The Privacy Project: When China Hacks You

February 11, 2020, *New York Times Privacy Project*

By Charlie Warzel

On Monday, the Justice Department announced that it was charging four members of China's People's Liberation Army with the 2017 Equifax breach that resulted in the theft of personal data of about 145 million Americans.

The attack, according to the charges, was part of a coordinated effort by Chinese intelligence to steal trade secrets and personal information to target Americans.

Using the personal data of millions of Americans against their will is certainly alarming. But what's the difference between the Chinese government stealing all that information and a data broker amassing it legally without user consent and selling it on the open market?

Both are predatory practices to invade privacy for insights and strategic leverage. Yes, one is corporate and legal and the other geopolitical and decidedly not legal. But the hack wasn't a malfunction of the system; it was a direct result of how the system was designed.

Equifax is eager to play the hapless victim in all this. Don't believe it. In a statement praising the Justice Department, Equifax's chief executive, Mark Begor, deflected responsibility, highlighting the hack as the work of "a well-funded and sophisticated military" operation. "The attack on Equifax was an attack on U.S. consumers as well as the United States," he said.

While the state-sponsored attack was indeed well funded and sophisticated, Equifax, by way of apparent negligence, was also responsible for the theft of our private information by a foreign government.

According to the indictment, the Chinese military exploited a vulnerability in Adobe's Apache Struts software, which Equifax used. As soon as Adobe disclosed the vulnerability, it offered a patch to prevent breaches. Equifax's

security team, according to the indictment, didn't employ the patch, leaving the drawbridge down for People's Liberation Army attackers. From there, the hackers gained access to Equifax's web servers and ultimately got a hold of employee credentials.

Though the attack was quite sophisticated — the hackers sneaked out information in small, hard to detect chunks and routed internet traffic through 34 servers in over a dozen countries to cover their tracks — Equifax's apparent carelessness made it a perfect target.

According to a 2019 class-action lawsuit, the company's cybersecurity practices were a nightmare. The suit alleged that "sensitive personal information relating to hundreds of millions of Americans was not encrypted, but instead was stored in plain text" and "was accessible through a public-facing, widely used website." Another example of the company's weak safeguards, according to the suit, shows the company struggling to use a competent password system. "Equifax employed the username 'admin' and the password 'admin' to protect a portal used to manage credit disputes," it read.

The takeaway: While almost anything digital is at some risk of being hacked, the Equifax attack was largely preventable.

Since its establishment in 1899 (it was originally named Retail Credit), Equifax has prompted concerns over the sheer volume of data it amasses. Those fears increased as the company entered the digital age. In a March 1970 Times article about the company, Alan Westin, a professor at Columbia University, offered this warning: "Almost inevitably, transferring information from a manual file to a computer triggers a threat to civil liberties, to privacy, to a man's very humanity … because access is so simple."

Five decades on, that statement rings especially true. Moreover, it's a useful frame to understand why, in a world where everything can be hacked,

bloated data brokers like Equifax present an untenable risk to our personal and national security.

It's helpful to think about a hack like what happened to Equifax as part of a chain of events where, the further down the chain you go, the more intrusive and potentially damaging the results. The Equifax data we know was stolen is a perfect example of what's known as Personally Identifiable Information. Obtaining the names, birth dates and Social Security numbers of almost half of all Americans is troubling on its own, but that basic information can then be used to procure even more personal information, including medical or financial records.

That more sensitive information can then be used to target vulnerable Americans for blackmail or simply to glean detailed information about the country by analyzing the metadata of its citizens. And so the revelations in the indictment in the Equifax case are alarming. The theft is one in a string of successful hacks, including of the federal Office of Personnel Management, Marriott International and the insurance company Anthem. Given the volume and granularity of the data and the ability of attackers to use the information to gain *even more* data, it's not unreasonable to ask, Does China now know as much about American citizens as our own government does?

In his statement on Monday, Begor, Equifax's chief executive, noted that "cybercrime is one of the greatest threats facing our nation today." But what he ignored was his own company's role in creating a glaring vulnerability in the system. If we're to think of cybercrime like an analog counterpart, then Equifax is a bank on Main Street that forgot to lock its vault.

Why rob a bank? Because that's where the money is. Why hack a data broker? Because that's where the information is.

The analogy isn't quite apt, though, because Equifax, like other data brokers, doesn't fill its vaults with deposits from willing customers. Equifax amasses personal data on millions of Americans whether we want it to or

not, creating valuable profiles that can be used to approve or deny loans or insurance claims. That data, which can help dictate the outcome of major events in our lives (where we live, our finances, even potentially our health), then becomes a target.

From this vantage, it's unclear why data brokers should continue to collect such sensitive information at scale. Setting aside Equifax's long, sordid history of privacy concerns and its refusal to let Americans opt out of collection, the very existence of such information, stored by private companies with little oversight, is a systemic risk.

In an endless cyberwar, information is power. Equifax's services as a data broker offer something similar to its customers, promising data and insights it can leverage for corporate power. China is behaving a lot like any other data broker. The big difference is that it isn't paying.