBot (also known as Shanghai Zhiyuan Xinchuang Technology Co., Ltd), which was founded in February 2023 by former Huawei wunderkind Zhi Hui Jun (known as Peng Zhihui).[11] In the past few months alone, the company has signed strategic cooperation agreements to provide digital services and core functions for companies like iSoftStone, a close partner and digital technology provider to Huawei, and iFLYTEK, which is currently sanctioned by the U.S. government for its associations with human rights violations in the Xinjiang Uyghur Autonomous Region.[12]

Oftentimes, the distinction between commercial and government applications is blurred in China, and (as with many countries) there has been a well-documented approach by the Chinese state to promote technologies for dual-use purposes.[13] Efforts to address the lack of visibility into U.S. outbound investment have come in the form of recent rules. For example, on Oct. 28, 2024, the Treasury Department issued its outbound investment final rule, which outlined restrictions on investment activities related to AI, quantum computing, semiconductors, and microelectronics.[14] The move has bipartisan support; several more hawkish members of Congress have criticized it for not going far enough, proposing an expansion of the covered areas to include more sectors.[15]

However, what is often missed in national security discussions on this issue is the effect of a lack of transparency requirements for venture capital firms on reporting potentially problematic sources of funding, which makes it more difficult for researchers to trace investment flows. For example, in the United States, VC firms are not required to publicly disclose information regarding the limited partners (LPs) on whose capital contributions they often rely. This can lead to problematic loopholes.[16] Sequoia in particular has come under fire for investing in firms that then go on to

subcontract with China's People's Liberation Army (PLA).[17] In 2021, the firm helped to raise around $700 million in funding for the PRC-based AI firm 4Paradigm, which in 2020 received a contract from the PLA's ground force to develop a battalion and company command decision-making model.[18]

The difficulties tracing U.S. venture capital funding into problematic sectors of the Chinese technology ecosystem highlight one of the core shortcomings of the current U.S. approach. While the intent is undoubtedly to limit impacts to non-strategic sectors and applications, narrowly-tailored restrictions issued via Executive Order or through rules issued by the Committee on Foreign Investment in the United States (CFIUS) by their design focus on specific problematic end users or end uses; as such they often do not map neatly onto the complex ecosystem in which they are designed to operate. In addition, the policy is reactive in that such screening requires a notification or review process initiated by the U.S. government. Efforts to enhance transparency and disclosure requirements for U.S.-based venture capital funds—to both government entities and to the public, where appropriate[19]—could go a long way in mitigating the risks posed by the inherent opacity of the Chinese system, and enhancing visibility into potentially problematic funding flows into China.[20]

U.S. Cloud Service Providers and AI-Powered Threat Models

Similar to the debate surrounding the misuse of U.S. venture capital, the U.S. national security community has also highlighted concerns surrounding PRC companies' use of U.S.-based cloud services to circumvent chip restrictions and train AI models for potentially nefarious purposes. An August 2024 Reuters investigation of public tender documents showed that around a dozen state-linked university labs and technology firms sought to access AI models and compute through Amazon's AWS and Microsoft's Azure.[21] A major concern outlined by national security officials is the potential for PRC actors to train models that could be used against the United States—posing significant cybersecurity risks and threats to the American information ecosystem.[22]

Other concerns involve cloud services providing enabling infrastructure for Chinese companies to compete with the United States in strategic sectors, or to undertake activities that undermine U.S. national security interests.[23] In response to these concerns, policymakers have taken action. For example, in January 2024, the Biden administration took up a rule from a 2021 Trump administration executive order that proposed implementing know-your-customer rules for cloud service providers, which would require companies to verify and report the identities of foreign users on their platforms that train large AI models.[24] More recently, the House of Representatives passed the Remote Access Security Act, which broadens the scope of U.S. export controls to include foreign access to cloud computing.[25]

These actions have been taken in response to legitimate concerns, as Chinese AI companies have already leveraged U.S. compute to boost competitiveness and engage in business activities that may run counter to U.S. values. For example, Aiwei Cloud services is an AI-powered video company offering a number of commercial AI services.[26] The company uses Amazon's AWS platform for the software side of its Industrial PC (IPC) security video products, including video surveillance and facial recognition technology, to Chinese firms across more than 200 countries, regions, and territories—including many involved in the Belt and Road Initiative.[27] As another example, a recent report from Australian think tank ASPI mentioned Mobvoi, an AI company founded by former Google scientist Li Zhifei,[28] and the first Chinese company to launch a listing on the Hong Kong Stock Exchange based on AI-generated content (AIGC).[29] According to a December 2022 announcement, Mobovi's global deployment of its AIGC digital human and voice technology is supported by Oracle Cloud Infrastructure (OCI).[30] One of the products the company offers is AI-generated avatars—including news anchors—through its app, Weta365. An ASPI investigation revealed that Weta365's avatars were used in PRC-

state-linked disinformation campaigns online, including in the lead-up to Taiwan's 2024 presidential election.[31] The former is an example of a company operating on cloud infrastructure within China as provided by AWS's China subsidiary, and the latter is an example of a company using cloud services to access compute in the United States.

As these examples show, the line between private industry's commercial offerings and the state's geopolitical incentives are easily blurred in the Chinese context. Again, however, this raises questions about the efficacy of narrowly tailored national-security-focused solutions. While the know-your-customer rules may seem to target only the most problematic uses of U.S. cloud infrastructure, the lack of understanding about how these laws would be enforced in practice—as well as past controversy over the United States' use of national security reasoning to access data stored on servers abroad—has given rise to serious concerns over the approach.[32] Most germane to the technical specifications of the restrictions themselves, AI researchers have pointed out that serious harm can come from threat models that use exponentially less compute power than the more advanced frontier models these actions target.[33] For example, an AI model used for protein sequence prediction, which can be used to develop biological weapons, may require only dozens of chips (compared to the 30,000-plus needed for something like GPT-4) and thus fall well below acceptable compute thresholds.[34]

U.S. Data Broker Firms and PRC Intelligence Gathering on Americans

Another vector of concern for the national security policymaking community is PRC access to sensitive data on Americans—an issue most often discussed in the context of U.S. actions against the social media platform TikTok. Multiple national security officials, from Avril Haines to William Burns to Christopher Wray, have warned that TikTok's ability to gather data from Americans—and the Chinese government's legal ability to compel the company to provide that data to the PRC—presents serious national security risks.[35] Indeed, China's 2017 National Security Law provides PRC intelligence authorities with sweeping powers to compel assistance in performing "national intelligence efforts."[36] In response, the U.S. government has undertaken a range of measures against the app, with the most recent being a law passed by Congress requiring its China-based parent company, ByteDance, to divest from the company or face a ban.[37]

China's appetite for data on U.S. persons is well documented. In October 2024, the Chinese hacking group Salt Typhoon was identified as responsible for stealing a huge amount of Americans' metadata via a massive data breach affecting at least eight U.S. telecommunications companies.[38] This follows a long line of sensitive data breaches, including a 2013 hack of personally identifiable information (PII) from the Office of Personnel Management that affected 22 million Americans, including millions of copies of government employees' SF-86 documents,[39] hacks of hotels and airlines like Marriott and United Airlines, and U.S. call records and communication information from a number of high-level politicians and government officials.[40] Scholars have written for years about how these hacks, supplemented with data purchased on the open market, have served as the basis for massive databases the PRC government may use for intelligence targeting or recruitment, among other nefarious activities.[41] One such company, Shenzhen Zhenhua, reportedly maintains a database of millions of data points on hundreds of thousands of individuals—some of whom are high-level politicians—from both open and proprietary data sources; the company also highlights on its website its close customer relationships to PRC intelligence and military services.[42]

Indeed, there is no doubt that PRC state entities see the value in collecting data on Americans for intelligence purposes. However, the proposed actions on TikTok leave open serious questions on how effectively a ban or divestment would protect Americans' data from exfiltration. The Digital Forensic Research Lab previously conducted a technical, policy, and legal analysis of the stated national security risks posed by TikTok. Our research found that TikTok can be said to present a unique

risk in terms of its Chinese ownership, in that the PRC's National Intelligence Law gives the government broad leeway in potentially compelling access to TikTok's data, including on Americans. In addition, even under the circumstances of outside control of TikTok's data storage, it would be almost impossible to know if Chinese intelligence authorities somehow maintained a backdoor into these data streams.[43]

At the same time, however, we found that TikTok's data collection practices on Americans are not outside what is commonly practiced by other social media companies, including Meta and X. Notably, the data that TikTok can provide on Americans pales in comparison to what the Chinese government has accessed through both its illegal hacking activities and what is available legally on the open market through U.S. based third-party data brokers. In fact, a report from Duke University's Sanford School of Public Policy found that, via data brokers, it is "not difficult to obtain sensitive data about active-duty members of the military, their families, and veterans, including non-public, individually identified, and sensitive data, such as health data, financial data, and information about religious practices," noting that location data was also available for purchase.[44]

In response to these challenges, in February 2024 the Biden administration issued an executive order seeking to prevent access to Americans' bulk sensitive personal data by countries of concern, including Russia, Iran, and China, with the final rule issued by the Department of Justice on Dec. 27, 2024.[45] While an important step in stemming the flow of sensitive data abroad, it applies only to certain transactions related to countries of concern and focuses only on national security implications, rather than addressing broader rights-related issues. This leaves open the ability for the domestic data market to continue to develop and sell Americans' bulk sensitive personal data for unscrupulous purposes. For example, while the executive order and final rule will ban Americans' genomic data from being sold to countries of concern, it does not ban such data from being sold to domestic customers or partner countries. That the market is still able to flourish domestically opens up the possibility of data broker companies exploiting backdoors and the many exceptions—including, for example, those applying to financial data—that still undermine Americans' privacy and data security in the long run.[46] In addition, a determined state threat actor could find ways to circumvent these restrictions if it really wanted to—know-your-customer rules can go only so far if China's intelligence services are the last customer in a line of 10 others, each obscured by layers of subsidiaries registered abroad.[47] Allowing a domestic market to continue leaves open more avenues for exploitation by China—or, for that matter, non-state actors like dark web scammers.

Again, a narrow, national-security-oriented focus on TikTok to address risks in the U.S. data ecosystem risks overlooking much broader security vulnerabilities and underscores the important reality that often—with regard to U.S. tech policy—the domestic and foreign are inherently linked. The focus on taking down TikTok as a means to save American data privacy distracts from more impactful policy solutions. In short, framing the risks to Americans' data security as a problem that can be solved by banning TikTok leaves a wider and more consequential swath of American data unprotected and available for purchase and acquisition.

Widening the Aperture on Tech Regulation

As the examples above illustrate, there are serious and legitimate national security concerns surrounding China's weaponization of the U.S. technology ecosystem to undermine American interests. Whether it's U.S.-based venture capital firms inadvertently (or, in some cases, explicitly) helping to fund Chinese technologies that undermine human rights, U.S. cloud infrastructure being leveraged by PRC actors to train or deploy AI models for use in surveillance activities abroad or malign information operations, or data purchased from U.S.-based data broker firms for use in intelligence gathering and targeting, there is real cause for concern. These activities demand a response, and the United States has

enacted a series of measures—including export controls, end-use and user restrictions on U.S. technology, and laws seeking to protect Americans' data from PRC exfiltration.

Some industry leaders have claimed that regulation will hurt U.S. national security and cause China to overtake the U.S. in the "AI arms race." As U.S. policymakers take various measures on these issues, it has become evident that a real conversation is needed about the trade-offs between regulating and setting standards for the technology industry at home while the U.S. seeks to compete abroad.[48]

First, the United States needs standards on algorithmic transparency for all platforms, not just TikTok. On the issue of TikTok, for example, the United States has very few transparency requirements for platform companies operating in the country—meaning that platforms do not have to provide any insight on algorithmic manipulation, the data collected and how it is used, etc.[49] Such requirements would go a long way in helping researchers, policymakers, and everyday Americans better understand what is happening to their data, beyond and inclusive of TikTok.

In addition, a clearer articulation from the government of its stated strategy of protecting a limited set of advanced, "sensitive" U.S. technologies with investment and trade restrictions—known as "small yard, high fence"—should include, for example, how the U.S. comes to identify which technologies are critical to national security. This would help set basic standards and inform thresholding conversations for issues like cloud computing—not just for China, but for other competitors. This requires government transparency around what the risks of adversary access to these technologies are. Specifying the risks enables communities of practice to come together to discuss the trade-offs and avenues for collaboration around setting general standards around design, deployment, and use. This also requires the U.S. government to more clearly articulate in its policies what technology specifically it is aiming to regulate. Much of the current debate treats "AI" as a monolithic entity. However, the ecosystem of capabilities, applications, and technologies that encompass AI are diverse and differentiated. The type of technology or industry matters. Not all tech is alike, and it cannot all be governed the same. We need clarity on this at the policy level.

Second, a better tech strategy requires a consideration of drivers and outcomes beyond those related to national security. Multistakeholder involvement in conversations on the risks, benefits, and regulatory requirements for AI-enabled technologies —including from technical, industry, government, and nonprofit sectors—is essential. National security concerns should not be the sole basis for decision-making. Doing so runs the risk of "cloak[ing] what are really policy decisions as technical decisions,"[50] which can limit the ability to deploy a more adaptive governance framework informed by multistakeholder deliberation—an approach that may be more appropriate for governing technologies with rapidly evolving capabilities.[51] For example, AI researchers have pointed out the limits of compute thresholds, such as those in the U.S. Treasury's current outbound investment restrictions, as a viable strategy for regulating outbound AI investments. Novel capabilities may emerge with massive scaling, and there are diminishing returns in performance as training compute reaches a certain threshold.[52]

Third, with tech, the domestic and foreign policy realms are inherently linked, and policy approaches should be reflective of this. The U.S. requires a stronger focus on achieving domestic innovation goals rather than an emphasis on preventing adversaries from achieving theirs. This includes an articulation of what the United States wants for core technologies like AI, rather than a focus on what it is trying to prevent. As the outgoing Secretary of Commerce Gina Raimondo said in a recent interview, "the only way to beat China is to stay ahead of them."[53] The U.S. needs a positive and proactive agenda for technology governance to go hand in hand with a more threat-based and reactive one. Much of this reactivity on the foreign side stems from the fact that the United States does not have an overarching strategy for domestic tech regulation. On the TikTok issue, for example, there is a lack of strategic clarity on how the United

States should protect its critical information infrastructure amid great power competition; the government is also equally limited by a lack of federal frameworks—beyond the Committee on Foreign Investment in the United States (CFIUS)—to protect Americans' data privacy.[54] Comprehensive federal privacy legislation would go a long way in plugging one of the most glaring holes in the U.S. data ecosystem: that Americans' data can be harnessed legally and sold on the open web.[55] While the recent data security regulations provide an important stopgap to the flood of Americans' data going abroad, the lack of federal privacy legislation and the domestic data broker market leave open potential loopholes and workarounds an enterprising threat actor can exploit—including the Chinese intelligence authorities.[56]

This reactive approach also means that what the United States is offering the world in terms of AI-powered solutions is less visible than what it is trying to limit. This is especially detrimental given the wariness with which U.S. partners and allies are viewing U.S. control over the AI boom. Global majority countries specifically are increasingly turning to countries like China for AI-driven solutions to provide public services to their populations[57] and, for some, to better engage in surveillance and repression.[58] And China has been active in multilateral fora like the United Nations and building coalitions to support its own AI governance measures.[59] If the United States wants to compete with China on AI, it must articulate its own value proposition.

In the end, China can serve as a forcing function for the United States to drive action in areas that are in desperate need of a regulatory conversation. However, the next step must be to articulate what good regulation and governance looks like. At its foundation should be an overarching tech strategy that connects different industry segments (noting that tech is not monolithic) and does so in a way that reflects U.S. interests and values. This approach will make the U.S. ultimately more resilient to the myriad ways bad actors seek to exploit the open technology ecosystem.

Endnotes

1. AI Now Institute, "Tracking the U.S. and China AI Arms Race," https://ainowinstitute.org/publication/tracking-the-us-and-china-ai-arms-race.
2. "2024 Republican Party Platform," UC Santa Barbara Presidency Project, https://www.presidency.ucsb.edu/documents/2024-republican-party-platform.
3. Federal Register, "Maintaining American Leadership in Artificial Intelligence," https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence. ; White House, "Memorandum on Advancing the United States Leadership in Artificial Intelligence," https://www.whitehouse.gov/briefing-room/presidential-actions/2024/10/24/memorandum-on-advancing-the-united-states-leadership-in-artificial-intelligence-harnessing-artificial-intelligence-to-fulfill-national-security-objectives-and-fostering-the-safety-security/; Congressional Report, "Report 116-617," U.S. Congress, https://www.congress.gov/116/crpt/hrpt617/CRPT-116hrpt617.pdf#page=1210.
4. Bureau of Industry and Security, "Commerce Strengthens Export Controls to Restrict China's Capability to Produce Advanced Technologies," https://www.bis.gov/press-release/commerce-strengthens-export-controls-restrict-chinas-capability-produce-advanced.
5. Reuters, "U.S. Finalizes Rules to Curb AI Investments in China," https://www.reuters.com/technology/artificial-intelligence/us-finalizes-rules-curb-ai-investments-china-impose-other-restrictions-2024-10-28/.
6. NPR, "Trump Signs Executive Order That Will Effectively Ban Use of TikTok in the U.S.," https://www.npr.org/2020/08/06/900019185/trump-signs-executive-order-that-will-effectively-ban-use-of-tiktok-in-the-u-s.
7. Select Committee on the CCP, "Investigative Report: American Financial Institutions Funneled Billions to PRC Companies," https://selectcommitteeontheccp.house.gov/media/reports/investigative-report-american-financial-institutions-funneled-billions-prc-companies.
8. Select Committee on the CCP, "THE CCP'S INVESTORS: How American Venture Capital Fuels the PRC Military and Human Rights Abuses," https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/2024-02-08%20-%20VC%20Report%20-%20FINAL.pdf.
9. The New York Times, "Sequoia Capital Splits into Separate U.S. and China Businesses," https://www.nytimes.com/2023/06/06/business/dealbook/sequoia-capital-split-china-india.html.; Newsweek, "China Investment and Sequoia's Role in AI Development," https://www.newsweek.com/china-investment-sequoia-artificial-intelligence-pla-1835996.
10. S&P Global Market Intelligence, "U.S.-Backed Funding Rounds in China Fall to Lowest in a Decade," https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/us-backed-funding-rounds-in-china-fall-to-lowest-in-a-decade-81822765.
11. Zhiyuan Robot, "Zhiyuan First Shareholder Meeting Held Successfully," https://web.archive.org/web/20250114222716/https://www.zhiyuan-robot.com/article/188/detail/13.html.; Zhiyuan Robot, "Project Introduction and Founding Team," https://archive.ph/fIz7j.; 21C Electronic Network, "After Leaving Huawei, Zhihuijun Received Three Rounds of Financing and Is Now Valued at US$1 Billion!," https://archive.ph/cd696#selection-455.33-455.70.
12. RobotTalk, "Zhiyuan Robotics Cooperates with iSoftStone on Huawei's Hongmeng Ecosystem," https://archive.ph/L3Myw. ; Sohu, "iSoftStone: Huawei's Capable Partner Both On and Off The Stage," https://archive.ph/Q9FGg#selection-383.38-383.100.; Network Enterprise News, "iFLYTEK and Zhiyuan Robotics Sign Strategic Cooperation Agreement," https://archive.ph/KWRL6.; Baker McKenzie, "US Government Adds 28 Chinese Entities Associated with Human Rights Violations and Abuses," https://sanctionsnews.bakermckenzie.com/us-government-adds-28-chinese-entities-associated-with-human-rights-violations-and-abuses/.
13. Meng J., Wang J. The policy trajectory of dual-use technology integration governance in China: A sequential analysis of policy evolution // Technology in Society. 2023. Vol. 72. p. 102175. https://www.sciencedirect.com/science/article/abs/pii/S0160791X22003165
14. U.S. Department of the Treasury, "Provisions Pertaining to U.S. Investments in Certain National Security Technologies and Products in Countries of Concern," https://home.treasury.gov/system/files/206/TreasuryDepartment-OutboundInvestmentFinalRuleWEBSITEVERSION_0.pdf.

15. Select Committee on the CCP, "Moolenaar: Biden Regulations on Outbound Investment to China a Good Step, Congress Must Strengthen," https://selectcommitteeontheccp.house.gov/media/press-releases/moolenaar-biden-regulations-outbound-investment-china-good-step-congress-must
16. Global Policy Watch, "CFIUS Issues Guidance on Disclosure of Information About Limited Partner Investors," https://www.globalpolicywatch.com/2023/05/cfius-issues-guidance-on-disclosure-of-information-about-limited-partner-investors-and-application-of-mandatory-filing-rules-to-multi-stage-transactions/.
17. Newsweek, "China Investment in Sequoia and Artificial Intelligence," https://www.newsweek.com/china-investment-sequoia-artificial-intelligence-pla-1835996.
18. CSET Georgetown, "Harnessed Lightning," https://cset.georgetown.edu/wp-content/uploads/CSET-Harnessed-Lightning.pdf
19. Washington Post, "VC Clean Capital Pledge and China," https://www.washingtonpost.com/politics/2024/12/19/vc-clean-capital-pledge-china/.
20. FDD, "The Weaponization of Capital - China's Private Equity and Venture Capital," https://www.fdd.org/analysis/2022/09/15/the-weaponization-of-capital-chinas-private-equity-venture-capital/.
21. Reuters, "List of Chinese Entities Who Have Turned Cloud Access Restricted in US Tech," https://www.reuters.com/technology/list-chinese-entities-who-have-turned-cloud-access-restricted-us-tech-2024-08-23/.
22. Reuters, "US to Propose Know-Your-Customer Requirements for Cloud Computing Companies," https://www.reuters.com/technology/us-propose-know-your-customer-requirements-cloud-computing-companies-2024-01-26/.
23. ASPI, "Persuasive Technologies: China's Implications for Future National Security," https://www.aspi.org.au/report/persuasive-technologies-china-implications-future-national-security.
24. Reuters, "Eying China, US Proposes 'Know Your Customer' Cloud Computing Requirements," https://www.reuters.com/technology/us-propose-know-your-customer-requirements-cloud-computing-companies-2024-01-26/
25. Congress, "House Bill 8152," https://www.congress.gov/bill/118th-congress/house-bill/8152.
26. Sohu, "A note on Aiwei IoT's Participation in The "Amazon Cloud Technology Innovation Conference," https://web.archive.org/web/20250114225150/https://www.sohu.com/a/560478063_121124374.
27. AWS, "Amazon Web Services Case Study: Aiwei IoT," https://web.archive.org/web/20240723051441/https://aws.amazon.com/cn/solutions/case-studies/ivyiot-case-study/; A&Smag, "Build a Secure and Compliant Platform to Help Enterprises Get on the Cloud and Go Global," https://www.asmag.com.cn/news/202204/109872.html.
28. ASPI, "Persuasive Technologies," https://www.aspi.org.au/report/persuasive-technologies-china-implications-future-national-security.
29. Technode, "AI and Electronics Maker Mobvoi Files for Hong Kong IPO," https://technode.com/2023/06/01/ai-and-electronics-maker-mobvoi-files-for-hong-kong-ipo/.
30. Oracle, "Oracle Cloud Technology Development Globalization Announcement," https://www.oracle.com/cn/news/announcement/development-globalization-oracle-cloud-technology-2022-12-20/.
31. ASPI Strategist, "As Taiwan Voted, Beijing Spammed AI Avatars, Faked Paternity Tests, and Leaked Fake Documents," https://www.aspistrategist.org.au/as-taiwan-voted-beijing-spammed-ai-avatars-faked-paternity-tests-and-leaked-fake-documents/.
32. EFF, "US CLOUD Act and EU Privacy Protection: A Race to the Bottom," https://www.eff.org/deeplinks/2018/04/us-cloud-act-and-eu-privacy-protection-race-bottom.
33. The Wire China, "The Cloud Conundrum: AI," https://www.thewirechina.com/2024/10/13/the-cloud-conundrum-ai/.
34. Center for New American Security, " Comments on the Advanced Computing/Supercomputing IFR: Export Control Strategy & Enforcement for AI Chips," https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/BIS-2022-0025-0062_attachment_1.pdf.
35. Congress, "House Report 63," https://www.congress.gov/congressional-report/118th-congress/house-report/63/1.
36. Chinese National People's Congress Network, "PRC National Intelligence Law (2017)," https://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf.
37. Reuters, "US Appeals Court Upholds TikTok Law Forcing Its Sale," https://www.reuters.com/legal/us-appeals-

court-upholds-tiktok-law-forcing-its-sale-2024-12-06/.
38. Reuters, "Large Number of Americans' Metadata Stolen by Chinese Hackers, Senior Official Says," https://www.reuters.com/technology/cybersecurity/large-number-americans-metadata-stolen-by-chinese-hackers-senior-official-says-2024-12-04/.
39. ABC News, "Exclusive: 25 Million Affected by OPM Hack, Sources Say," https://abcnews.go.com/US/exclusive-25-million-affected-opm-hack-sources/story?id=32332731.
40. The New York Times, "Trump and China Trade," https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html.; Reuters, "United Airlines Data Breached by China-Backed Hackers," https://www.reuters.com/article/markets/united-airlines-data-breached-by-china-backed-hackers-bloomberg-idUSL3N1093MC/.; CISA, "Joint Statement by FBI and CISA on People's Republic of China (PRC) Targeting Commercial Telecommunications," https://www.cisa.gov/news-events/news/joint-statement-fbi-and-cisa-peoples-republic-china-prc-targeting-commercial-telecommunications.
41. Chen, Ming Shen, "China's Data Collection on US Citizens: Implications, Risks, and Solutions," https://www.sciencepolicyjournal.org/uploads/5/4/3/4/5434385/chen_jspg_v15.pdf
42. Balding, Christopher, Chinese Open Source Data Collection, Big Data, And Private Enterprise Work For State Intelligence and Security: The Case of Shenzhen Zhenhua (September 13, 2020).
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3691999
43. DFRLab, "TikTok: Hate the Game, Not the Player," https://dfrlab.org/2024/02/14/tiktok-hate-the-game-not-the-player/.
44. "Data Brokers and the Sale of Data on US Military Personnel," https://techpolicy.sanford.duke.edu/data-brokers-and-the-sale-of-data-on-us-military-personnel/.
45. Justice Department, "Final Rule Addressing Threat Posed by Foreign Adversaries' Access," https://www.justice.gov/opa/pr/justice-department-issues-final-rule-addressing-threat-posed-foreign-adversaries-access.
46. Atlantic Council, "What Biden's New Executive Order About Americans' Sensitive Data Really Does," https://www.atlanticcouncil.org/blogs/new-atlanticist/experts-react/experts-react-what-bidens-new-executive-order-about-americans-sensitive-data-really-does/#jackson-data.
47. CSIS, "Analysis: New Executive Order on Personal Data," https://www.csis.org/analysis/new-executive-order-personal-data.
48. Wired, "Big Tech Breaking Up Will Only Help China," https://www.wired.com/story/big-tech-breaking-will-only-help-china/.
49. DFRLab, "TikTok: Hate the Game, Not the Player," https://dfrlab.org/2024/02/14/tiktok-hate-the-game-not-the-player/.
50. Kaminski, Margot E., Regulating the Risks of AI (August 19, 2022). Boston University Law Review, Vol. 103:1347, 2023, U of Colorado Law Legal Studies Research Paper No. 22-21,
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4195066
51. Reuel, Anka, and Trond Arne Undheim. "Generative AI Needs Adaptive Governance." arXiv preprint arXiv:2406.04554 (2024). https://arxiv.org/html/2406.04554v1#Sx4
52. Hooker, Sara. "On the limitations of compute thresholds as a governance strategy." arXiv preprint arXiv:2407.05694 (2024). https://arxiv.org/abs/2407.05694
53. Wall Street Journal, "Raimondo Says Holding Back China in Chips Race Is a 'Fool's Errand,'"https://www.wsj.com/politics/national-security/china-biden-chip-manufacturing-gina-raimondo-b98c2606.
54. DFRLab, "TikTok: Hate the Game, Not the Player," https://dfrlab.org/2024/02/14/tiktok-hate-the-game-not-the-player/.
55. Foreign Policy, "The Data Arms Race Is No Excuse for Abandoning Privacy," https://foreignpolicy.com/2018/08/14/the-data-arms-race-is-no-excuse-for-abandoning-privacy/.
56. Lawfare, "Tackling Data Brokerage Threats to American National Security," https://www.lawfaremedia.org/article/tackling-data-brokerage-threats-to-american-national-security.
57. NED, "Smart Cities and Democratic Vulnerabilities," https://www.ned.org/wp-content/uploads/2022/12/Beth-Kerley_Smart-Cities-and-Democratic-Vulnerabilities.pdf.
58. Atlantic Council, "Venezuela: A Playbook for Digital Repression," https://www.atlanticcouncil.org/wp-content/

uploads/2024/07/Venezuela-a-playbook-for-digital-repression.pdf.
59. SCMP, “China’s Cyberspace Regulator Vows to Work with Africa on AI Governance,” https://www.scmp.com/news/china/diplomacy/article/3257862/chinas-cyberspace-regulator-vows-work-africa-ai-governance.

SALVE
THE PELL CENTER

About the Pell Center

The Pell Center for International Relations and Public Policy at Salve Regina University is a multi-disciplinary research center focused at the intersection of politics, policies, and ideas. Dedicated to honoring Senator Claiborne Pell's legacy, the Pell Center promotes American engagement in the world, effective government at home, and civic particpation by all Americans.

www.pellcenter.org