CONGRESSIONAL TESTIMONY: FOUNDATION FOR DEFENSE OF DEMOCRACIES

Senate Judiciary Committee
Subcommittee on Privacy, Technology, and the Law

Protecting Americans' Private Information from Hostile Foreign Powers

MATTHEW POTTINGER

China Program Chairman
Foundation for Defense of Democracies

Former U.S. Deputy National Security Advisor

Washington, DC
September 14, 2022

FDD
FOUNDATION FOR
DEFENSE OF DEMOCRACIES

www.fdd.org

Introduction

Chairman Coons, Ranking Member Sasse, and members of the Subcommittee, it's a privilege to appear before you today.

Xi's Data Vision

For years now, Washington's engagement on data issues has been dominated by thorny disputes, on Capitol Hill and with European regulators, over privacy rules for America's tech giants. Meanwhile, the even greater data threat from Beijing has largely gone unaddressed.

From his earliest days in power, Chinese Communist Party (CCP) General Secretary Xi Jinping made clear that "whoever controls big data technologies will control the resources for development and have the upper hand."[1] To the CCP, data is not merely information. Rather, it is an instrument Beijing uses to improve its military capabilities, its surveillance state, and its bid for commercial dominance in the technologies of the future. The personal data it captures is used to influence and intimidate, to reward and blackmail, and, ultimately, to divide and subvert.

Assembling dossiers on people and institutions, both foreign and domestic, has always been a mainstay of Leninist regimes. Today's challenge, which must be made central to America's China policy going forward, stems from Beijing's penetration and exploitation of digital networks worldwide and the CCP's growing ability to impose its will on cross-border data flows. This evolving threat poses risks not only to Americans' privacy but increasingly to our country's economic competitiveness and national security.

In testifying before the U.S. Senate Select Committee on Intelligence last year, William Evanina, who served as Director of the National Counterintelligence and Security Center, highlighted a startling finding about the extent of China's data grab: "It is estimated that 80% of American adults have had all of their personal data stolen by the CCP, and the other 20 percent most of their personal data."[2] The wellspring of this data is all of us. More specifically, it is our private health records and genetic sequences, our online preferences, our financial records, our legal documents, and the supply chains of our businesses, not to mention the terabytes of imagery and other data processed by our phones, our drones, and our autonomous vehicles.

For its part, the Biden administration has underscored the importance of data in our competition with Beijing. U.S. National Security advisor Jake Sullivan has said that America's "strategic competitors see big data as a strategic asset," and Washington "must see it the same way."[3] And

---

[1] Xifeng County People's Government, "习近平同志的大数据观 [Comrade Xi Jinping's Big Data View]," November 22, 2017. (http://www.xifeng.gov.cn/zwgk/zdlygk/dsjjsgl/201810/t20181028_62992041.html)

[2] William R. Evanina, "The Comprehensive Threat to America Posed by the Communist Party Of China (CCP)" *Testimony before the Senate Select Committee on Intelligence*, August 4, 2021. (https://www.intelligence.senate.gov/sites/default/files/documents/os-bevanina-080421.pdf)

[3] National Security Advisor Jake Sullivan, The White House, *Remarks at the National Security Commission on Artificial Intelligence Global Emerging Technology Summit*, July 13, 2021. (https://www.whitehouse.gov/nsc/briefing-room/2021/07/13/remarks-by-national-security-advisor-jake-sullivan-at-the-national-security-commission-on-artificial-intelligence-global-emerging-technology-summit/)

yet no visible American counterstrategy has emerged. The result, regrettably, is that China is already beating the United States and its allies when it comes to harnessing data to achieve commercial, technological, and military advantages.

China's drive for data control flows from the CCP's almost obsessive historical fixation on information and Xi's campaign to apply Marxist ideology to 21st-century conditions. In classifying data as a "basic and strategic resource," Xi has spent the last decade establishing the laws, regulatory mechanisms, and enforcement leverage necessary to ensure that data — in all its forms — is controlled, accumulated, and exploited to advance the strategic interests of the single-party regime seated in Beijing.[4]

And, while Beijing's regulatory moves were initially directed against Chinese companies and the country's 1.4 billion citizens, China's campaign now extends to a wide range of international targets, including all of us participating in today's hearing.

A Fast-Expanding Legal Regime

One thing China has not done is camouflage its global data ambitions. In public speeches going back to 2013, Xi has likened big data's potential to the exalted status Mao Zedong once gave to indigenous Chinese oil production in the 1950s.

Xi correctly sees data as an enabler of China's national power and economic progress, one capable of improving the delivery of government and commercial services. These advancements are, in part, intended to alleviate the financial, social, and productivity pressures resulting from China's rapid economic slowdown — pressures that are set to intensify as the party confronts China's steep demographic decline. Already, Beijing's investments have yielded some impressive results, with China now ranked among the top three countries for artificial intelligence vibrancy, according to Stanford University's annual Artificial Intelligence Index.[5]

But China's AI prowess and centralized data regime have been put to use in ways that couldn't be more antithetical to human freedom. Most notably, it has been used to monitor, oppress, and incarcerate millions of ethnic and religious minorities, including the Uyghur population, which even the United Nations now recognizes is the target of probable crimes against humanity.[6] Beijing wants to export that data-driven surveillance technology and know-how to other autocratic governments around the world.

Just as important, Beijing's evolving data regime also advances its key aims of global propaganda, censorship, and influence, including Xi's stated goal of winning the digital "public

---

[4] "习近平带政治局集体学习 领导干部要学懂用好大数据 [Xi Jinping led the Politburo to collectively study leading cadres to learn how to make good use of big data]," *China Central Television* (China), December 10, 2017. (http://news.cctv.com/2017/12/10/ARTI3HNR1LMiMiNZKmr1NMD1171210.shtml)

[5] "Global AI Vibrancy Tool," *Stanford University Human-Centered Artificial Intelligence*, accessed September 13, 2022. (https://aiindex.stanford.edu/vibrancy/)

[6] Nick Cumming-Bruce and Austin Ramzy, "U.N. Says China May Have Committed 'Crimes Against Humanity' in Xinjiang," *The New York Times*, August 31, 2022. (https://www.nytimes.com/2022/08/31/world/asia/un-china-xinjiang-uyghurs.html)

opinion struggle."[7] Xi says he wants to enhance what he calls China's "discourse power" — that is, the party-state's ability to set and shape global narratives. It should concern free societies everywhere that the autocratic regime in Beijing now regulates the AI algorithms that are the "secret sauce" in Chinese-owned social media apps whose popularity is growing rapidly around the globe.

Beijing has invested heavily in developing a framework of overlapping hardware, software, network security, and data management solutions designed to will Xi's data vision into being. Beijing is also using the law to advance its strategy, aiming to ensure not only access but also de facto control over global data flows.

First came Beijing's 2017 National Intelligence Law. Then two laws passed in 2021 — the Data Security Law and the Personal Information Protection Law — that together embody Beijing's demand for unlimited state control over data and the entities that process it, even if they are located overseas.[8]

These laws assert Beijing's veto power over foreign governments' requests for data from China and criminalize compliance with U.S. or foreign sanctions against China that involve data. The result is that foreign firms operating in China, including many U.S. companies, must not only relinquish control over their data but must also accept a permanent limbo between Chinese and U.S. laws. In these cases, U.S. firms can comply with U.S. law, or they can comply with Chinese law, but not both. This is by Beijing's design. U.S. banks and tech companies operating in China have been the first to feel the effects of the CCP's digital coercion, but Beijing's primary target is the U.S. policy process itself.

Beijing will use its new data regime and threats of data reviews as coercive geopolitical levers while sanctions and counter-sanctions mount between the two governments. When Washington takes any action to restrict data or technology flows between the U.S. and China, U.S. policymakers should expect Beijing to retaliate against some U.S. target, adding greater pressure on U.S. entities and persons operating in China.

U.S. Counterstrategy and Recommendations

There are several steps the United States can take that would strengthen our position in light of Beijing's data strategy.

---

[7] President Xi Jinping, "言论方面要敢抓敢管敢于亮剑 [Dare to grasp, control, and show the sword in terms of speech]," *Address Before the National Propaganda and Ideological Work Conference*, August 19, 2013. (https://chinadigitaltimes.net/chinese/321001.html)

[8] Order of the President of the People's Republic of China No. 84, 2021 (http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml); 中华人民共和国个人信息保护法 [Personal Information Protection Law of the People's Republic of China], 2021. (http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml)

1. The Committee on Foreign Investment in the United States (CFIUS) should do more to block Chinese acquisitions of and investments in U.S. companies with sensitive data, while the new Information and Communications Technology and Services (ICTS) regime should block data flows that undermine national security. CFIUS has largely continued its stepped-up efforts, which began during the Trump administration, to review and restrict a wider range of would-be investments by Chinese entities in U.S. companies. Similarly, the Commerce Department has taken initial steps toward better regulating data-related trade and exchange by establishing the new ICTS regime, but implementation appears to have stalled.

2. Data Free Flow with Trust (DFFT), a blueprint put forward by the late Japanese Prime Minister Abe Shinzo in 2019, should be the basis for a new allied data policy. Washington is not alone in confronting China's digital dictatorship. Going forward, the United States and its democratic allies must promote enhanced data sharing among themselves while also limiting dangerous data flows to China. Such work will require that U.S. policymakers not only devise a comprehensive approach to data governance, one that protects Americans' data, but also lead an allied policy process that helps other rule-of-law societies do the same.

3. The U.S. must develop a tailored data denial strategy to curb the flow of sensitive U.S. and allied data to China that can be exploited by the CCP. Information and activity generated on high-risk social media platforms and mobile applications represent one vulnerability. The case of TikTok and its China-based parent company ByteDance is an important and urgent policy test, given mounting reports of exposure of U.S. user data to China. Any significant action to mitigate the national security and privacy risks posed by TikTok should be part of a broader effort that considers all Chinese-owned or -controlled apps and other means of potential data flow.

4. The U.S. should consider ways to restrict the sale of Americans' sensitive personal data to high-risk entities, including those controlled by or subject to the influence of the CCP. In April 2021, Director of National Intelligence Avril Haines acknowledged concerns over foreign adversaries getting "commercially acquired" personal data of Americans.[9] While some transactions related to the acquisition of and investments in U.S. companies holding sensitive data come under government review, existing CFIUS scrutiny does not extend to the commercial sale and export of data itself. Efforts in Congress to address this shortcoming are welcome.

5. Congress should encourage the adoption of standards for the protection of sensitive personal data held in the private sector. The work of establishing a domestic governance framework is critical to enabling effective governance abroad. Approaches like the congressionally-mandated Cyberspace Solarium Commission's recommendation that Congress "pass a national data security and privacy protection law establishing and standardizing requirements for the collection, retention, and sharing of user data" would add another layer of data protection against the threat posed by the CCP and other adversaries.[10]

---

[9] Drew Harwell, "Wyden urges ban on sale of Americans' personal data to 'unfriendly' foreign governments," *The Washington Post*, April 15, 2021. (https://www.washingtonpost.com/technology/2021/04/15/personal-data-foreign-government-ban/)

[10] Senator Angus King and Representative Mike Gallagher, "Cyberspace Solarium Commission," *Cyberspace Solarium Commission*, March 2020. (https://cybersolarium.org/wp-content/uploads/2022/05/CSC-Final-Report.pdf)

6. Apply Cyber Data Management Throughout the Federal Government. The FY22 NDAA required the "development of a policy and processes that secure the routing infrastructure within the Department of Defense." This is important given that the "CCP leverages technologies at the core of the global internet infrastructure to hijack foreign data to ensure it travels through Chinese-controlled servers."[11] Congress should pass new legislation mandating this cyber data management provision for the entire federal government. Efforts to reform the Federal Information Security Modernization Act (FISMA) are a good place to start.

Thank you for the opportunity to testify today. I look forward to your questions.

[11] Georgianna Shea and Trevor Logan, "It Is Time to Counter China's Data Strategy," *Foundation for Defense of Democracies*, January 12, 2022. (https://www.fdd.org/analysis/2022/01/12/it-is-time-to-counter-chinas-data-strategy/)