The Washington Times

We're in a cyber cold war with China. Here's how we gain the upper hand.

By Matt Sandgren | Monday, September 21, 2020

Last month, President Trump announced his intentions to ban TikTok unless the Chinese company finds an American buyer. The news came just weeks after a European Court struck down the EU-US Privacy Shield, which facilitated data sharing on both sides of the Atlantic.

What do these seemingly disparate events have in common? They both underscore growing concerns over the misuse of consumer data—and the urgent need for Congress to pass a federal privacy framework. Passing this framework is essential to securing America's digital leadership in the new cold war with China.

Over the last decade, China has become Silicon Valley's fiercest competitor, proving that it's not just good at stealing technology but building its own innovations as well. Beijing has established itself as a near-peer adversary in quantum computing, artificial intelligence, and 5G technology. Huawei, meanwhile, is growing faster than any other smartphone maker in the world, even as the company's reputation for being a pawn of Chinese intelligence grows with it.

Then there's TikTok, the white-hot social media platform with more than 1 billion users across the globe, including more than 80 million in the United States alone. Like Huawei, US officials consider TikTok a tool of the Chinese Communist Party (CCP). They even suspect the CCP of

using the app to spread propaganda and harvest American user data—hence the President's decision to take action against its parent company, ByteDance.

Set against the backdrop of China's rise in tech, its long record of IP theft, and recent acts of cyberaggression, the significance of the TikTok controversy comes into focus. This isn't some run-of-the-mill corporate dispute but a crucial battle in a new cold war. For all intents and purposes, the United States and China are locked in a technological arms race, seeking to build influence and soft power through social media, 5G networks, and other innovations. TikTok just happens to be the latest battlefield.

Bringing TikTok under American oversight would help us score an important victory against China in the short term. But it's not enough. if we want to claim lasting victory in the cyber cold war—and secure US digital dominance for decades to come—we need to enact federal data privacy legislation.

Here's why: If US-based Oracle becomes the service provider for TikTok, it would protect Americans from having their data exploited by the CCP. Even in this scenario, however, third-party brokers could still legally purchase user data and in turn, sell it to the Chinese government. That's why we need a national privacy standard that applies to all companies operating in the United States, regardless of their country of origin. To keep our data safe, we can't expect American tech firms to buy every foreign app that goes viral. We can, however, require every internet platform seeking to do business here to comply with a US privacy standard.

Our European partners have been pushing us to adopt a uniform privacy standard for years. And our inability to do so contributed to the dissolution of the EU-US Privacy Shield last July. Since 2016, the Privacy Shield has governed transatlantic data flows, allowing companies to innovate and grow on both sides of the pond. But without the guidance provided by the Privacy Shield, small and mid-size American companies will have more difficulty navigating European markets, where the slightest privacy infraction could result in an existential lawsuit.

In striking down the agreement, the chief concern of EU regulators was NSA surveillance, but our lack of a national privacy standard didn't help either. What assurances do Europeans have that US companies will protect their data if Americans don't even have a comprehensive law in place to protect their own?

That's why enacting a federal privacy law is critical to reopening transatlantic data flows and strengthening our position against China. By leading on data privacy, we can differentiate Silicon Valley from surveillance-obsessed Beijing to build trust with our foreign trade partners and increase American tech influence abroad.

The good news is there's growing support for a national privacy standard. Major tech CEOs from Facebook's Mark Zuckerberg to Apple's Tim Cook have called for comprehensive privacy legislation. And a majority of the American people are behind them: according to a Pew Research Center poll, 75 percent of adults support stronger online privacy protections. The key

will be striking an agreement that uniformly protects consumers without imposing undue burdens on free enterprise.

This won't be easy, but Congress is up to the task. As the former staff director of the Senate Republican High-Tech Task Force, I helped craft the CLOUD Act—one of the most important pieces of data privacy legislation to pass Congress in the last decade. What helped get the CLOUD Act across the finish line will also help with a federal privacy proposal: strong (and growing) bipartisan support.

Both Republicans and Democrats have long recognized the need for a federal framework—and that need is greater today than ever before. By passing national data privacy legislation, Congress can give Silicon Valley a competitive edge over China and help ensure US digital hegemony in the 21st century.

Matt Sandgren is the executive director of the Orrin G. Hatch Foundation, the former staff director of the Senate Republican High-Tech Task Force, and a 15-year veteran of Capitol Hill.