https://www.npr.org/2021/02/24/969532277/china-wants-your-data-and-may-already-have-it

China Wants Your Data — And May Already Have It

- **Facebook**
- **Twitter**
- **Flipboard**
- **Email**

February 24, 202110:11 AM ET

Heard on All Things Considered

GREG MYRE

FacebookTwitter

LISTEN· 4:264-Minute Listen**Add toPLAYLIST**

-
- **Embed**
  - <iframe src=
-

Visitors walk past the giant word "Data" during the Guiyang International Big Data Expo 2016 in southwestern China. China says it's determined to be a leader in using artificial intelligence to sort through big data. U.S. officials say the Chinese efforts include the collection of hundreds of millions of records on U.S. citizens. The photo was released by China's Xinhua News Agency.
AP

As COVID cases began to rise a year ago, a Chinese company contacted several U.S. states and offered to set up testing labs. As a byproduct, the Chinese firm, Beijing Genomics Institute, would likely gain access to the DNA of those tested.

The offer was tempting for states struggling to set up their own testing facilities for a new virus on short notice. But U.S. national security officials urged the states to reject the offer, citing concerns about how China might use personal data collected on Americans.

"We certainly reached out to our partners and the community to make sure people were aware that the Chinese were pushing out these tests, informing them of what the risks were and really asking them not to take these tests," said Mike Orlando, the head of the National Counterintelligence and Security Center, which is part of the Office of the Director of National Intelligence.

WORLD

What Trump's Declassified Asia Strategy May Mean For U.S.-China Relations Under Biden

"As far as I know, they all turned them down," Orlando added.

Meanwhile, Beijing Genomics Institute, a major global player in the world of genomics research, reportedly set up labs in at least 18 other countries, and provided COVID testing kits to 180 nations, including the U.S. The U.S. officials stressed that their main concern was preventing the establishment of full-service labs. The officials do not consider the testing kits to pose a serious risk. Biotech companies in China, the U.S. and elsewhere routinely collect DNA data and use it to help guide the development of cutting-edge medicines that can benefit people worldwide. And BGI says it abides by all the laws in countries where it operates.

However, human rights groups say the Chinese government uses DNA testing for security purposes — such as identifying and tracking Uigher Muslims, the ethnic and religious minority whose members are being held in detention camps, in huge numbers, in western China.
Chinese police are also working to gather DNA samples from the country's male population — numbering roughly 700 million — to help keep tabs on the half of the population most likely to commit crimes, *The New York Times* reported last year.

A sweeping effort

U.S. officials add that DNA collection by Chinese companies, even when done openly and legally, should be seen as part of a comprehensive effort to vacuum up millions and millions of records on U.S. citizens. And many Chinese efforts violate U.S. law, the officials say.

"Most Americans have probably had their data compromised by the cyber intelligence units of the Chinese government and Chinese military intelligence," said April Falcon Doss who worked at the National Security Agency and wrote the book *Cyber Privacy:Who Has Your Data And Why You Should Care.*

Falcon Doss said China is collecting detailed personal information on a massive scale for multiple reasons: to boost its economy, advance its technology and to support its espionage efforts.

"China has really set as one of its strategic goals, trying to achieve dominance in artificial intelligence," she said. "What you need to feed artificial intelligence algorithms is lots and lots and lots of data."

NATIONAL SECURITY

Chinese Hackers Charged In Alleged Cyber-Theft Of 145 Million Americans' Data

The U.S. and China both spy aggressively on each other. In recent years, one striking feature of this rivalry is China's pursuit of personal data on Americans.

Since 2014, China's been blamed for a series of huge data thefts. They include individual records taken from the credit agency Equifax (145 million records), the hotel chain Marriott (400 million), the health insurer Anthem (78 million), and the U.S. Office of Personnel Management (21 million), which stores sensitive files on government workers, including fingerprints and information on security clearances.

The Justice Department has filed charges against Chinese citizens in these and other cases, though most remain in China and beyond the reach of U.S. law enforcement. Some of those accused are serving in the Chinese military.

China's aim

China denies responsibility for these hacks. Still, Beijing acknowledges it wants to be a world leader in gathering big data, and using artificial intelligence to sort through it.

"If you look at the cyber hacks of our credit information, our travel information, and then you layer in the DNA information, it creates an incredible targeting tool for how the Chinese could surveil us, manipulate us and extort us," said Orlando, whose office keeps watch over attempts by foreign countries to spy on the U.S.

NATIONAL SECURITY

In China's Push For High-Tech, Hackers Target Cutting-Edge U.S. Firms

U.S. officials, past and present, say it's difficult to tell exactly how the Chinese may be using the hacked data. But they say the possibilities are limitless.

"It gives them tremendous access into who we are," said retired Army Gen. Keith Alexander, who led the National Security Agency under President Barack Obama.
The files from the Office of Personnel Management would help China identify U.S. intelligence officers.

Credit information from Equifax could flag people who have money problems and might be susceptible to spying for China in exchange for financial help.

Alexander said China could cross-reference the data to send a highly personalized phishing email to a person in a key U.S. tech industry that China hopes to exploit.

"So it says in a email that China sends to a specific individual, 'You have Type 2 diabetes. Here's a new Type 2 diabetes solution. Click here,'" said Alexander, who is now the president of the private firm IronNet Cybersecurity.

After gaining access to that person's email account, hackers could look for sensitive personal or company information.
The U.S. and China signed a 2015 agreement that said neither government would seek to steal intellectual property from private companies in the other nation. But Alexander said it had only a brief and limited impact on the Chinese hacking of U.S. companies. He said the ongoing theft of American technology and data has given China a huge economic lift, and inflicted great damage on the U.S.

"The Chinese need access to intellectual property to fuel that economic engine," he said. "That theft is the greatest transfer of wealth in history."

Greg Myre is an NPR national security correspondent. Follow him @gregmyre1.