

Beijing's Plan To Spy On The World's Data Was Taught To China By Google

Thu, 08 Sep 2022 21:31:41, newstips66, [category: afghanistan, post_tag: beijings-plan-to-spy-on-the-worlds-data-was-taught-to-china-by-google, category: brotopia, category: community-service-programs, category: elon-musk, category: energy-dept-slush-fund, category: facebook-meta, category: google-alphabet, category: hired-assassins, category: housing, category: idea-theft, category: lithium-batteries, category: netflix, category: news-manipulation, category: patents-and-inventions, category: political-bribes, category: repairing_silicon_valley, category: san_francisco_corruption, category: senator-insider-trading, category: silicon_valley_death, category: sony_pictures, category: stanford_univ_bribes, category: tesla_motors_lies_and_defects, category: web-spying, category: worldnews]

Beijing's Plan To Spy On The World's Data Was Taught To China By Google

- You Can See What Google Is Doing To America By Seeing What China Is Doing To The World
- Idiot Senators In Congress Are Technically And Intellectually Incapable Of Understanding The Threat

By [Adam Piore](#).

Few cases better show how U.S.-China relations have deteriorated in the age of Big Data than the response Wang Jiang got when he offered, at the height of the pandemic, to set up labs for COVID-19 testing in the U.S.

Wang is a known quantity in the world of U.S. biotech. He cut his teeth as a genetics researcher at the major public research universities of Texas, Iowa and Washington. He's now the snowy-haired, charismatic chairman of Shenzhen-based BGI, the world's largest biotech company, which for decades has been collaborating with some of America's leading geneticists. BGI participated in the global effort to sequence the first human genome, formed a partnership with the Children's Hospital of Philadelphia to identify genes associated with pediatric diseases, and named an institute in China after Harvard's George Church, a gene-editing pioneer, who continues to work with the company.

FE Cover China Big Data BANNER

But Wang's offer ran afoul of the National Counterintelligence and Security Center, which issued a stark warning: "Foreign powers can collect, store and exploit biometric information from COVID tests." The Trump Administration's top U.S. counterintelligence official, Bill Evanina, later told 60 Minutes that the labs were "modern-day Trojan horses," an effort by the Chinese government to establish a "foothold" to bring in equipment, collect DNA and start "mining your data." No one in the U.S. took BGI up on its offer.

Evanina's suspicions highlight a growing tension between the U.S. and China, one that is expected to get significant attention in Washington this fall. The rise of Big Data—the vast digital output of daily life, including data [Google](#) and [Facebook](#) collect from their users and convert into advertising dollars—is now a matter of national security, according to some policymakers. The fear is that China is vacuuming up data about the U.S. and its citizens not just to steal secrets from U.S. companies or to influence citizens but also to build the foundation of technological hegemony in the not-too-distant future. Data—lots of it, the more the better—has, along with the rise of artificial intelligence, taken on strategic importance.

In recent months, some of the more hawkish national security mavens in Washington, D.C. have warned that the Chinese Communist Party (CCP) is aggressively moving to control all the data that flows through the country—even data that originate from American and other Western firms working in China. This would represent an escalation of Beijing's well-established campaign of corporate espionage through hacking and the export of Chinese-made technologies that allegedly contain back-doors for Chinese spies to access foreign data at will.

China hawks are calling on the Biden Administration to launch a broad review of Chinese internet, telecom and tech companies operating in the U.S. and restrict activities—and the ability to access American data—of those deemed a threat to U.S. national and economic security. Complacency in the face of this threat, they say, could harm U.S. economic, military and commercial interests and leave citizens vulnerable to spying and manipulation.

The pressure seems to be working. A new round of congressional hearings are expected on the issue in the fall. And Reuters reported in May that the Biden Administration has been putting the final touches on an executive order that would give the [Department of Justice](#) new powers to stop foreign adversaries, like China, from accessing Americans' personal data. Commerce Department officials told *Newsweek* that in recent months they've launched at least four active investigations of tech companies with ties to China or other foreign adversaries and plan a more far-reaching investigation.

Although the Biden Administration has declined to comment, the arguments are well-known in Washington policy circles. The issue has become a matter of growing bipartisan concern.

"It is estimated that 80 percent of American adults have had all of their personal data stolen by the CCP, and the other 20 percent most of their personal data," Evanina told the [Senate Select Committee on Intelligence](#) in August, 2021. "China's ability to holistically obtain our intellectual property and trade secrets via illegal, legal and sophisticated hybrid methods is like nothing we have ever witnessed. Our economic global supremacy, stability and long-term vitality is not only at risk, but squarely in the cross hairs of [Xi Jinping](#) and the communist regime."

Xi Jinping. Xie Huanchi/Xinhua/Getty

The threat goes well beyond trade secrets, argue Matt Pottinger, the Trump Administration's deputy national security adviser, and David Feith, former U.S. deputy assistant secretary of state for East Asian and Pacific affairs. "Data is the oil of the 21st century, the indispensable resource that will fuel artificial-intelligence algorithms, economic strength and national power," they wrote in a [New York Times](#) op-ed last fall.

This view is by no means unanimous in national-security circles, however. Broad fears of technological hegemony may be overblown, some policy experts say. And harsh measures against China could alienate allies and trigger a rash of similarly harsh measures by countries abroad toward U.S. tech firms.

In any case, the U.S. is in an exceedingly weak position to lead a moral crusade for the sanctity of data. The concept of harvesting clicks, text, internet addresses and other data from unsuspecting citizens and exploiting them for commercial and national-security ends was invented in the halls of the National Security Agency, the [CIA](#) and the tech startups of Silicon Valley. Facebook (now [Meta](#)), Google, [Amazon](#), [Microsoft](#) and [Apple](#) currently lead a vast industry based on trading and compiling user data. Taking measures to protect the data of American citizens from the ravages of Silicon Valley would go a long way to protecting them from China, too. Any measures directed solely against China would likely be ineffective because vast troves of consumer data would still be available for purchase on secondary data markets.

An overreaction on the part of the U.S., meanwhile, could hasten a tendency towards a kind of digital Balkanization, where nations erect their own barriers to the flow of data. "Whatever the U.S. does will send a signal to other countries around the world as to how they should also define and apply national security in a digitalized world," says Nigel Corey, associate director of trade policy at the Information Technology and Innovation Foundation. "I'm concerned about an overreaction that fundamentally undermines the openness of the internet, which has so clearly benefited the US economy, and tech sector."

How the U.S. responds to China's authoritarian spin on Big Data in the coming months is one of the trickiest issues of U.S. foreign policy. In the long term, it may turn out to be one of the most consequential.

The Devolution of the Internet

When the internet first took off, back in the 1990s, it was supposed to be a boon for democracy. Few people believed authoritarian nations like Russia and China would be able to stem the tide of digital information. "We know how much the Internet has changed America. Imagine how much it could change China," said then-president [Bill Clinton](#) in March 2000 at the Johns Hopkins University. Trying to crack down on the internet was "sort of like trying to nail Jell-O to the wall."

China Targets Israeli Technology in Bid for Global Dominance As U.S. Frets

[Read more](#)

[China Targets Israeli Technology in Bid for Global Dominance As U.S. Frets](#)

That was a miscalculation. In the late 1990s and early 2000s, China began constructing "the great firewall," a system of technological surveillance and information control. And it pioneered "Golden Shield," software that enabled the government to inspect data being received or sent within its borders and block destination IP (internet-protocol) addresses and domain names. In 2004, the Communist Party issued new guidelines on internet censorship that called for Chinese universities to recruit internet commentators who could guide online discussions in "politically acceptable" directions and report comments that did not follow Chinese law to authorities, according to the book *The Third Revolution: Xi Jinping and the New Chinese State*, by Elizabeth C. Economy.

China also launched a new era of economic espionage. Chinese hackers penetrated the servers of American companies and stole intellectual property valued, by some estimates, at between \$200 billion and \$600 billion per year, between 2008 and 2013. Most famously, they breached the servers of a Lockheed Martin subcontractor and made off with plans for Lockheed's \$400 billion F-35, the most advanced and expensive aircraft ever produced. China's J-31 stealth fighter jet, introduced a few years later, bears a striking resemblance to the F-35.

A model of a Chinese J-31 stealth fighter. Johannes Eisele/AFP/Getty

Xi Jinping, who rose to president in 2013, took digital control of Chinese society to a new level. He poured millions of dollars into technological upgrades to monitor and censor content, passed new laws making it easier to restrict content, and launched an aggressive campaign to punish anyone who violated the new restrictions. "The internet has become the main battlefield for the public opinion struggle," he said at the time.

Under Xi, China also demonstrated how these new technologies could be harnessed to create a new kind of Orwellian surveillance state, empowering authorities to amass a staggering

amount of data on its own citizens—and increasingly those in other nations—and experimenting with different ways to use them to exert social control. For instance, China's "smart cities" initiative includes a comprehensive monitoring system called "Skynet" that uses pattern recognition technologies to identify and track individuals using facial recognition, gait analysis and other unique personal characteristics. In some cities, Skynet is used to evaluate compliance with state policies, such as bans on jaywalking.

Xi's Made in China 2025 economic development plan identified the control of data as a key to the nation's ambitions. "Whoever controls big data technologies will control the resources for development and have the upper hand," he told the Chinese Academy of Sciences in the early months of his tenure.

FE Big Data China 09



Protesters in London. Vuk Valcic/Getty

Not long after that speech, Chinese hackers began expanding their efforts from the theft of valuable industrial and defense technologies towards collection of sensitive personal data from abroad. In 2015, hackers who were later connected to the People's Liberation Army breached the servers of the Marriott Hotel Chain and stole the passport, credit card information and other personal details of roughly 500 million guests. They hacked into Anthem healthcare in the U.S. and made off with the personal information of 78 million Americans.

Hackers also broke into the U.S. Office of Personnel Management and stole files on roughly 2 million former or retired federal employees and more than two million current ones. These dossiers included information on nearly all the background investigations of Americans who held top-secret security clearances. Tufts China scholar Michael Beckley characterized this haul as "the deepest darkest secrets from American government works, including CIA operatives," including details on drug use, debts, foreign travel and a list of all foreign relatives and friends in other nations.

Finally in 2017, Chinese hackers broke into Equifax, the credit reporting agency, stealing sensitive personal information such as names, birth dates and social security numbers of roughly 148 million U.S. citizens—nearly all American adults. It was one of the biggest state-sponsored thefts of personally identifiable information on record.

The effort to suck up and warehouse the personal data of American consumers continues. Last year, the Washington Post reviewed bidding documents and contracts for 300 Chinese government projects issued by agencies ranging from police, military, propaganda and state media at the beginning of 2020. The files contained orders for software designed to collect data on foreign targets from sources such as [Twitter](#), Facebook and other Western social media companies.

Meanwhile, China has pushed aggressively to help [Huawei](#) and other telecommunications firms win the battle to build the infrastructure for 5G systems around the globe—technology that U.S. law enforcement and intelligence officials have warned would allow China to further penetrate systems and steal data. Over the years, Beijing provided as much \$75 billion in grants, credit facilities, tax breaks and other forms of financial assistance to Huawei Technologies Co., according to a Wall Street Journal tally, allowing the company to undercut rivals on prices by 30 percent and grow from a little-known vendor of phone switches to the world's largest telecom-equipment company. It has also worked to pack international standards boards with candidates sympathetic to Chinese-made technologies central to the internet's future infrastructure.

FE Big Data China 07



Huawei's research center in Shanghai. Visual China Group/Getty

Thirst for Data

Advances in artificial intelligence have raised the stakes in the battle for data. For one thing, AI is thought to be a key technology for national competitiveness with broad national security implications. AI can make existing weaponry more effective, such as by giving guided missiles or drones more smarts in pursuing elusive targets and by opening up new ways to carry out cyber-attacks. It makes it possible for a military power to attack effectively in new ways, such as by manipulating public opinion of an opponent or undermining its democratic institutions. Applied to U.S. citizen data, some experts warn, it could also find people in financial distress and in jobs that would make them juicy recruits for espionage.

China made no secret of its goal of becoming "the world's primary AI innovation center" in a seminal document published by the State Council in 2017. It has poured billions into information technology with the goal of building a \$150 billion industry by 2030. But AI is only as good as the data it has to work with. For instance, machine intelligence, a form of AI, learns from experience and must be "trained" on data sets to pick out patterns that allow them to make accurate predictions.

The Rift Between the U.S. and China Is a Global Health Hazard

Read more

[The Rift Between the U.S. and China Is a Global Health Hazard](#)

China's recognition of the strategic importance of data is apparent in the way it has tightened up on Western companies. In 2019, the CCP declared data a "national resource" on par with land, labor, capital and technology in importance to economic growth. Last fall, Chinese authorities began implementing a series of laws and regulations that codify the government's ability to control the flow of all the information generated within its borders and restrict cross-border data flows and grant the government the right to access and review all the data collected within the nation's borders, by both domestic and foreign companies. Beijing can prevent foreign companies from transferring "core state data" overseas, even to their own corporate headquarters. (Core state data is anything that involves national security, the national economy or is otherwise essential to specific regions and industries.)

In response, both [Tesla](#) and Apple recently agreed to build new data centers in China to house information they collect there. Apple, according to a New York Times investigation, has largely "ceded control" of the data in at least two of its new centers to the Chinese government, abandoning its encryption technologies and allowing state employees to physically manage its computers.

FE Big Data China 10

Tesla's Gigafactory in Shanghai. Visual China Group/Getty

Other tech companies chose to close up shop and go home. In October, 2021 Microsoft announced plans to shut down its Chinese version of LinkedIn due a "significantly more challenging operating environment and greater compliance requirements in China."

In Washington, the question of how the Biden Administration should respond to the new restrictions has been the subject of vigorous lobbying by China hawks, industry groups, data policy experts and other competing factions. It also has increasingly become an issue of concern on Capitol Hill, with new hearings expected in the fall.

So far, President Biden has, on paper at least, maintained the tough stance of his predecessor. In June, 2021 he signed an executive order reaffirming portions of a new regulatory regime put in place in the final days of the Trump administration. It grants broad authority to the Secretary of Commerce to evaluate risks posed by internet, telecom and tech companies operating in the United States from nations deemed "foreign adversaries" and take protective action. The order allows the Commerce Department to ban or restrict new transactions between U.S. and foreign firms and to curb the activities of foreign internet and telecom companies operating in the U.S.

The executive order also allows Commerce to act retroactively. That's what President Trump tried to do to the social-media platform TikTok, which he suggested was collecting and warehousing the data of U.S. users. Trump ordered the Chinese firm ByteDance to divest itself of ownership and threatened to shut down its U.S. operations if it didn't comply. The order was successfully challenged in court—most recently in December, 2020, when a Trump appointed judge ruled that the president overstepped his authority, failed "to adequately consider an obvious and reasonable alternative," and that the ban was "arbitrary and capricious."

FE Big Data China 06

U.S. officials warned Congress in 2015 to expect more breaches of government computer networks by "sophisticated, well funded and focused" adversaries. Brendan Smialowski/AFP/Getty

Biden sidestepped the TikTok controversy by revoking Trump's ban in his executive order but appears willing, in theory, to go after other companies. In March, the administration established a new Commerce Department group to focus on data risks posed by companies from nations deemed foreign adversaries. In the most recent budget request, Biden asked for \$36 million to fund the new effort. [Congress](#) is expected to approve it.

In January, Reuters, citing three anonymous sources, reported that the Biden administration was reviewing e-commerce giant [Alibaba's](#) cloud business, the world's fourth largest cloud provider, focusing on how the company was storing U.S. client data, including personal information and intellectual property and whether the Chinese government could gain access to it. They could force the company to prevent the transfer of data overseas or ban Americans from using the service. No such action followed.

Commerce officials declined to comment on Alibaba, saying they cannot discuss individual cases. But they told *Newsweek* that they have recently launched at least four investigations of internet and telecom companies of "foreign adversaries." Of all the nations on that list—which also includes North Korea, Iran, Venezuela, Cuba and Russia—China has by far the most formidable tech presence in the U.S. Meanwhile, the department plans to launch a more extensive review once Congress approves its new budget.

According to the July Reuters story, which was based on unnamed sources, the White House is also considering granting U.S. Attorney General [Merrick Garland](#) the authority to review and potentially bar commercial transactions involving the sale of or access to data if they pose an undue risk to national security. It would also instruct the Department of Health and Human Services (HHS) "to ensure that federal assistance, such as grants and awards, is not supporting the transfer of U.S. persons' health, health-related or biological data...to entities owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries," according to an excerpt of a draft executive order that, according to Reuters, is being circulated.

Overzealous Enforcement

What data constitutes risk to U.S. national security and how that risk will be evaluated and enforced remain open questions. The dangers that Pottinger and other China hawks point out may be real, but overzealous enforcement of the new rule could also have unintended consequences that hurt American interests.

Indeed, as anti-Chinese rhetoric in the U.S. rise to a near hysterical pitch, the American Civil Liberties Union (ACLU) and other organizations point to early signs of government overreach. Last January, a federal court in Boston dismissed charges against MIT professor Gang Chen, a Chinese-American nanotechnology engineer accused of failing to disclose research ties to China. Aggressive prosecution of Chinese-American scientists working in U.S. institutions could cause a reverse brain drain in areas ranging from cancer research to semiconductors.

China, Eyeing Taiwan, Sees Lessons in Russia's Reckless Ukraine War

Read more

[China, Eyeing Taiwan, Sees Lessons in Russia's Reckless Ukraine War](#)

"Policy makers are increasingly viewing science—and biotechnology in particular—through the lens of national security," says Abigail Coplin, an assistant professor of sociology and science, technology, and society at Vassar College, who studies biotechnology development in China. "No one seems to be considering what is lost as a result." In the case of biotechnology, what Coplin calls "over-securitization" poses real risks to American patients, American competitiveness, and the global progression of science by disrupting collaborations and knowledge-sharing that could lead to the discovery and development of new treatments and cures for diseases.

Read more

- [The Greatest National Security Threat No One Is Talking About](#)
- [Trump Repeats Praise of 'Smart' Putin, Touts Xi's 'Iron Fist' Rule of China](#)
- [China Targets Israeli Technology in Bid for Global Dominance As U.S. Frets](#)

Indeed, while media accounts of China's data harvesting have largely focused on the threat to the privacy of Americans, overseas many view the United States as the primary threat. Many Europeans have not forgotten American whistleblower [Edward Snowden](#) and the millions of U.S. National Security Agency documents, detailing American intelligence gathering techniques, he released in 2013. The documents suggested that it was in fact the U.S. doing the "hoovering" of data of world leaders and ordinary citizens alike, and secretly warehousing millions of emails, text messages and cell phone location data from all corners of the globe so they could be mined for intelligence purposes—among them the personal text messages of millions of Chinese citizens.

"Sometimes we only think about this in the U.S. versus China framework," says Samm Sacks, a senior fellow at Yale Law School's Paul Tsai China Center and an authority on the geopolitics of data privacy and cross-border data flows, who also consults for U.S. companies operating overseas. "We forget that in places like Europe and India there's already growing concern about American surveillance and how American companies use citizens' data."

Many data privacy experts overseas regard warnings from the U.S. about the threat of Chinese data hegemony with deep skepticism. American tech titans like Google's [Eric Schmidt](#) and former Facebook executive Sheryl Sanders have argued that the threat of a dominant China makes it unwise to break up their companies or regulate their wanton collection of data. [Mark Zuckerberg](#) has publicly stated that he views TikTok as a major competitor and threat to Facebook's market position. In the months leading up to President Trump's August 2020 executive order cracking down on TikTok, Zuckerberg met with members of Congress and the Trump Administration behind closed doors and raised concerns about the firm's Chinese owners and the threats they pose to American security. During this period, the company spent more on lobbying than any other single company, the Wall Street Journal reported.

Overzealous enforcement of data laws against Chinese companies could also result in unintended consequences—not just forcing other nations to choose sides, but also establishing a troublesome precedent. Nations around the globe that are equally concerned about their own data could use tough measures against U.S. companies.

A rule like the one being implemented by the Commerce Department "creates a roadmap or a blueprint that will make it much easier to turn these same tools against American companies in other parts of the world in ways that can actually, paradoxically, advantage Chinese companies in those third country markets," says Sacks.

FE Big Data China 12



China's DJI Inspire 1 Pro drone. Qilai Shen/Bloomberg/Getty

Striking a Balance

China's aggressive efforts to wall off and control its own data—and its ability to easily access ours—highlight an uncomfortable truth that is often missing from the discussion about China's aims. While nations around the globe have begun to grapple with data privacy laws, partisan rancor and aggressive lobbying by big American tech companies have paralyzed efforts in the U.S. Congress to pass even basic consumer-data protections. Such consumer protections could form the basis for a new framework that could later be adapted to protect U.S. data from Chinese exploitation.

The same chaotic, largely unregulated free-flow of American data that U.S.-tech behemoths like Facebook, Google and Amazon have exploited to grow into 10,000 pound gorillas is what also enables China to collect and warehouse American data.

Although a Commerce-Department committee on foreign investment reviews acquisitions and investments by foreign companies to evaluate national security risks, unlike China and the E.U., the U.S. currently has no top-down policy classifying private consumer data as sensitive and protecting it, even though such measures enjoy wide public support. Instead, there is a patchwork of sector-specific policies, standards and regulations, spread out across dozens and dozens of different agencies, that attempt to limit the circulation of some data—health-care regulations, for instance, provide protection for confidential data—and not others, says Yale's Sacks.

The U.S.'s patchwork approach to data regulation leaves Americans wide open for exploitation—not just by China and American social-media companies, but also by anyone with an internet connection. In a report released earlier this year, Justin Sherman, a cybersecurity policy fellow at New America, surveyed 10 major data brokers and found them openly and explicitly advertising the sale of sensitive data on millions of U.S. individuals, ranging from demographic information to personal activities and life preferences, such as political views, travel habits, healthcare data, the names of family members and relatives, and even the real-time GPS locations of current and former [U.S. military](#) personnel and other U.S. government employees.

Yet lawmakers seem to view the need to protect the data of Americans from China as separate from the need to protect it from Silicon Valley. Other countries do not make this distinction.

India's Parliament, for instance, is debating how to regulate the flow of data, potentially with sweeping new requirements, Sherman says. In Europe, American lawyers and diplomats have for months been renegotiating the agreement that serves as the legal basis for all trans-Atlantic data flows between the E.U. and the U.S. to ensure that U.S. firms respect the E.U.'s laws on consumer privacy protections. Under a "privacy shield" agreement negotiated in the wake of the Edward Snowden revelations, the U.S. pledged to take new measures to ensure its intelligence agencies did not violate the rights of European citizens by illegally collecting private information. But that agreement was subsequently annulled in 2020 by the European Court of Justice, and negotiators were deadlocked for months over the thorny issue of how European citizens can seek redress if U.S. intelligence agencies violate the terms of the pact. Although the two sides reached a preliminary deal in March, negotiations have been stalled over the final wording in the document ever since.

The voracious appetite for data of U.S. social media companies is inextricably caught up in the debate. In July, the Irish Data Protection Commission submitted a draft decision to European regulators that would block Meta, Facebook's parent company, from sending user data from Europe to the U.S. In its response to that filing, regulators in Norway wrote that they support imposing hefty fines on Meta if it continues to transfer data overseas, Politico reported in August, citing documents obtained by Freedom of Information Act requests. As a result, Meta has warned that the company might shut down European access to Facebook and [Instagram](#) if the U.S. and E.U. fail to reach an agreement on a new E.U. privacy shield law.

If negotiations break down and the E.U. bars Facebook from transferring the data of European citizens out of the E.U., the precedent could upend trans-Atlantic data flows and potentially cost businesses "billions of dollars," according to Paul Triolo, senior vice president for China tech policy at Albright Stonebridge Group, a global business strategy firm based in Washington and a former senior U.S. government official who worked on China technology policy.

How the U.S. deals with this state of affairs will have a broad impact on other nations. In the past five years, at least 62 countries have passed new data localization rules, which either place restrictions on what can be transferred beyond their borders or require companies to store a domestic copy of whatever is collected. Even the U.S. requires cloud companies contracting with the Department of Defense to store classified data on servers in the United States.

Meanwhile, "pro data nationalism rhetoric" has gone "through the roof," says Sherman. If the pendulum swings too far towards data protectionism, it will choke off foreign investment and economic growth. Rising tensions between China and the U.S. could feed the trend.

Requiring companies to store data locally raises a barrier to entry, even for domestic companies. "As soon as I'm collecting data on, say, Indians, I have to spend all this money on extra

data infrastructure and pay attention to where the data's going," says Sherman. "I have to spend money on lawyers and compliance specialists to make sure I'm not breaking the law. When I transfer data or email to someone about a customer, if I want to work with an international client, I now have to go through this whole approval process."

Some experts are arguing for new multilateral agreements and the establishment of an international body like the World Trade Organization that regulates the flow of data, serves as a forum to hammer out differences and ensures business can continue to operate efficiently across borders. Such a forum could also help western companies compete with China in the event its government walls off its data from the rest of the world.

"We need to come up with some framework for a coalition of the willing of sovereign nations, like the United States, where we would set up binding principles that would govern the flow of data across borders," says Matthew Slaughter, an economist and dean of Dartmouth Tuck School of Business. "We don't have anything like that right now."

Many nations would likely support such a framework, at least in principle. During the World Economic Forum Annual Meeting in 2019 in Davos, Switzerland, then Japanese Prime Minister Shinzo Abe introduced a concept he called "data free flow with trust." The Organization for Economic Co-operation and Development, an intergovernmental economic organization with 38 member countries, has an initiative underway that aims to create a set of shared principles for member nations that would create checks on government surveillance and explicitly spell out law enforcement access to data. The Biden administration has also set up the E.U.-U.S. working group on data governance.

FE Big Data China 13

A summit with Presidents Biden and Xi makes the evening CCTV news broadcast in Beijing. Kevin Frayer/Getty

A Tale of Two Internets

Hammering out international policies to protect data will take years. How much should the U.S. worry about China's data appetite in the meantime? Some China-watchers argue that at the moment Beijing's data policies likely have more to do with domestic concerns than establishing dominion over the world's data. "The Chinese Government and Communist Party recognize data has tremendous value but also presents security vulnerabilities," says Sacks. "At this point, the country is simply focused on a massive effort simply to get a handle on it."

Other China experts warn that the long term consequences are dangerous regardless. "The value of the information they are collecting is not obvious at first," says Pottinger, currently a distinguished visiting fellow at the Hoover Institution and a consultant for companies doing business in China. "It's like looking at a mountain and saying, it's just a mountain. Well, actually, it's also a gold mine," he told *Newsweek*. "That value is latent, but later it can be immensely powerful in ways that compromise our security as well as our competitiveness."

Whatever the case, some suggest the world is already moving inexorably towards a bipolar digital world—a move that will only accelerate as the burgeoning race for AI dominance between China and America picks up steam.

That future may already be in sight. "We now have two internets," says Frank H. Wu, president of Queens College and author of *Yellow: Race in America Beyond Black and White*. "There's a Chinese internet behind the great firewall and then there's an American-led internet. And when you look at cell phone technology, and AI, it's now being divided up. Countries in Europe, Africa and Latin America are increasingly being told to pick—you need to join the Chinese side or the U.S. side."

What the Biden administration does in the coming months could serve to avoid such a digital divide—or hasten its arrival.

FE Cover China Big Data COVER

[In the Magazine](#)