TESTIMONY OF SAMM SACKS
Hearing: "How America Competes to Win the Future Versus China"
House Energy & Commerce Subcommittee on Innovation, Data, and Commerce

February 1, 2023

Chairman Bilirakis, Ranking Member Schakowsky, Chair Rodgers, Ranking Member Pallone, and Members of the Subcommittee, thank you for the opportunity to testify today.

I am a Senior Fellow at Yale Law School's Paul Tsai China Center and at New America's International Security Program. I also am a Senior Fellow for China with the Cross Border Data Forum, a non-profit group that addresses international data transfer policy issues. I have worked as an analyst of Chinese data and technology policies for the last decade, in the U.S. national security community, and in the private sector. I also advise corporate clients on China's technology policies.

Today I will focus my testimony on technology competition with China, particularly in the context of global cross-border data flows.

While my expertise focuses on China, my view is that the most effective solutions for strengthening U.S. competitiveness and U.S. leadership in governing emerging technologies requires an approach that is more comprehensive than our response to any single country. Some of these challenges do require tools that are specific to risks posed by China, but these policy challenges are bigger than China. Passing comprehensive federal privacy law that addresses how all companies collect, transfer, and process data will enhance competition while also addressing harms regardless of where risk originates. U.S. lawmakers have an opportunity to address transnational security threats while also advancing a more secure, ethical, and democratic global internet in its own right.

China's Evolving Data Regime

Data as a Strategic Asset

The Chinese leadership has embarked on an ambitious national data strategy with the goal of acquiring, controlling, and extracting value from large volumes of data. My previous testimonies provide further details about China's approach, including the Data Security Law and Personal Information Protection Law.[1] Beijing has elevated the concept of data as an economic and strategic asset[2], centralizing state power over information flows:

- An April 2020 directive issued by the State Council and Central Committee of the Chinese Communist Party (CCP) designates data as the fifth factor of production—after land, labor, capital, and technology.[3] At the National People's Congress in March 2021, the outline of

[1] https://www.finance.senate.gov/download/12072021-sacks-testimony; https://www.judiciary.senate.gov/meetings/protecting-americans-private-information-from-hostile-foreign-powers; https://www.judiciary.senate.gov/download/sacks-testimony. For further readings on China's data laws and policies, please see: Jamie Horsley, "How Will China's Privacy Law Apply to the State?" https://www.newamerica.org/cybersecurity-initiative/digichina/blog/how-will-chinas-privacy-law-apply-to-the-chinese-state/ and additional resources available by DigiChina Project, Stanford Cyber Policy Center, https://digichina.stanford.edu/.

[2] The concept of data as a strategic resource is not new in China. It appears in the Big Data White Papers (2014, 2016, 2018) published by an influential think tank under the Ministry of Industry Information Technology (MIIT), as well as in the Big Data Strategy (2017). The 13th Five Year Plan (2016–2020) calls for "fully implementing the promotion of the big data development initiatives and accelerating the sharing of data resources and development of applications, to assist in industrial transformation and upgrading . . . "

[3] Ouyang Shijia, "New guideline to better allocate production factors," April 10, 2020, China Daily, https://www.chinadaily.com.cn/a/202004/10/WS5e903fd7a3105d50a3d15620.html.

the 14th Five-Year plan called for “improving the market of data factors” (健全数据要素市场), and stressing the need to unlock the value of data to fuel the digital economy.[4]

- On November 30th of 2021, China’s Ministry of Industry and Information Technology released the 14th Five Year Plan (2021-2025) for China's big data industry. The plan defines big data as a strategic emerging industry, slated for greater state support to unlock the value of data. State supporting measures focus on expanding “international cooperation” between Chinese and foreign “big data services” companies in standard setting and research & development (R&D), and encourage multinationals to set up R&D centers in China. By 2025, the plan calls for China to set up new mechanisms to facilitate China’s role in data trading and cross-border transfers. (建立数据资源产权、交易流通、跨境传输和安全等基础制度和标准规范) and “encourages Chinese firms to offer big data services in Belt and Road Initiative (BRI) countries and regions."

Beijing is also taking steps to centralize state control over data by breaking down silos or data islands across different government ministries and between the government and private companies, which have long plagued the government’s ability to aggregate and coordinate data. Barriers to data sharing are due to a variety of reasons. Chinese companies are reluctant to share their data as valuable commercial intellectual property, while government agencies often push back against one another’s access requests, guarding their data as a form of political power.[5] These data silos may be less of a

[4] Sina Online, “What Is the Meaning of the ‘14th Five-Year Plan’ Outline (Draft) to Improve the Market of Data Elements? (“十四五”规划纲要（草案）提出健全数据要素市场有何深意),” March 5, 2021, https://finance.sina.com.cn/china/2021-03-05/doc-ikftssaq1688850.shtml.

[5] Yuan Yang and Nian Liu, “Alibaba and Tencent refuse to hand loans data to Beijing,” Financial Times, September 18, 2019, https://www.ft.com/content/93451b98-da12-11e9-8f9b-77216ebe1f17; Martin Chorzempa, Paul Triolo, Samm Sacks, “China’s Social Credit System: A Mark of Progress or a Threat to Privacy?” Peterson Institute for International

problem for data sharing than in the past, however, given the way that datasets were integrated to form the basis for the system of health apps used for COVID control.[6] Platforms aggregated information from multiple sources and across localities, including: the state-owned telecom companies, vaccination and testing from National Health Commission, and public transportation sources, and other government platforms containing public records.

Automotive Data

Beijing has also prioritized certain data-intensive sectors slated for greater state support and policy focus. The auto industry was among the first to be targeted by the Cyberspace Administration of China (CAC) for stricter data regulations.[7] The "Regulations on Management of Automotive Industry Data Security" (took effect October 2021) outline which types of data collected by smart cars are designated as belonging to categories that are subject to increased security protections. The regulations lay out obligations for handling different types of data collected or generated by the vehicle—including about the surrounding environment, drivers and passengers, and infrastructure—which is of use for entities ranging from manufacturers to Internet platforms.

Economics Policy Brief, June 2018, https://www.piie.com/publications/policy-briefs/chinas-social-credit-system-mark-progress-or-threat-privacy; Samm Sacks testimony before Senate Judiciary Committee hearing "Dangerous Partners: Big Tech and Beijing," March 4, 2020, https://www.judiciary.senate.gov/imo/media/doc/Sacks%20Testimony.pdf; Amba Kak and Samm Sacks, "Shifting Narratives and Emerging Trends in Global Data Governance Policy," AI Now and Yale Law School Paul Tsai China Center Policy Report, August 21, 2021, https://law.yale.edu/sites/default/files/area/center/china/document/shifting_narratives.pdf.

[6] Mia Zhong, "China's COVID Apps: A Primer," *DigiChina,* https://digichina.stanford.edu/work/chinas-covid-apps-a-primer/.

[7] Samm Sacks, Kendra Shaefer, Xiaomeng Lu, "With Auto Data, China Buckles In for Security and Opens Up for Future Tech," *DigiChina,* https://digichina.stanford.edu/work/with-auto-data-china-buckles-in-for-security-and-opens-up-for-future-tech/.

My assessment is that foreign automakers would have more difficulty gaining approvals for arrangements that would allow them to gather data from cars on Chinese roads and incorporate it into R&D efforts conducted outside China. For instance, two weeks after the auto data provisions were released, Tesla announced that all data generated by vehicles sold in China will be stored locally.

Driving the regulation is a recognition by China's leadership that automotive data holds significant economic value and creates security and privacy risks. It also illustrates the ways in which the Chinese government is moving forward in articulating a vision for how to control and manage data at a granular level, sector-specific level.

Risks to the United States

What are the implications for the United States of China's domestic and international efforts to acquire and make use of data as a strategic economic asset? It is important to distinguish national security and economic competitiveness risk.

From a national security perspective, potentially the concerning uses of aggregated data by the Chinese government would primarily impact only individuals with national security clearances or with access to critical infrastructure. Beijing is already presumed to have sensitive national security information from the theft of personnel records of roughly 21 million individuals from the U.S. Office of Personnel Management; travel information from a cyber attack on Marriott hotels covering roughly 400 million records; and credit data from Equifax on roughly 145 million people.[8] If additional sources of personal data such as location, social media, or pattern of life data were to be acquired 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 target individuals in sensitive government national security positions or military personnel for manipulation, blackmail, or other forms of coercion.

The impact on economic competition between the United States and China may be potentially more significant, however. Access to large datasets collected abroad provides also 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. Better tailored AI products and services strengthens the ability of Chinese firms to compete for market share with U.S. firms. The competition is playing out less in each other's countries, as Beijing and Washington pursue economic decoupling policies, but increasingly in other parts of the world from Europe to the Asia, where the competition for market share is increasing. Chinese firms access to more data for AI training models will provide fuel as AI and Quantum become differentiators for the 21st century and beyond.

Recommendations

The most significant step U.S. lawmakers can take to strengthen U.S. global competitiveness and enhance privacy protections is to pass comprehensive federal privacy law (American Data Privacy

[8] "China's Collection of Genomic and Other Healthcare Data from America: Risks to Privacy and U.S. Economic and National Security," National Counterintelligence and Security Center Fact Sheet, February 2021.

and Protection Act) to address the harms outcomes of all data processing, regardless of country of origin. Setting high standards on what data can be collected and retained by all companies will help protect U.S. personal and other sensitive data. Inaction by the United States means ceding leadership and influence in setting international standards to both Europe and China.

Bans on Chinese software applications are not an effective way to secure Americans' data. Even if TikTok were American-owned, for example, it and its competitors could still legally sell data openly to data brokers that could transmit it to China's security services. As a result, American data is shockingly exposed and will remain that way so long as restrictions on data flows only focus on specific companies from countries deemed adversaries.

In addition, the United States should work with like-minded governments to develop a common set of standards that would allow data to flow—building off of the concept of "data free flows with trust" put forward by Japan in the Osaka Track of the G-20.[9] A multilateral approach should be based on creating a system of incentives for compliance. The objective would be to establish an interoperable data framework encouraging other countries in the world to set similar but not identical standards. The United States could lead the way in setting up a certification system that would extend benefits to countries whose data regimes and companies meet certain clear criteria for data protection. The Organization for Economic Cooperation and Development (OECD) privacy guidelines, for example, could serve as a reference in creating a baseline for commercial data flows.[10] The OECD Declaration on Government Access to Personal Data held by Private Sector Entities

[9] Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows, World Economic Forum, https://www.weforum.org/whitepapers/data-free-flow-with-trust-dfft-paths-towards-free-and-trusted-data-flows/.
[10] "The OECD Privacy Framework," Organisation for Economic Co-operation and Development, https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

on is an important step.[11]

I'd also like to note the potential for the Global Cross Border Privacy Rules Forum, a data transfer alliance that requires companies to certify to common standards for privacy protection and enables cross-border transfers for those certified companies. This U.S.-backed system offers the potential to address many facets of protecting American data, as it not only takes into consideration the country where data is traveling, but also requires that companies certify to a government-backed standard to be able to transfer data.

Such an approach creates a coalition of allies sharing data with the United States. The ability of U.S. firms to maintain a high rate of innovation depends upon access to global markets, talent, and international datasets. If U.S. firms cannot send data out of countries in which they operate overseas, this directly impacts economic growth and AI innovation that are core to building applications that work across a variety of different geographies, languages, cultures, and demographics. As the technology competition between the United States and China increasingly plays out less in each other's countries than in third countries around the world, data will fuel U.S. technological leadership that is vital to playing offense.

Technical measures to ensure that data is collected in a privacy protective way also should be part of the solution. Congress and the Administration should work with American companies to create incentives to develop privacy preserving technologies— which allow for computing on data without seeing it—and implement them in an open-source way available to everyone. Federated learning

[11] https://www.oecd.org/newsroom/landmark-agreement-adopted-on-safeguarding-privacy-in-law-enforcement-and-national-security-data-access.htm.

(which keeps the raw training data on the device) and differential privacy (providing data anonymization) are two examples. American companies are right now leading the global conversation on privacy preserving technologies and investment in these technologies by the government will enable companies of any size to implement these technological innovations.

Conclusions

I urge U.S. lawmakers to address national security risks by putting forward an affirmative vision for U.S. data governance. ADPPA marks an important step in this regard that merits further attention and discussion. Inaction will make United States less secure, less prosperous, and less powerful, and allow more space around the world for CCP to set the rules and norms for technologies that will shape the future.