OPINION POLICY ASIA

Share article

TikTok’s Plan to Stay in the U.S. Could Pose a Threat—to U.S. Tech Companies

TikTok's plan to localize its operations in the U.S. sets a dangerous precedent for internet freedom abroad.

By Matt Perault
Perault is the director of the Center on Technology Policy at the University of North Carolina at Chapel Hill.

March 9, 2023 9:00 AM PST

TikTok CEO Shou Zi Chew photographed in the company's Washington, D.C. office. Photo by Getty.

In a bid to avoid a U.S. ban, TikTok is embarking on a **project** to restructure its product and operations in the country. It plans to store local citizen data on local servers, create a domestic entity to house that data, comply with local legal and law enforcement requests for data, limit the flow of data across national borders—and spend billions of dollars to make all of this possible. In short, it plans to bring to life the model of internet governance the tech industry and the U.S. government have spent the past 20 years vehemently resisting.

The irony, of course, is that this outcome is the result of sustained pressure by U.S. lawmakers. Politicians have battered TikTok in the press and in congressional hearings, calling it a threat to U.S. national security because ByteDance, its parent company, is headquartered in China. Critics have alleged that TikTok could provide U.S. user data to the Chinese government or manipulate its algorithm to promote Chinese propaganda.

> **THE TAKEAWAY**
>
> **TikTok is desperately trying to avoid the kind of outright ban gaining support in Washington, D.C. But accepting the company's plan would come at significant cost to U.S. tech companies.**

To date, these allegations have been based on thin **support**. While some incidents have raised concerns—the company long **maintained** a privacy policy that allowed it to share data with ByteDance, for instance, and it recently **disclosed** that some employees had improperly accessed journalists' personal data—none of TikTok's critics have produced evidence that data on U.S. citizens has systematically flowed from its servers to the Chinese government.

Nevertheless, in response to the steady drumbeat of criticism, lawmakers have passed new laws at the **state** and **federal** level banning the app from government devices and have introduced **proposals** to **ban** the app entirely. The Committee on Foreign Investment in the U.S. is conducting an ongoing investigation into TikTok-related security risks, and calls are increasing to ban the app or force the company to sell a majority stake to a U.S. entity. A bill introduced earlier this week by Sens. Mark Warner and John Thune would require the government to develop a **"holistic, methodical approach"** to reviewing and potentially banning tech products that pose a national security risk.

In response to this pressure, TikTok has developed **Project Texas**, a program to dramatically alter its operations in the U.S. Under Project Texas, ByteDance will establish a separate entity to run its U.S. business. In addition to storing all U.S. citizen data, this entity will house sensitive technology such as TikTok's algorithm and content moderation functionality. Employees of this new entity will have to be U.S. citizens or green card holders, and the U.S. government will have final say over employment decisions. The leadership of Project Texas will report to an independent board, whose members the U.S. government must approve.

This new system will be costly—$1.5 billion to start up and at least $700 million a year to run it—and will almost certainly degrade app performance since some data will have to travel significant distances to reach users or content stored outside the U.S. Even though that data is traveling at the speed of light, those miles add up to **slower** apps. ByteDance has been willing to embark down this path without a decision from the U.S. government confirming that such a model will address its national security concerns, which tells you how concerned the company is about a potential ban.

For years, foreign governments have pushed U.S. companies to adopt models like Project Texas within their borders, and for years, tech companies have said no. Localizing data would endanger human rights, they've argued, by subjecting it to surveillance and censorship laws. Localizing data is too expensive, they've claimed, since it requires companies to open new data centers or rent server space in foreign countries. And they have argued that localization doesn't work for certain products—imagine a tweet with responses from users in multiple different countries. Where would you store that data?

Skeptics would argue that the strong stance against localization is due primarily to self-interest. Resisting local data storage requirements reduces the amount companies must spend on infrastructure. A company that does not have to localize its product for every country in the world will also have access to more users, and more users translates to more advertisers.

Even if companies do have selfish reasons for maintaining the status quo, it's hard to dispute there are real, large-scale benefits too. Pushing back on localization makes it easier for companies to **resist** foreign law enforcement requests for user data and government efforts to censor political speech. In 2007, members of Congress labeled Yahoo executives moral "pygmies" for **turning over data** to the Chinese government, which led to the arrest of a journalist, and since then tech companies have gone to great lengths to avoid getting the same label, even if they encountered serious repercussions from foreign powers. For example, a Facebook executive faced **arrest** in Brazil in 2016 after refusing to hand over user data to Brazilian law enforcement. And Google, Airbnb, Apple and others all **are dealing with fines** in Russia for failing to comply with data localization laws.

Project Texas would undermine these arguments against localization. How could a large tech company with deep pockets like Alphabet or Meta Platforms argue that localization is prohibitively expensive when TikTok is willing to pay the price? How could social media companies claim they can't parse location data when TikTok has developed a means of doing so? The shift will affect policy advocacy not only by companies, but also by the U.S. government, which has long **stood alongside** the tech industry in this fight. How could the U.S. government continue to argue that localization endangers human rights after it has imposed localization on TikTok?

With Project Texas as a model, other countries will no doubt push for the same arrangement within their own borders. Countries including **China**, **India**, **Brazil**, **France** and **Germany** have already taken meaningful steps toward requiring tech companies to localize, and more governments will likely follow. The pace will accelerate as more countries adopt this model, and companies like Meta, Alphabet, Microsoft, Twitter and Snap will likely be forced to change their operations. Project Texas, a code name that ironically suggests a change in only one state in one country, will spark a change in internet governance throughout the world.

This result isn't inevitable. The U.S. government has other policy tools it could use to address national security risks without increasing the risk of data localization. For example, it has the power to restrict specific foreign transactions that pose a national security risk using a little-known executive **rule**. Originally **issued** by the Trump administration and later **utilized** by the Biden administration, the rule outlines a **process** for the government to monitor and address national security risk in the tech sector from "foreign adversaries," including China. The rule includes clear evidentiary requirements as the basis for government action. That administration could apply that process to TikTok and other technology companies to ensure their business operations in the U.S. pose no threat. The new proposal from Sens. Warner and Thune would strengthen this process, **requiring** the Commerce Department to "identify, deter, disrupt, prevent, prohibit and mitigate" activity in the tech sector that creates national security risk.

Although these types of scalpel-size tools exist, it might be too late to use them. With lawmakers calling for outright bans on TikTok, state houses and Congress introducing new proposals to restrict TikTok access almost every week and both Republicans and Democrats trying to outdo each other in getting tough on China, a negotiated deal that requires TikTok to implement Project Texas as a condition of remaining operational in the U.S. seems like the best outcome the company could hope for. If it happens, the results will be devastating for the future of the internet. States will succeed in gaining more control over user data, but with significant costs to our human rights online and the quality of the technology we use.

Author's bio has been updated to show that his organization has received funding from TikTok.

Have an opinion The Information should publish? Find out how to reach us and more ***here.***

Matt Perault is the director of the Center on Technology Policy at the University of North Carolina at Chapel Hill, a professor of the practice at UNC's School of Information and Library Science and a consultant on technology policy issues at Open Water Strategies. (The Center on Technology Policy at UNC Chapel Hill has received funding from TikTok.)

Subscriber Comments

Keith Teare

Founder - SignalRank Corp

When I did a deal with China's CNNIC in early 2000, it included permission from China's Ministry of Information. It included provisions that all servers must be in China and be capable of performing if China was cut off from the rest of the world. Technically that was easy to implement (the company was RealNames). I think today, and there would be no barrier to such architecture.

Like · Reply · Report · 17 minutes ago

Jud Valeski

Executive

hmmm. with EU's data privacy/user protection laws, and China dynamics (such as this), I've simply been moving forward assuming that data storage in general has to account for physical localization at the architecture level. firms NOT operating w/ politically motivated silo'ing of "user data" are at a severe disadvantage going forward. as much as that sucks at the technology-level (users have accepted horrible app experiences (e.g. performance) forever and that will never stand in our way of a good dopamine hit), it feels like table stakes in the future.

Like · Reply · Report · 8 minutes ago

Matt Perault

Not you? Log Out

Want to edit your profile? Edit Profile

POST NEW COMMENT

Featured Partner

Corporate Subscriber Circle