A Framework for Assessing U.S. Data Policy Toward China

By Samm Sacks and Peter Swire

Access to and use of personal data has moved to the center of the U.S.-China technology conflict. TikTok is the most prominent but far from the sole example of this conflict. Republicans and Democrats have found common ground in the concern that unacceptable national security and privacy risks arise from Beijing's access to Americans' data through open commercial channels. Over the last several years, U.S. policymakers have expanded their earlier focus on cyber theft and industrial espionage to grapple with new risks posed by Chinese firms handling Americans' data or data flowing to China by data brokers or other means.

In support of proposed legislation requiring export controls of certain U.S. personal data, Director of National Intelligence Avril Haines said, "There's a concern about foreign adversaries getting commercially-acquired information…and [I] am absolutely committed to trying to do everything we can to reduce that possibility."[1]

The Biden administration and Congress are building on the effort, which started in the Trump administration, by proposing a range of measures that aim to create new guardrails for data flows to China. These include executive orders for reviewing "transactions" involving foreign adversaries' access to Americans' sensitive data, bans on Chinese software applications, creating blacklists of countries approved to receive Americans' data as an export-controlled item, etc. The spate of proposals remains in draft form, unresolved amid debate that does not map onto political party lines. To date, we have not seen any systematic approach to address what limits on data flows should apply, and for what reasons.

In this article, we offer a framework that assesses the different approaches currently under discussion by U.S. policymakers. Our framework identifies four policy models and analyzes the costs and benefits of each, drawing on the perspectives of trade/economics, national security, and privacy. First, the **Digital Free Trade model** emphasizes the benefits to the U.S. from having robust trade in goods and services in general, and with China more specifically. Second, the **Blocking Adversaries model** emphasizes specific national security harms that can come from trade in which sensitive national security information goes into the hands of the Chinese

[1] Wyden, Lummis, Whitehouse, Hagerty, Heinrich and Rubio Introduce Bipartisan Bill to Protect Americans' Data from Unfriendly Foreign Nations, Bar TikTok Employees in China From Accessing U.S. Information, https://www.wyden.senate.gov/news/press-releases/wyden-lummis-whitehouse-hagerty-heinrich-and-rubio-introduce-bipartisan-bill-to-protect-americans-data-from-unfriendly-foreign-nations-bar-tiktok-employees-in-china-from-accessing-us-information#:~:text=reduce%20that%20possibility.

government. Third, the **Privacy Law model** builds on the growing bipartisan consensus that the U.S. should enact comprehensive privacy legislation, with the goal of addressing collection by domestic companies, but with the more recent rationale that privacy legislation can also address privacy harms by transnational actors. Fourth, the **Data Allies model** provides a way to address specific national security and privacy risks posed by non-democracies, while retaining a willingness to engage in global trade when such risks are manageable.

This article does not seek to advocate for particular policy outcomes; instead, we offer an intellectual framework for systematic analysis of the risks and benefits of different solutions across economics, security, and privacy standpoints. U.S. limits on data transfers to China are likely to help shape the limits other governments set on cross-border data transfers. Our aim is to inform the policymaking process to account for the ripple effects now impacting not only the U.S.-China relationship but also the future of global data governance.

Unpacking the Risk

We begin by first identifying how U.S. policymakers have perceived the nature of the risk itself. This section explains the national security concerns motivating policy proposals focused on blocking or restricting China's access to Americans' sensitive data.

As discussed further below, the Trump administration raised concerns about transfer of data to China, such as by its effort to ban TikTok and by blocking transactions in the Committee on Foreign Investment in the United States (CFIUS) that would have transferred sensitive personal information to Chinese companies.[2]

The Biden administration has explained its rationale for action in the Executive Order (EO) 14034 released in June 2021 ("Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries") as follows:

> The ongoing emergency declared in Executive Order 13873 arises from a variety of factors, including the continuing effort of foreign adversaries to steal or otherwise obtain United States persons' data. That continuing effort by foreign adversaries constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States. To address this threat, the United States must act to protect against the risks associated with connected software applications that are designed, developed,

[2] Executive Order on Addressing the Threat Posed by TikTok, August 6, 2020, https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/ and Regarding the Acquisition of Musical.ly by ByteDance Ltd., Federal Register, August 19, 2020, https://www.federalregister.gov/documents/2020/08/19/2020-18360/regarding-the-acquisition-of-musically-by-bytedance-ltd.

> manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary.[3]

A separate EO issued in September 2022 clarified the specific factors related to personal data that the CFIUS should consider in evaluating national security risks of inbound investment. The EO stated that foreign government access to certain kinds of data posed potential adverse impacts on national security:

> Data is an increasingly powerful tool for the surveillance, tracing, tracking, and targeting of individuals or groups of individuals, with potential adverse impacts on national security. In section 1702(c)(5) of FIRRMA, the Congress recognized that the Committee may consider whether a covered transaction may "expose, either directly or indirectly, personally identifiable information, genetic information, or other sensitive data of United States citizens to access by a foreign government or foreign person that may exploit that information in a manner that threatens national security." Moreover, advances in technology, combined with access to large data sets, increasingly enable the re-identification or de-anonymization of what once was unidentifiable data. Therefore, it is important for the United States Government to stay current with threats posed by advances in such technology, including by considering potential risks posed by foreign persons who might exploit access to certain data on United States persons to target individuals or groups within the United States to the detriment of national security.[4]

These policy statements suggest that U.S. policymakers' concerns go beyond the risk posed by Beijing's access to individual datasets held by one company or platform. Instead, the concern also applies to how combining individual company data with other commercial and proprietary data sets could compromise U.S. national security in different ways, including:

- If additional sources of personal data such as location, social media, or pattern of life data were to be acquired legally from companies or bought openly through unregulated data brokers and combined with what Beijing has already acquired through cyber theft, Chinese security services could use it to gain leverage over and to **target Americans in sensitive government national security positions or military personnel** for manipulation,

[3] The full text of the Executive Order is available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/. The Executive Order also defines "connected software applications" as "software, a software program, or a group of software programs, that is designed to be used on an end-point computing device and includes as an integral functionality, the ability to collect, process, or transmit data via the Internet;" "foreign adversary" means "any foreign government or foreign non-government person engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons."

[4] https://www.whitehouse.gov/briefing-room/presidential-actions/2022/09/15/executive-order-on-ensuring-robust-consideration-of-evolving-national-security-risks-by-the-committee-on-foreign-investment-in-the-united-states/.

blackmail, or other forms of coercion. These concerns would be most relevant for individuals with security clearances or those with access to critical infrastructure. A related concern is that the data could be used in **sophisticated spear-phishing campaigns** targeting these government and other personnel.

- Beijing's analysis of such lawful and unlawfully acquired datasets could be used to identify and monitor **Chinese dissidents** abroad.

- Beijing could use aggregated data sources in ways that **enable large-scale electronic surveillance**. As Chinese online services and network infrastructure gain in prominence around the world, U.S. policymakers are worried that the Chinese government could filter or monitor data processes abroad in utilizing data transmissions for intelligence gathering, both in bulk and with targeting.

- Access to large datasets collected abroad provides Chinese companies insight into population-level and individual consumer behavior, risk tolerance, and other preferences. This helps to strengthen the **economic competitiveness** of Chinese firms by enabling them **to develop AI applications** that better serve diverse demographics in markets around the world.

- If Beijing were to attempt to push out **misinformation** to audiences abroad, insights about individual preferences or psychology decision-making trends could help make that information more convincing and realistic.

- These data-driven insights could enable China to launch **more effective cyber-attacks** such as phishing attacks or preparations for disruption of critical infrastructure. According to the White House National Cybersecurity Strategy, digital technologies create new cyber vulnerabilities, with "the quantity and intimacy of personal data collection … growing exponentially" opening "novel vectors for malicious actors."[5]

Across these distinct risks, U.S. officials see data as posing a challenge because it can be copied, stored, and analyzed at a later time. Thus, officials considering risks related to China's potential access to sensitive U.S. data are not just concerned about how data might be used today, but how such data could eventually be aggregated with other types of data to damage U.S. national security in the future.

The line between economic competitiveness and national security risk may blur following the logic of the Biden administration's National Security Strategy. China is defined as presenting the

[5] National Cybersecurity Strategy, March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

"greatest geopolitical challenge" and as a "competitor" intent on reshaping the international order.[6] According to this rationale, there are geostrategic implications if Chinese firms outcompete U.S. firms in third countries, competing with the United States for dominance over network infrastructure and the social media space. One consideration U.S. policymakers view as important but has received less attention in public discussion is that the success of Chinese companies poses risks to U.S. national security and intelligence collection capabilities.

Many of the recent risks concerning policymakers coalesce in a single company. The future of TikTok in the United States has become a policy issue itself. U.S. government concerns about the company have focused on unauthorized data access and the data-driven recommendation algorithm, with the possibility of state influence on what content is promoted or hidden. Negotiations for a CFIUS national security agreement with TikTok continue. TikTok has proposed the so-called "Project Texas," designed to limit data flows to China as managed by the U.S.-based Oracle Corporation.[7] Any decision on TikTok's fate is likely to have far-reaching implications for U.S. data policy toward China.

Seeking Trade/Economics, National Security, and Privacy Outcomes

Three perspectives inform U.S. policymakers as they assess China-related data risks: trade/economics, national security, and privacy. Effective overall U.S. policy depends on understanding each of these important perspectives and the policy outcomes sought in order to distinguish, in particular, settings in which data flows should be blocked or allowed to continue.

Anupam Chander and Paul Schwartz have previously described the tension between free trade and privacy: "Privacy and trade appear to be in a mortal contest. Will trade be the death of data privacy, as international flows of personal information across the world place our privacy at risk? Or will data privacy be the death of trade, as restrictions on information flows make modern trade increasingly difficult?"[8] In some instances, however, trade considerations may result in greater privacy protections. The influence of Europe's strict privacy protections is greater precisely because the U.S. and other nations wish to continue to trade with Europe, and so this "Brussels effect" has created an incentive for countries outside Europe to enact privacy protections.[9] Different types of privacy standards could increase free trade or block adversaries.

---

[6] National Security Strategy, October 2022, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.
[7] Matt Perault and Samm Sacks, "Project Texas: The Details of TikTok's Plan to Remain Operational in the United States," *Lawfare*, January 26, 2023, https://www.lawfareblog.com/project-texas-details-tiktoks-plan-remain-operational-united-states.
[8] Anupam Chander and Paul Schwartz, "Privacy and/or Trade," 90 University Chicago Law Review 49 (2023), https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3462&context=facpub.
[9] Anu Bradford, "The Brussels Effect: How the European Union Rules the World," (2020), https://scholarship.law.columbia.edu/books/232/.

A similar dynamic can exist between national security and free trade. National security arguments can justify preventing foreign adversaries from gaining insights about U.S. nationals and economic activity. On the other hand, U.S. national security can benefit from global trade. U.S. technology competitiveness and access to global data helps fuel innovation and strengthens the ability of U.S. firms to compete with Chinese firms in third-country markets. Moreover, U.S. firms collect data from around the world that creates opportunities for access, subject to the rule of law, for U.S. law enforcement or national security purposes.

To understand policy options related to China data risks, we next examine the policy implications if we maximize any one of these three goals. The Digital Free Trade model optimizes for economic growth. The Blocking Adversaries model optimizes for national security. The Privacy Law model would create strict data privacy standards for all companies, domestic and foreign. The Data Allies model works within a framework to develop principles for transferring data amongst a coalition of partners (democracies with systems based on rule of law as well as other like-minded governments).

For each model, we identify tradeoffs among the three perspectives, as well as analyze the ways in which these perspectives can overlap, depending on scope and implementation. Our aim is to inform policy discussion amid much debate about how to achieve the most effective policy outcomes.

I. Digital Free Trade Model

To achieve economic growth and other benefits from international trade, the Digital Free Trade model would place no limits on China or other countries simply because they have authoritarian political systems. This model has largely described the status quo in the United States. The free trade perspective contributed to the U.S. support for China to enter the World Trade Organization in 2001, and the WTO today has over 160 members with widely varying systems of governance.[10]

The data free flow provisions of the United States-Mexico-Canada Agreement (USMCA) illustrate this model. USMCA does not allow restrictions on cross-border data transfers and prohibits requirements to use or locate computing facilities in a territory as a condition for doing business.[11]

Under the Digital Free Trade model, the main question is what presumptions and showing of risk would need to be established as a basis for limiting trade. USMCA does have exceptions allowing

[10] World Trade Organization, "Members and Observers," (2023), https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm.
[11] See Chapter 19 "Digital Trade" (Articles 19.8, 19.11, 19.12) Agreement between the United States of America, the United Mexican States, and Canada 7/1/20 Text, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf.

for data localization related to government procurement, privacy, national security, and other public policy objectives.[12] Similar categories of exemptions exist under the WTO.[13]

A variation on the Digital Free Trade model emphasizes the role of reciprocity in achieving tariff reduction and optimal levels of international trade. As economists have discussed since John Stuart Mill, when one government imposes a tariff (or other restriction on trade), then another government has an incentive to counter by imposing its own tariff (or other restriction). The goal of the second government can be to create an incentive for the first government to negotiate, with the goal of achieving lower tariffs from both governments, and thus greater overall benefits from international trade.[14] As economists Bagwell & Staiger have pointed out, this sort of reciprocity approach can be justified in the name of achieving free trade, and mechanisms to do so have long been built into international trade agreements.[15]

The free-trade reciprocity approach could use sanctions and limits on data handling as tools to push China to ease restrictions on foreign tech firms. For example, the United States could respond to data localization requirements in China by establishing symmetrical requirements. Beijing requires partnerships with domestic Chinese firms in sectors like cloud services as well as local data storage and processing in certain cases, and may require source code reviews. TikTok's Project Texas model could represent a form of reciprocity, if done for the purpose of encouraging China to open its own markets to U.S. services. By contrast, if Project Texas is designed to prevent data flows to China as an end unto itself, then the rationale for U.S. regulation would be a non-trade rationale such as national security or privacy, as discussed later in the paper.

Limits on free trade, including those based on a national security rationale, can also be self-defeating. Chad Bown has called export controls "America's Other National Security Threat," saying that they can have "negative commercial consequences," be "ineffective at addressing national security risks," and be "problematic for trade and diplomatic relations."[16] Agathe Demarais has highlighted how export restrictions in the space market were "very successful in creating a global network of companies making competing products while ensuring U.S. companies cannot compete."[17] The U.S. share of the global space market declined from 75 percent

[12] Nigel Cory, "USMCA Data and Digital Trade Provisions: Status Check," *The Wilson Center*, December 19, 2021, https://www.wilsoncenter.org/article/usmca-data-and-digital-trade-provisions-status-check.
[13] The "National Security Exception" and the World Trade Organization, *Congressional Research Service,* November 28, 2018, https://crsreports.congress.gov/product/pdf/LSB/LSB10223.
[14] For a discussion of the literature, see Kyle Bagwell & Robert W. Staiger, "GATT-Think," NBER Working Paper 8005 (2000), available at https://www.nber.org/system/files/working_papers/w8005/w8005.pdf.
[15] Id.
[16] Chad P. Bown, "Export Controls: America's Other National Security Threat," 30 Duke J. Comp. & Int'l L. 283 (2019-2020), available at https://scholarship.law.duke.edu/djcil/vol30/iss2/4/.
[17] Demarais, Agathe. *Backfire: How Sanctions Reshape the World Against US Interests*. Columbia University Press, 2022 as cited in Meyers, "Klaus E. Meyer, Tony Fang, Andrei Y. Panibratov, Mike W. Peng, Ajai Gaur, International business under sanctions, Journal of World Business, Volume 58, Issue 2, 2023.

in 1998 (following the introduction of a set of export controls to protect American aerospace companies' expertise) to less than 50 percent a decade later.[18]

Trade-offs

Recent U.S. policy debates have highlighted ways that national security and privacy can come into conflict with the Digital Free Trade model. For national security, the Trump and Biden administrations have both emphasized risks to national security such as EO 14,034's finding of an "extraordinary threat to the national security" from adversary efforts "to steal or otherwise obtain United States persons' data." For privacy, surveillance within China is pervasive, personal data held by companies in China is routinely accessible to the government, and China lacks rule-of-law safeguards against excessive surveillance.[19] More generally, some argue that the era of borderless data is over amid rising mistrust around the world concerning foreign government access to data.[20]

These are legitimate national security concerns. Policy analysis should recognize, however, the ways that global trade may also advance national security and cybersecurity goals. Proponents of free trade have argued, for instance, that free trade supports national security by creating stronger ties with potential adversaries such as China and reducing the likelihood and magnitude of conflict.[21] Joseph Nye writes that "entanglement is an important means of making an actor perceive that the costs of an action will exceed the benefits."[22] He points to the exponential increase in cross-border data flows underpinning global commerce as a factor in cybersecurity and other forms of deterrence.[23] For those inclined to cut ties with China, it is worth considering what conflict would look like if the U.S. were to block trade and create sanctions at the level now applying to North Korea. Some degree of trade and entanglement with China, therefore, likely supports U.S. national security.

A stronger U.S. economy can also benefit U.S. national security in several ways. First, U.S. and Chinese firms today are both large net importers of data, positioning them to compete for market share and technology leadership. The soft power resulting from U.S. commercial success creates

---

[18] Demarais, Agathe. *Backfire: How Sanctions Reshape the World Against US Interests*. Columbia University Press, 2022 as cited in Meyers, "Klaus E. Meyer, Tony Fang, Andrei Y. Panibratov, Mike W. Peng, Ajai Gaur, International business under sanctions, Journal of World Business, Volume 58, Issue 2, 2023.

[19] Peter Swire, "Annotated Bibliography on Chinese Surveillance and European Union Data Privacy," (2019), https://fpf.org/wp-content/uploads/2019/07/Peter-Swire-le-monde-annotated-bibliography.pdf.

[20] David McCabe and Adam Satariano, "The Era of Borderless Data Is Ending," *New York Times*, May 23, 2022, https://www.nytimes.com/2022/05/23/technology/data-privacy-laws.html#:~:text=Nations%20are%20accelerating%20efforts%20to,a%20kind%20of%20digital%20currency.&text=As%20a%20subscriber%2C%20you%20have,can%20read%20what%20you%20share.

[21] Daniel Day, "Free Trade Agreements and National Security: Five Key Issues," *American Security Project*, August 1, 2014, https://www.jstor.org/stable/resrep06003.

[22] Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," International Security, Vol. 41, No. 3 (Winter 2016/17), pp. 44–71, https://www.belfercenter.org/publication/deterrence-and-dissuasion-cyberspace.

23 Nye, 58-59.

strategic advantages beyond profit alone, including greater engagement with the global South and other parts of the world. Related, under the rule of law, U.S. national security and law enforcement agencies can gain lawful access to data, with substantial privacy safeguards.[24] In addition, maintaining commercial ties with China can also help U.S. and allied firms gain visibility into developments with cutting-edge private sector players and an on-the-ground understanding of the tech sector in China.

II. Blocking Adversaries Model

The second approach seeks to restrict data from flowing to certain countries, such as China, deemed foreign adversaries by the U.S. government. The stated goal is to eliminate national security harms that could result if authoritarian governments were to gain access to information about either specific U.S. persons or population-level insights.

U.S. policy proposals currently under discussion that fall into the Blocking Adversaries model include the following:

- The Biden Administration's June 2021 Executive Order "Protecting Americans' Sensitive Data from Foreign Adversaries"[25] establishes a criteria-based framework to assess "foreign adversary connected software applications." Criteria include a review of potential risk indicators, including:

> ownership, control, or management by persons that support a foreign adversary's military, intelligence, or proliferation activities; use of the connected software application to conduct surveillance that enables espionage, including through a foreign adversary's access to sensitive or confidential government or business information, or sensitive personal data; ownership, control, or management of connected software applications by persons subject to coercion or cooption by a foreign adversary; ownership, control, or management of connected software applications by persons involved in malicious cyber activities; a lack of thorough and reliable third-party auditing of connected software applications; the scope and sensitivity of the data collected; the number and sensitivity of the users of the connected software application; and the extent to which identified risks have been or can be addressed by independently verifiable measures.[26]

[24] David Hoffman, "Schrems II and TikTok: Two Sides of the Same Coin," *North Carolina Journal of Law and Technology*, Volume 22. Issue 4, May 2021, https://ncjolt.org/wp-content/uploads/sites/4/2021/05/NCJOLT-Vol.-22.4_573-616_Hoffman.pdf.
[25] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/.
[26] Ibid.

- The Commerce Department's Final Rule on Securing the Information and Communications Technology and Services Supply Chain (the ICTS Rule) implements the above Executive Order, defining connected software applications as a category of ICTS vulnerable to exploitation by a foreign adversary, and grants the Secretary of Commerce power to block transactions posing unacceptable risks to U.S. national security.[27]

- Senator Ron Wyden introduced the "Protecting Americans' Data from Foreign Surveillance Act,"[28] which would amend the export control list to add certain personal American data to the list of controlled items. It aims to create a "shared zone of mutual trust" for coordination on data export controls with U.S. allies. It also would deny licenses for export/re-export where national security harms are found, considering, for example, whether the foreign government has conducted hostile foreign intelligence operations or the ability for a foreign government to coerce access to personal data.

- Senator Mark Warner introduced the Restricting the Emergence of Security Threats that Risk Information and Communications Technology Act (the RESTRICT Act) in March 2023. The Restrict Act "requires federal actions to identify and mitigate foreign threats to information and communications technology (ICT) products and services (e.g., social media applications)." In addition, under the bill, "the Department of Commerce must identify, deter, disrupt, prevent, prohibit, investigate, and mitigate transactions involving ICT products and services (1) in which any foreign adversary (such as China) has any interest, and (2) that pose an undue or unacceptable risk to U.S. national security or the safety of U.S. persons."[29]

In addition to its current negotiations with TikTok, CFIUS has cited national security as a basis for limiting ownership or control by China-related entities. In 2019, CFIUS ordered the Chinese gaming company Beijing Kunlun Tech to divest its ownership of the gay dating app, Grindr. One specific concern was that Beijing could be able to combine data on personal relationships from Grindr with what it was presumed to have obtained from the Office of Personnel Management data breach of over 21 million U.S. national security personnel records. The CFIUS rationale addressed both risks to individual U.S. government employees, as well as the possibility of aggregated data profiles for coercion or blackmail.[30]

---

[27] https://www.federalregister.gov/documents/2023/06/16/2023-12925/securing-the-information-and-communications-technology-and-services-supply-chain-connected-software.
[28] https://www.wyden.senate.gov/news/press-releases/wyden-lummis-whitehouse-rubio-and-hagerty-introduce-bipartisan-legislation-to-protect-americans-private-data-from-hostile-foreign-governments.
[29] S.686 - RESTRICT Act, https://www.congress.gov/bill/118th-congress/senate-bill/686.
[30] Carl O'Donnell, "Exclusive: Told U.S. security at risk, Chinese firm seeks to sell Grindr dating app," *Reuters*, March 27, 2019, https://www.reuters.com/article/us-grindr-m-a-exclusive/exclusive-told-u-s-security-at-risk-chinese-firm-seeks-to-sell-grindr-dating-app-idUSKCN1R809L and Samm Sacks, "Addressing the Data Security Risks of U.S.-China Technology Entanglement," *Brookings*, https://www.brookings.edu/wp-content/uploads/2020/11/Samm-Sacks.pdf.

Trade-offs

The Blocking Adversaries model, by focusing restrictions on the nationality of companies, is in tension with the Digital Free Trade model. It is true that the WTO and other trade agreements provide an exception for national security, but widespread prohibitions based on nationality could turn the exception into the rule.

The economic effects of these sorts of nation-based prohibitions can arise with China specifically, or for other countries more generally. If the U.S. government were to name China to a list of countries prohibited from accessing Americans' data without an export control license or other nation-based restrictions, Beijing could retaliate with its own blocking mechanism through laws such as the Personal Information Protection Law (PIPL). The PIPL has a provision that could be used to prohibit U.S. firms from handling Chinese citizen data anywhere in the world.[31] This could not only affect firms operating inside China, but could impact U.S. cloud service providers, banks, and other multinationals handling Chinese data globally.

It is also possible that new limits on data export from the U.S. could lead Chinese regulators to reciprocate by closing off remaining channels for outbound transfers. There is debate within China's cyber regulatory system about the extent to which authorities will fully implement data localization requirements.[32] Multinationals are currently waiting for approvals from China's cyber regulator on outbound transfers. Anecdotal evidence indicates that only a small number of U.S. firms have so far received an unofficial greenlight for outbound transfers.

Potentially, China's data localization rules may create space for Chinese firms, operating data centers in China, as the only viable way for any global business to mix Chinese and non-Chinese data. Strict implementation of China's data localization rules, however, would also appear to put severe limits on the ability of Chinese firms themselves to send personal data out of the country.

New limits on outbound U.S. data transfers would likely have a significant effect on the actions of countries other than China. Already, there are data sovereignty policies around the world that require geographically based storage and processing of data.[33] These policies are an increasing

[31] According to Article 43 of the PIPL: "Article 43: Where any country or region adopts discriminatory prohibitions, limitations or other similar measures against the People's Republic of China in the area of personal information protection, the People's Republic of China may adopt reciprocal measures against said country or region on the basis of actual circumstances," Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021, https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.

[32] Translation: Outbound Data Transfer Security Assessment Measures – Effective Sept. 1, 2022, Stanford Cyber Policy Center DigiChina Project, https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-effective-sept-1-2022/.

[33] Jennifer Daskal and Justin Sherman, Data Nationalism on the Rise, *Data Catalyst,* June 2020, https://datacatalyst.org/wp-content/uploads/2020/06/Data-Nationalism-on-the-Rise.pdf; Théodore Christakis,

obstacle to the ability of U.S. companies to operate internationally, beyond China, including for sectors where U.S. companies lead, such as cybersecurity.[34] In this context, U.S. actions will be a reference and a roadmap for other governments that are concerned about U.S. companies and the U.S. government getting access to their citizens' data. In the wake of U.S. actions to limit TikTok, for instance, France has considered also banning data exports for U.S. social media companies such as WhatsApp and Instagram.[35] Since the rise of the Internet in the 1990's, the U.S. has generally supported "the free flow of information."[36] To the extent that the U.S. departs from that decades-long policy, other countries can more easily point to U.S. restrictions as the basis for their own new restrictions on data flows.

The Blocking Adversaries model may also have negative unintended consequences for national security and cybersecurity, despite the explicit security rationale driving current policy proposals. Restrictions on data flows imposed on U.S. firms by countries beyond China undermine the competitiveness of U.S. digital industries, reducing leadership in cybersecurity-related capabilities and technologies. Data localization laws hurt cybersecurity by creating obstacles for integrated cybersecurity management, the provision of cybersecurity services, and cooperation on cyber defense, including information sharing.[37] More broadly, as noted above by Agathe Demarais, export controls on American technology can lead to reductions in the global market share of U.S. providers. For instance, limits on exports of personal data such as the telemetry used in cybersecurity could reduce the ability of U.S. cybersecurity companies to service the global market.[38]

The impact of the Blocking Adversaries model on privacy remains uncertain. Potentially, federal policy that focuses only on protecting data from foreign threats does not address privacy harms by U.S. firms. On the other hand, greater transparency on data flows to China is included in the American Data Protection and Privacy Act (ADPPA), which is discussed in more detail below. National security concerns about China thus might add political support for enacting federal privacy legislation.[39]

"'European Digital Sovereignty'": Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy," (Dec. 7, 2020), https://ssrn.com/abstract=3748098.

[34] Swire, Peter and Kennedy-Mayo, DeBrae, The Effects of Data Localization on Cybersecurity – Organizational Effects (last revised June 23, 2023) https://ssrn.com/abstract=4030905.

[35] Laura Kayali, "It's not just TikTok: French also warn against WhatsApp, Instagram," *Politico* (March 22, 2023), https://www.politico.eu/article/french-top-officials-warn-lawmakers-against-using-tiktok-whatsapp-instagram.

[36] The White House, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," at 5 (May 2011), https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[37] Swire, Peter and Kennedy-Mayo, DeBrae, The Effects of Data Localization on Cybersecurity – Organizational Effects (last revised June 23, 2023) https://ssrn.com/abstract=4030905.

[38] Swire, Peter et al., "Risks to Cybersecurity from Data Localization, Organized by Techniques, Tactics, and Procedures" (June 13, 2023), https://ssrn.com/abstract=4466479.

[39] U.S. House Energy & Commerce Committee, "ICYMI: E&C Republicans and Technology and Cybersecurity Experts Renew Calls for Comprehensive Data Privacy Protections," (Feb. 6, 2023),

III. Privacy Law Model

Under the Privacy Law model, the primary goal is to ensure the statutorily-required level of privacy protection. That goal is pursued even though there could be reduction of international trade, such as with countries that lack effective privacy protections. The goal is also distinct from national security because the focus of privacy policy is on overall protection of the data of individuals, rather than on an assessment of the risk of such data in the hands of a particular adversary.

Privacy concerns have motivated recent proposals for U.S. law relevant to China, notably in the ADPPA. The ADPPA has progressed further in Congress than previous proposed comprehensive privacy laws, including with a 53-2 vote in favor of the bill in 2022 in the House Energy & Commerce Committee.[40] The ADPPA contains a transparency provision requiring the covered entities or service providers to include in their privacy policies any data flows of personal information to China, Russia, Iran, and North Korea,[41] and House committee documents in early 2023 have stressed the importance of this provision, especially concerning China.[42]

A new comprehensive privacy law would seek to address harms from data processing generally, applying most or all protections regardless of the nationality of the company. Such laws have utilized a variety of approaches, including permitting data transfers to third countries or prohibiting them. The ADPPA as drafted in 2022 has a default of permitting outbound data transfers, except with the notice requirement for the named countries such as China. In contrast, the EU and United Kingdom have a default against permitting transfers of personal data to third countries, with a stated concern that privacy will not be protected adequately once it goes abroad. The EU and UK do allow transfers of data to countries that meet a standard for "adequate" protection.[43] Adequacy assessments, notably in the EU, have been held to apply to access by governments for national security or other law enforcement purposes, in addition to concerns about commercial transfers. For countries that do not provide overall protections at that level, the EU and UK laws can permit

---

https://energycommerce.house.gov/posts/icymi-e-and-c-republicans-and-technology-and-cybersecurity-experts-renew-calls-for-comprehensive-data-privacy-protections.

[40] Peter Swire, "The Bicameral, Bipartisan Privacy Proposal is a Big Deal," *Lawfare*, June 9, 2023, https://www.lawfareblog.com/bipartisan-bicameral-privacy-proposal-big-deal; Cameron Kerry, "Federal Privacy Regulators Should Accept Victory Gracefully," Brookings (Aug. 12, 2022), https://www.brookings.edu/blog/techtank/2022/08/12/federal-privacy-negotiators-should-accept-victory-gracefully/

[41] https://www.congress.gov/bill/117th-congress/house-bill/8152/text.

[42] Hearing Memo and Chairs Rodgers' Opening Remarks on Strengthening American Competitiveness and Beating China , "Economic Danger Zone: How America Competes to Win the Future Versus China," https://energycommerce.house.gov/posts/chairs-rodgers-opening-remarks-on-strengthening-american-competitiveness-and-beating-china and https://d1dth6e84htgma.cloudfront.net/Briefing_Memo_IDC_2023_02_01_1_a94f2f0063.pdf?updated_at=2023-01-30T15:42:00.604Z.

[43] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en; https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183.

data flows pursuant to Standard Contractual Clauses, under which the data exporter and importer promise to maintain privacy protections equivalent to those applying if the data remains locally.

Trade-offs

As discussed previously, there are ways that Privacy Law may either restrict or enable transfers of personal data. Privacy Law may be "the death of trade" by restricting transfers of personal data if done aggressively. On the other hand, strict EU privacy laws have created an incentive for the U.S. to adopt comprehensive privacy legislation, which if enacted would help U.S. firms maintain access to European markets.[44]

Similarly, for the national security concerns, the effects of the Privacy Law model could go in either direction. Privacy Law might complement national security concerns, such as if support in Congress for privacy legislation included restrictions on transfers to China or other countries deemed adversaries or weak protectors of privacy. Additional restrictions on bulk data sales involving data brokers, even if based on security concerns, could also reinforce Privacy Law by closing off a vector for foreign government access. By contrast, a focus only on transfers to adversary countries could reduce overall data protection, if legislation failed to protect against privacy harms from domestic and allied countries.

IV. Data Allies Model

The Data Allies approach broadly reflects the Biden Administration's current approach. It involves a coalition of partners (democracies with systems based on rule of law as well as non-democracies considered like-minded governments such as Singapore) working together within a framework to develop principles for transferring data among themselves. Data Allies use a principled basis to facilitate more data sharing with each other, while also using a stricter standard for "adversary" countries like Russia and China to access Americans' data. The core concepts underpinning this model are captured in the Declaration of the Future of the Internet, which aims to "realize the benefits of data free flows with trust based on our shared values as like-minded, democratic, open and outward looking partners.[45]

[44] Peter Swire, Testimony on "The Invalidation of the EU-U.S. Privacy Shield and the Future of Transatlantic Data Flows," Senate Commerce Committee (Dec. 9, 2020), https://peterswire.net/wp-content/uploads/Swire-Senate-Commerce-Committee-Testimony.final-as-submitted.pdf.

[45] FACT SHEET: United States and 60 Global Partners Launch Declaration for the Future of the Internet, April 28, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/28/fact-sheet-united-states-and-60-global-partners-launch-declaration-for-the-future-of-the-internet/. See also First U.S. Cyber Ambassador Nathaniel Fick on His Vision for Cyber Diplomacy, *Homeland Security Today,* (Dec. 14 2022), https://www.hstoday.us/featured/hstoday-qa-first-u-s-cyber-ambassador-nathaniel-fick-on-his-vision-for-cyber-diplomacy/.

The U.S. is already participating in a Data Allies approach across a number of channels. It is working with G-7, OECD, and other partners on the "Data Free Flow with Trust" efforts initiated by Japan. This past December, the U.S., European Union member states, and other OECD members announced the "Declaration on Government Access to Personal Data Held by Private Sector Entities."[46] This Declaration highlighted "common approaches to safeguarding privacy and other human rights and freedoms when accessing personal data for national security and law enforcement purposes." Among other recent developments, earlier in 2022, the U.S. Commerce Department participated in the "Global Cross Border Privacy Rules (CBPR) Declaration," which promotes data flows among participating countries based on an international certification system.[47]

The Data Allies approach is also formally incorporated into at least three U.S. legal instruments. First, the EU/U.S. Data Privacy Framework, drafted after the EU/U.S. Privacy Shield was struck down in court in the European Union, is the most recent of the three examples. This past October, President Biden issued Executive Order 14086 to create new privacy safeguards that would apply to "qualifying states."[48] Qualifying states would be designated by the Attorney General, in consultation with the Secretary of State, the Secretary of Commerce, and the Director of National Intelligence. The new safeguards would apply to persons from qualifying states such as EU member states, but not to persons from other countries.

Second, the Judicial Redress Act of 2015 extends certain rights of judicial redress that have been available to U.S. persons under the Privacy Act of 1974.[49] These rights apply to persons from "covered countries" as designated by the Attorney General, with concurrence from the Secretary of State, Secretary of the Treasury, and Secretary of Homeland Security.

Third, the Clarifying Lawful Overseas Use of Data Act of 2018 (CLOUD Act) also uses the approach of "qualifying foreign governments."[50] For such governments, the CLOUD Act authorizes negotiation of an executive agreement that would enable the non-U.S. government to

---

[46] OECD, "Landmark agreement adopted on safeguarding privacy in law enforcement and national security data access," (Dec. 14, 2022), https://www.oecd.org/newsroom/landmark-agreement-adopted-on-safeguarding-privacy-in-law-enforcement-and-national-security-data-access.htm.

[47] At the time of the announcement in April, 2022, the participating countries were Canada, Japan, the Republic of Korea, the Philippines, Singapore, Chinese Taipei, and the United States of America. https://www.commerce.gov/global-cross-border-privacy-rules-declaration. For additional discussions of recent cooperative efforts among data allies, see Sujit Raman, "Lawfare – Two Visions of Digital Sovereignty," *Cross-Border Data Forum* (June 5, 2023), https://www.crossborderdataforum.org/lawfare-two-visions-of-digital-sovereignty; Kenneth Propp, "More than adequate: New directions in international data transfer governance," *Atlantic Council*, (June 19, 2023), https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/more-than-adequate-new-directions-in-international-data-transfer-governance.

[48] https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities.

[49] https://www.justice.gov/opcl/judicial-redress-act-2015.

[50] U.S. Department of Justice, "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act," (April 2019), https://www.justice.gov/opa/press-release/file/1153446/download.

access communications held by U.S. service providers. Executive agreements are signed by the Attorney General, with notice to Congress and the opportunity for Congress to override. Under the law, the qualifying foreign government must meet a number of privacy and civil liberties criteria.[51]

Trade-offs

The Data Allies model emphasizes convergence rather than conflicts in pursuing the three goals of economic growth, national security, and privacy protection. It presents a kind of mirror of the Blocking Adversaries model by using an allowlist of approved countries rather than a blocklist.

Creating a coalition of data-sharing allies helps the United States more seamlessly exchange data with economic and national security benefits. Despite the emphasis in recent China-related policy proposals on restricting outbound U.S. data transfers, we benefit from policies that help create a durable coalition of countries allowing their data to be sent to and from the United States. The ability of U.S. firms to maintain a high rate of innovation depends upon access to global markets, talent, and, perhaps most important, datasets.

This model sets up a framework for countries to share their data—even if those countries lack identical data protection laws—by setting achievable, similar standards for data to flow. It allows more companies both large and small to operate globally, in contrast to a situation where only a few of the largest firms can afford to comply with different data protection laws in many countries.

Being part of a large data sharing coalition, the United States can create more economic incentives for other parts of the world to join, from Latin America to parts of Southeast Asia.[52] The economic pull of such a coalition offers an appealing alternative to other countries that otherwise might consider modeling their own system on China's model. China's PIPL may be attractive to some nations in offering consumer data protections in such a way that minimally constrains the state.[53]

The specific impact of the Data Allies model depends on the definition of the limits put in place on countries not included in the coalition. Broad and strict limits on all data transfers to non-participating countries like China would mean that in effect, Data Allies functioned the same as Blocking Adversaries, discussed previously. Moreover, implementation will face two main

[51] Peter Swire & Jennifer Daskal, "Frequently Asked Questions about the U.S. CLOUD Act," (Apr. 16, 2019), https://www.crossborderdataforum.org/frequently-asked-questions-about-the-u-s-cloud-act/.
[52] Peter Swire & DeBrae Kennedy-Mayo, "Two Ways that Smaller Countries Could Participate in Emerging Global Systems for Transfer of Electronic Evidence," *Cross-Border Data Forum* (May 30, 2019), https://www.crossborderdataforum.org/two-ways-that-smaller-countries-could-participate-in-emerging-global-systems-for-transfer-of-electronic-evidence/.
[53] There is debate about the implications of the PIPL on China's state actors. See Jamie Horsley, "How Will China's Privacy Law Apply to the State?" *DigChina Project*, January 29, 2021, https://www.brookings.edu/articles/how-will-chinas-privacy-law-apply-to-the-chinese-state/. Mark Jia writes in *Authoritarian Privacy*, that privacy law can "enhance perception of state performance and shore up Party legitimacy," see *Authoritarian Privacy* (February 17, 2023), University of Chicago Law Review, Vol. 91, 2023, https://ssrn.com/abstract=4362527.

hurdles: determining how countries actually qualify to have data flowing and the possibility that the European Court of Justice will continue to strike down agreements.

In addition, there may be more advantages to multilateral rather than bilateral Data Allies solutions. DFFT and CBPRs, for example, provide the benefit of scale, creating more economic incentives for participation, along with established mechanisms like the OECD.

In conclusion on the Data Allies model, cooperation among allies facilitates the goal of Digital Free Trade, in at least two notable ways. First, a Data Allies approach enables commercial transfers among allies. Second, both the EU and the U.S. have had legal limits on transfers of data to nations that lack effective protections against government access to data. A Data Allies approach facilitates transfers of data, such as for countries that have "adequate" protection against government access for data, as addressed in the EU/U.S. Data Privacy Framework.

The Data Allies Model similarly supports privacy goals. Under the U.S. CLOUD Act, transfers of data are permitted more freely to "qualifying foreign governments" with strong privacy protections than to other nations. For the EU, adequacy findings in recent years have extended to allies such as Japan and South Korea, in addition to the current EU/U.S. Framework, with its new protections against government access.

Finally, the Data Allies Model addresses national security concerns by setting stricter rules to limit transfers of personal data to adversaries. The conceptual approach of the Data Allies Model does not specify precisely what limits apply for trade, privacy, and national security purposes. The approach does, however, appropriately direct attention to the particular effects on trade, privacy, and national security from any particular policy proposal.

Conclusions

This article has described the Digital Free Trade, Blocking Adversaries, Privacy Law, and Data Allies models to clarify what is at stake for the single policy issue of possible limits on transfers of Americans' data to China. Each of these models can align or create tension with the others in pursuit of the goals of economic growth, national security, and privacy protections.

Considering these three goals is consistent with the objectives laid out in the 2021 Executive Order 14034, which called for a "through, rigorous, evidence-based analysis." That order acknowledged that not all data have the same level of sensitivity, and listed factors to consider in evaluating risks such as "the scope and sensitivity of the data collected" and the "number and sensitivity of users." With respect to economic growth and international trade, we assume that these goals remain in effect with respect to China for many exports, imports, and sectors, and therefore a blanket ban on

trade with China would be an over-reaction to concerns about data-related harms to national security and privacy.

We also highlight the Data Allies model as a way to conceptualize the emerging U.S. approach for international data transfers. That model is already instantiated in multiple ways, including in: the Data Free Flow with Trust initiative; the OECD Declaration on government access to data; the CPBR certifications; the Judicial Redress Act of 2015; the CLOUD Act of 2018; and the current EU/U.S. Data Privacy Framework.

With the current attention on TikTok and other Chinese-based companies, there is a risk that ill-considered limits will have harmful spillover effects on U.S. national interests. Privacy and national security arguments to wall off Americans' data or ban platforms entirely should take into consideration the consequences of doing so that go beyond a national security rationale. Such a U.S. blocking approach makes it more challenging for U.S. firms to push back against rising digital sovereignty in the EU, India, and globally in ways that hurt trade and undermine relations with those nations. It also weakens cooperation with allies by making it more difficult to effectively share data for law enforcement, intelligence, cybersecurity, health research, and other common purposes.

While we provide a framework for analyzing these important issues, we do not presume to have all the facts needed to make comprehensive policy recommendations. One path worthy of consideration for those who do have such insight is to enact the sort of comprehensive privacy legislation Congress has considered, perhaps with targeted provisions limiting data flows in certain circumstances and addressing the most serious risks from data brokers. Greater attention to the details of such an approach is beyond the scope of this article. Our hope instead is that this framework can serve as a foundation, useful to those across the political spectrum, that can help determine the most effective approach for meeting the multiple goals of U.S. policy.

Samm Sacks is a Senior Fellow with New America's International Security Program and the Yale Law School Paul Tsai China Center. She is a Senior Fellow for Asia with the Cross-Border Data Forum. She also advises corporate clients on China's technology regulations.

Peter Swire is the J.Z. Liang Chair in the Georgia Tech School of Cybersecurity and Privacy and Professor of Law and Ethics in the Georgia Tech Scheller College of Business. He is Research Director of the Cross-Border Data Forum and senior counsel with Alston & Bird, LLP.

The views expressed in this report are those of the authors alone, and do not represent the views of any organization.