ADDRESSING THE DATA SECURITY RISKS OF US-CHINA TECHNOLOGY ENTANGLEMENT

SAMM SACKS

EXECUTIVE SUMMARY

U.S.-China technology interdependence creates a suite of challenges for cross border data flows, data privacy, and data security. These challenges extend beyond the traditional risks of cyber espionage and protecting intellectual property (IP) to daunting new problems in managing the vast quantities of data created by digital technologies that underpin the global economy. The right way to address these issues, however, requires a broader approach than narrowly focusing on them within the U.S.-China technology conflict. Instead, it is time for the United States to propose a holistic and comprehensive vision for internet governance.

The value of data is realized when it is flowing, but the right safeguards must be in place. Rather than create new sovereign borders around data or one-off bans on Chinese companies, U.S. policymakers must put forward a U.S. vision of internet governance to create a more privacy protective, secure, and open internet in its own right, regardless of China's actions. Anne-Marie Slaughter has also argued for an open international order, but she writes that problems arise when we are "too connected, not connected enough, or connected in the wrong ways to the wrong people or things."[1] The challenge is to create a system in which the United States connects and disconnects in the right places. Below are the main pillars of what such system should look like:

- Pass a comprehensive federal privacy law with strong enforcement to manage how all companies collect, retain, and share data.
- Create a multilateral approach focused on allowing certain kinds of commercial data to flow, creating incentives for countries whose data regimes meet agreed upon thresholds, yet without blocking data flows to those who do not.
- Develop a targeted way to evaluate the risks posed by access to different kinds of data in various transactions, because not all data has the same levels of sensitivity, and it is important to distinguish between national security and privacy risks.
- Create policy that works in coordination with the development of technical solutions (e.g., encryption, federated learning, etc) to make security possible in low trust environments, recognizing that the world is interconnected, and it will not be possible to fully disconnect from networks utilizing Chinese equipment.

Now is the time to recapture U.S. global leadership in setting the rules for governing emerging technologies fueled by data. Inaction will mean ceding leadership to Europe, China, and other governments as these rules are in incipient stages and the digital economy reshapes the world.

THE PROBLEM

The distinction between data privacy and national security is blurring in a technology standoff between the U.S. and China. Data has become the great power competition of our time, driven by who creates it, who owns it, with whom its shared, and who writes the rules. There is a growing bipartisan consensus that the U.S.-China rivalry will define this century, with a race over technology as the battleground, and that the way to win is for the United States to erect more walls to protect our crown jewels from Beijing.

In the most recent and visible manifestation of this data conflict, the Trump administration invoked the International Emergency Economic Powers Act (IEEPA) to ban "transactions" between U.S. entities and the parent companies of TikTok and Wechat on August 6.[2] Roughly a week later, he directed the Committee of Foreign Investment in the United States (CFIUS) to compel ByteDance to divest itself of TikTok.[3] From the perspective of the national security community, the risk is less about Beijing using data on individual TikTok users for coercion or blackmail and more about the potential use of that data, if integrated with other datasets, by Beijing's security apparatus to perform link analysis or train machine learning systems in ways that could more precisely target and manipulate Americans.

A flurry of proposed legislation also seeks to address these risks by requiring that apps disclose their country of origin[4] or stopping U.S. citizen data from flowing to countries deemed adversaries.[5]

The list of Chinese companies facing greater U.S. government scrutiny over data security and China is growing. In January, the U.S. Department of the Interior (DoI) issued an order to ground its entire drone program because of concerns that data could be sent to China since the majority of the DoI's fleet of drones are either made by the Chinese drone maker DJI or with components from other Chinese suppliers.[6] In 2019, CFIUS ordered the Chinese gaming company Beijing Kunlun Tech to divest its ownership of the gay dating app Grinder because of concerns that Beijing could combine data on personal relationships from Grindr with what it is presumed to have obtained from the Office of Personnel Management data breach of over 21 million U.S. national security personnel records.[7]

The risks cut two directions: not only security concerns that U.S. citizen data could be accessed by the Chinese government but also ethical concerns over the way in which U.S. firms operating inside of China handle Chinese citizen data. Apple has faced criticism for storing encryption keys in China for iCloud user accounts, potentially making it vulnerable to access demands under China's legal system.[8] Nearly two decades ago, Yahoo became the posterchild for a worst-case scenario when the company turned over email content to Chinese authorities that resulted in a ten year jail sentence for a dissident.[9]

Taken together, these different controversies reveal a tangle of issues impacting civil liberties, national security, and U.S.-China technology competition. The complexity is compounded by the fact that they are occurring at a moment when we are shoveling more data to technology companies in the virtual world of the COVID lockdown, while U.S. social media platforms like Facebook and Twitter are shaping public information in ways that impact election security and public health.

Trying to protect data by constructing walls around it will not make data any more secure, nor will it help the U.S. to compete more effectively with China. This is a 20th century approach to solve a 21st century problem. The power that comes from data is not zero sum, because its value is realized when it is flowing rather than being locked inside the borders of states. Data requires an entirely new way of conceptualizing power — one that recognizes the need for data to flow but also creates the proper safeguards since openness can be exploited by government surveillance and corporate profit. This is the dilemma of an open data world.

OBJECTIVES

Data should flow freely around the world to preserve cross border digital trade, not restricted based on geography.[10] In the next five years when half of the global economic output will be created digitally,[11] there is much good that will come from ensuring that data is combined and shared across borders. A Deloitte report for the European Commission found that data flows would generate an additional 4% of gross domestic product growth by 2020.[12] Numerous economic models show that data flows are the lifeblood of the modern economy, underpinning international trade by sending consumer data across borders and allowing smaller businesses in far flung regions of the world to reach vastly bigger markets over the internet.

To understand why this is the case, it is important to think about what will happen in a world in which countries do not allow data to cross borders. It would be a world in which countries do not share data needed to decode how immune systems respond to COVID-19 to develop treatments and a vaccine or analyze how thousands of genes fight cancer.[13] Where information systems are more vulnerable to hackers. Where repressive governments around the world have easier pathways to surveil and crack down on dissidents when they demand data be stored locally in easy reach of domestic police. Where the data collected from the sensors on aircraft flying around the world does not get sent back to a central location to be combined and analyzed for safety.[14] Where a consumer appliance company cannot weave together information from its research and development center in Japan with parts sourced from South Korea and China, sent to be manufactured in Taiwan, and distributed to Singapore and Brazil.[15]

The United States must step up to lead a new international order based on interconnection and turn the tide against the rising trend of countries seeking to retain this vital new currency within their borders. The problem is that openness also can be exploited, posing legitimate risks from a privacy and national security perspective.

We must create the right safeguards to account for national security and privacy risks that accompany an interconnected world. The Justice Department warned that Google's planned undersea cable linking the U.S. with Hong Kong would expose data flowing through those networks to spying by the Chinese government. What was meant to be a data hub linking the U.S. across Asia could allow data to be siphoned off to China's intelligence services. Huawei's dominance in telecommunications infrastructure could allow the Chinese government to intercept communications crossing those networks or disrupt or shut off connectivity given that everything from water to transportation systems will rely on software in the future. Open data flows are not just exploited by governments, either. In her book *The Age of Surveillance Capitalism*, Shoshana Zuboff argued that companies vacuuming up data for profit threaten democratic freedoms. She said in an interview that "If we are treated as a mass of 'users', to be herded and coaxed, then this promise becomes meaningless. I am a distinctive human. I have an indelible crucible of power within me. I should decide if my face becomes data, my home, my car, my voice becomes data. It should be my choice."[16]

Anne-Marie Slaughter has also argued for an open international order, but she writes that problems arise when we are "too connected, not connected enough, or connected in the wrong ways to the wrong people or things."[17] There are sometimes legitimate reasons to close off, but the goal is to avoid launching a race to bottom with countries hoarding their data inside their borders or undermining innovation with data as a force for good. It is critical to be selective about the kind of guardrails and where they belong.

We want to be in a strong position to compete effectively with China. U.S. actions to respond to data security risks posed by the Chinese government are not occurring in a vacuum. The policy approach of the United States should be tailored to account for the fact that technology competition with China will play out not only in the United States and China but also in other places, from India to Europe. How the U.S. government responds to Chinese companies operating in the United States will have ramifications for whether other countries are willing to accept an American vision of data governance.

Moreover, the ability of U.S. firms to maintain a high rate of innovation depends on access to global markets, talent, and large and diverse international datasets. An increasing obstacle to the ability of U.S. companies to operate internationally — beyond China — is rising data sovereignty elsewhere, from Europe to India to Vietnam. If U.S. firms cannot transmit data out of the countries in which they operate overseas, they lose access to the value of creating international datasets. This directly impacts economic growth and AI innovation because of the ways large, diverse datasets are core to building AI applications that work across a variety of geographies, languages, cultures, and demographics.

The U.S. must recapture global leadership in setting the rules for digital technologies. Inaction on federal privacy law and the creation of a comprehensive approach to data security and privacy will mean ceding leadership to Europe, China, and other governments at a moment when the rules for governing emerging technologies are in early stages.

The path we are on now will strengthen China's leadership in global technology governance. By compelling ByteDance to sell TikTok to a U.S. company, the U.S. government has legitimized China's own model, which requires foreign cloud service providers to take a minority share in a partnership with a Chinese company that will run their services in China. Our actions have set the stage for others around the world to do the same. Already, Chinese think tanks and scholars are promoting this approach as the solution for creating a global cloud governance model that allows for data sovereignty. The U.S. needs to step up to offer an alternative vision for data governance to preserve an open and secure global internet.

RECOMMENDATIONS

Looking back at different junctures in history, there are short periods of time in which the rules that are written create an order for the forthcoming several decades. In the aftermath of World War II, the institutions and rules ushered in the integration of trade, capital, and labor that underpin globalization as we know it today. We are now at one of these inflection points, but this time what is at stake is our own data and whether it will be a force for empowerment or a resource to exploit. If we can get this right, the U.S. has a chance to regain its lost leadership to create a more privacy protective, secure, and open internet.

The challenge is not just how the U.S. should most effectively compete with China, but part of a much bigger set of questions about how to secure data in an interconnected world and protect civil liberties and national security while also enabling data to fuel economic and technological development as it crisscrosses the world. Some policy solutions are specific to China, and some are much broader.

1. Pass a comprehensive federal privacy law that comes with strong enforcement mechanisms.

The U.S. needs to develop rules not limited to Chinese companies operating in America, but also to govern how all companies collect, retain, and share their data. Instead of playing a game of whack-a-mole against a rotating cast of Chinese tech companies, the U.S. would be wise to spend more time developing legislation and standards for how all companies, regardless of what country they come from, protect online privacy and secure data. No company should have access to and then retain sensitive data in the first place that could then be transmitted to a government that could employ it to do harm or be hacked by state actors. With such criteria in place, the next TikTok or app in question could be reviewed against a clear set of criteria in order to use U.S. data.

If policy makers do not adopt a federal privacy law with meaningful enforcement, U.S. citizen data held by all unregulated private companies — not just Chinese companies — will be more vulnerable to breaches by state hackers, as well. For example, Equifax's many security issues are well documented, such as the company's failure to patch known vulnerabilities that ultimately left exposed the data of 145 million Americans. But the hack was also conducted by a Chinese government entity with sophisticated hacking capabilities and access to considerable state resources. Setting minimum standards for what data can be collected and retained by all companies will help protect U.S. personal data, regardless of whether the risk is exacerbated by a state-sponsored hacker, a data seller, or a private company transferring the data to China.

2. Create a multilateral approach focused on commercial data flows, creating incentives for countries whose data regimes meet agreed upon thresholds, yet without blocking data flows to those who do not.

A number of recent initiatives[18] are advancing proposals for a kind of democratic technology alliance as a counterweight to China. There is no question that a multilateral approach is needed to facilitate cross border data transfers underpinning digital trade while also increasing pressure on Beijing to make reforms. Such a multilateral approach, however, will only be effective if the following considerations are taken into account.

First, these coalitions or agreements should not be limited to democracies since the future of the digital economy is likely to be shaped in places from Brazil to countries across Southeast Asia where the digital economy is surging.[19]

Second, one of the first orders of business will be to address the digital chasm between Europe and the United States. The transatlantic divide is among the greatest obstacles not just to preserving free data flows around the world, but also to our ability to work constructively with European partners as we compete with China. In July, the Court of Justice of the European Union invalidated the EU-US Privacy Shield, the established mechanism to transfer personal data from the EU to the U.S. (the case is known as Schrems II).[20] The ruling found insufficient protections in U.S. surveillance law, making clear the seriousness of EU concerns over U.S. government access to data. We must reach a broader agreement with Europe on best practices and norms regarding government access to data. These issues further underscore the importance of the U.S. getting its own house in order on data governance before we can even begin to collaborate in a forum with other democracies.

Finally, a multilateral approach should be based on creating a system of incentives rather than excluding countries like China from participation. Prime Minister Shinzo Abe's initiative to create a framework for the "free flow of data with trust" among likeminded governments is based on the idea of cutting off data flows to China and others. Instead, the U.S. could lead the way in setting up a certification system that would extend certain benefits to countries whose data regimes and companies meet certain clear criteria for data protection. The OECD privacy guidelines, for example, could serve as a reference in creating a baseline for commercial data flows.[21]

3. Develop a targeted way to evaluate the national security risks of different kinds of data involved in various transactions, because not all data has the same levels of sensitivity.

Some kinds of data are more sensitive alone or in combination and need to stay within the physical borders of the U.S. — some kinds of financial, location, children's, and health and genomic data, and data related to the military, for example. There are cases where walls need to be erected around data while keeping other kinds of data flowing. As part of assessing different security risks associated with access to different kinds of data, national security and privacy risks must be distinguished, as the line between the two has become blurred.

There are sometimes legitimate reasons to keep some kinds of data stored on local servers inside sovereign borders, either in United States or elsewhere. There are ways to store data that avoid launching a race to bottom with countries hoarding their data inside their borders. Being selective about the kind of guardrails and where they belong is critical. There are two examples in the United States of legitimate reasons to keep our data inside the physical border: 1) The Defense Department has deemed that some kinds of national security data should remain on local servers; and 2) After the financial crisis of 2008, financial regulators determined that certain financial data must be kept in the United States to be easily accessible for auditors to ensure America does not confront similar circumstances again.

The mere fact that a Chinese company handles U.S. citizen data in and of itself may not necessarily warrant putting sovereign walls around the company in the form of banning transactions or blacklisting that specific company. The risks to U.S. national security should be evaluated based on an investigation to determine (a) what kind of U.S. citizen data is being accessed (for example, metadata, images, geographic data, or critical infrastructure data), (b) how that data is being used and what data protection measures have been implemented to protect the rights and interests of U.S. consumers, and (c) with whom that data is being shared and through what mechanisms. If, based on the outcomes of such an evaluation, the U.S. government cannot verify that the interests and rights of U.S. consumers will be protected, then that specific company should be prohibited from storing and sharing U.S. personal data.

4. Find technical solutions to incorporate security into low trust environments.

Policies that work in coordination with the development of technical solutions to create security in low trust environments must be created, recognizing that our interconnected world does not make it possible to fully disconnect from networks made up of Chinese equipment. Former Deputy Director of National Intelligence Sue Gordon told *The New York Times* that even in the best of circumstances, the reality is that American data will flow over Chinese networks, so we have to figure out how to create security in so-called dirty networks.[22] There is a role for encryption, where the data is scrambled when it is stored or as it is transmitted. There is also a role for other techniques like federated learning to keep data anonymous even as companies use it train their artificial intelligence systems to get smarter. Specific sectors provide other examples like the use of a shallow sequencing in biotechnology, for example, where only part of a genome sequence is used in order to employ the mountains of human genetic data needed to develop cures for diseases. These kinds of technical solutions must go hand-in-hand with policy solutions, especially when it comes to sharing certain kinds of sensitive data like health or children's data.

CONCLUSIONS

Now is the time to recapture U.S. global leadership in setting the rules for governing emerging technologies and data privacy when these rules are in early stages. The United States has an opportunity to set the standards for protecting the flow of data that has underpinned economic growth and the free flow of information around the world by ensuring that the right safeguards are implemented. Doing do will allow America to reap the benefits of an open data flow world while minimizing any potential harm to both national security and privacy.

The U.S. government needs a more effective strategy to protect U.S. personal data than one-off bans on companies or the destinations of their data. The U.S. needs to address legitimate national security risks where they exist and also as one part of a broader U.S. initiative on comprehensive data privacy and higher standards for cybersecurity for all companies (whether American or foreign). These efforts should not name China as a bad actor, but, instead, they should set a high bar for all companies to meet in managing their data and build incentives for countries to sign on. Failure to establish a compelling vision for U.S. internet governance will only allow more space around the world for Beijing's vision for the internet to flourish.

REFERENCES

1 Anne-Marie Slaughter, "How to Succeed in a Networked World: A Grand Strategy for the Digital Age," *Foreign Affairs* 95 no. 6 (November/December 2016), 76-89.

2 Donald Trump, "Executive Order 13942, of August 6, 2020, Addressing the Threat Posed by TikTok," Washington: White House. https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/ and "Executive Order 13943, of August 6, 2020, Addressing the Threat Posed by WeChat," Washington: White House. https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-wechat/.

3 Donald Trump, "Order Regarding the Acquisition of Musical.ly by ByteDance Ltd," Washington: White House. https://www.whitehouse.gov/presidential-actions/order-regarding-acquisition-musical-ly-bytedance-ltd/.

4 Justine Coleman, "Senators Introduce Bipartisan Bill to Mandate Digital Apps Disclose Country of Origin," *The Hill*, September 23, 2020, https://thehill.com/homenews/senate/517823-senators-introduce-bipartisan-bill-that-would-mandate-digital-apps-to.

5 "Senator Hawley Introduces Bill to Address National Security Concerns Raised by Big Tech's Partnerships with Beijing," Office of Senator Josh Hawley, November 18, 2019, https://www.hawley.senate.gov/senator-hawley-introduces-bill-address-national-security-concerns-raised-big-techs-partnerships.

6 "Secretary Bernhardt Signs Order Grounding Interior's Drone Fleet for Non-Emergency Operations," U.S. Department of the Interior, January 29, 2020, https://www.doi.gov/pressreleases/secretary-bernhardt-signs-order-grounding-interiors-drone-fleet-non-emergency.

7 Evan Perez, "FBI Arrests Chinese National Connected to Malware Used in OPM Data Breach," CNN, August 24, 2017, https://www.cnn.com/2017/08/24/politics/fbi-arrests-chinese-national-in-opm-data-breach/index.html.

8 Stephen Nellis and Cate Cadell. "Apple Moves to Store ICloud Keys in China, Raising Human Rights Fears," Reuters, February 24, 2018, https://www.reuters.com/article/us-china-apple-icloud-insight-idUSKCN1G8060.

9 https://www.nytimes.com/2012/09/01/world/asia/wang-xiaoning-chinese-dissident-in-yahoo-case-freed.html.

10 Robert Knake, *Weaponizing Digital Trade*, Council on Foreign Relations, Special Report No. 88 (September 2020), https://cdn.cfr.org/sites/default/files/report_pdf/weaponizing-digital-trade_csr_combined_final.pdf.

11 Josh Kallmer, "Dear World Leaders: Tear Down Your Digital Walls," German Marshall Fund, December 12, 2017, 3. https://www.gmfus.org/publications/dear-world-leaders-tear-down-your-digital-walls.

12 Joshua P. Meltzer and Peter Lovelock, "Regulating for a digital economy: Understanding the importance of cross-border data flows in Asia," (Washington, D.C., The Brookings Institution, March 20, 2018), https://www.brookings.edu/

research/regulating-for-a-digital-economy-understanding-the-importance-of-cross-border-data-flows-in-asia/ and "Measuring the economic impact of cloud computing in Europe," January 10, 2017, https://ec.europa.eu/digital-single-market/en/news/measuring-economic-impact-cloud-computing-europe.

13 "Data Science," Fred Hutch Cancer Research Center, https://www.fredhutch.org/en/research/research-areas/data-science.html.

14 Kallmer 4.

15 Ibid.

16 Joanna Kavenna, "Shoshana Zuboff: 'Surveillance Capitalism Is an Assault on Human Autonomy,'" *The Guardian*, October 4, 2019, https://www.theguardian.com/books/2019/oct/04/shoshana-zuboff-surveillance-capitalism-assault-human-automomy-digital-privacy.

17 Anne-Marie Slaughter, "How to Succeed in a Networked World: A Grand Strategy for the Digital Age," *Foreign Affairs* 95 no. 6 (November/December 2016), 76-89.

18 Knake, "Weaponizing Digital Trade." See also Jared Cohen and Richard Fontaine, "Uniting the Techno Democracies," *Foreign Affairs* 99 no. 6, (November/December 2020), https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies and "Common Code: An Alliance Framework for Democratic Technology Policy," Center for a New American Security, forthcoming.

19 "E-Conomy SEA report 2019: Powering Southeast Asia's $100 billion Internet economy," PRNewswire, October 3, 2019, https://www.prnewswire.com/news-releases/e-conomy-sea-report-2019-powering-southeast-asias-100-billion-internet-economy-300930442.html.

20 Ryan Blaney, "One Cross-Border Mechanism Invalid, Another Upheld: Thoughts after the CJEU's Schrems II Decision," *National Law Review*, July 21, 2020, https://www.natlawreview.com/article/one-cross-border-mechanism-invalid-another-upheld-thoughts-after-cjeu-s-schrems-ii. See also Jennifer Daskal, "What Comes Next: The Aftermath of European Court's Blow to Transatlantic Data Transfers," *Just Security*, July 17, 2020, https://www.justsecurity.org/71485/what-comes-next-the-aftermath-of-european-courts-blow-to-transatlantic-data-transfers/.

21 "The OECD Privacy Framework," Organisation for Economic Co-operation and Development, 2013, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

22 David Sanger, and Julian Barnes, "Is TikTok More of a Parenting Problem Than a Security Threat?" *The New York Times*, August 07, 2020, https://www.nytimes.com/2020/08/07/us/politics/tiktok-security-threat.html.