Samm Sacks, Yale Law School & New America

Graham Webster, Stanford University

Address Data Security Risks from China with Comprehensive Legislation

The United States needs a federal privacy law and higher cybersecurity standards—a patchwork of executive actions and politicized bans leaves Americans vulnerable.

One thing that Democrats and Republicans agree on is the need for a **comprehensive federal privacy law**. Americans have the right to control their personal data, including where it goes, and need better protection from hackers—so said Representative Cathy McMorris Rodgers (R-Washington) and Senator Maria Cantwell (D-Washington) last year, unveiling their bipartisan, bicameral draft legislation. In 2023, Rodgers made a similar case while **chairing a hearing** on how to "win the future versus China."

Policymakers in both parties rightly recognize that U.S. data remains vulnerable to a host of threats, at home and abroad. The Biden administration did take action, investigating **connected vehicles from China** that some believe could be used to spy on or sabotage American life, and establishing a **new program** to scrutinize where Americans' sensitive personal data is flowing, including to China. Biden also signed a law that would ban TikTok if its Chinese owners would not sell the app.

But threats from China are part of a much bigger set of questions about how to secure data and ensure the integrity of diverse digital systems in an interconnected world. These challenges blur the boundaries between cybersecurity, privacy, and national security—as evidenced by the Biden administration's revelations that it identified Chinese state hacker groups deep in **critical infrastructure** and **telephone networks**.

Bipartisan support for protecting Americans' data and for defending against China creates an opportunity.

In an era when U.S. policymakers are so often bitterly divided, bipartisan support for protecting Americans' data and for defending against China creates an opportunity. Lawmakers should advance a U.S. vision for governing digital technologies and an internet that is at once protective, secure, and open. Legislation is needed that addresses how all online platforms collect, retain, and share data, and that demands high standards of security and safety for connected infrastructure—regardless of where the threats emanate from.

Targeting solely Chinese companies just won't cut it. If one app that poses perceived risks is shut down, there will be others, foreign and homegrown. When sales to Chinese data brokers are banned, spy agencies can set up a front somewhere else. Therefore, even where the concern is China specifically, data protection and cybersecurity need to improve comprehensively to meet the challenge. Besides, the executive branch can be capricious: Trump proposed the TikTok ban in 2020, but he campaigned against it in 2024.

USEFUL EXAMPLES

Because the United States is late to the data protection game, legislators can learn from what has come before. The European Union implemented its data privacy law, the General Data Protection Regulation (GDPR), in 2018 with a focus on **individual data rights**. China, for its part, passed its Personal Information Protection Law in 2021, adopting much of the European model but also focusing on **national security risks**.

Where these and other attempts succeed, and where they fall flat, is instructive. GDPR gave rise to the cumbersome 'allow' buttons on every website that are engineered to encourage people to consent to data collection—not an inspiring example. Experts have argued that **moving away from consent-centric** approaches could give people more control over their data. GDPR also doesn't account for the scale of data collected, so small startups have to comply with all the same requirements as multi-billion-dollar tech giants.

Meanwhile, China's data laws and slow regulatory rollout have increased business uncertainty for years. And they do not protect Chinese users from state surveillance. But the same laws have **helped protect Chinese consumers** from once common practices like price discrimination.

Overseas examples aren't the only models for Congress to build on. **State-level privacy laws** that have already overcome U.S. political divides also illuminate a way forward. Most of the 20 existing state privacy laws, including those in **Delaware**, **Connecticut**, and **Indiana**, have achieved a workable balance. They require greater checks on companies' collection and use of data. At the same time, the laws do allow for multiple uses of data—through disclosures to the consumer—for developing new AI products and services, and for public interest research.

There is also a role for technical solutions to data protection and security challenges. In the wake of the discoveries about Chinese hacker groups and telecommunications, the FBI and Department of Homeland Security **urged** Americans to use encrypted messaging apps. U.S. legislation could also push industry to incorporate security and privacy into the design process and recognize that technology will change over time. A **2023 White House strategy** calls for investing in the development of privacy-enhancing technologies to unlock the utility of data. These too could be built into comprehensive legislation and supplement its implementation.

A WIN-WIN

Unfortunately, at the national level, privacy legislation is stuck. Novel **data minimization proposals** that would strictly limit collection and use of personal information have created a logjam between Democrats and Republicans. Any legislative compromise will upset some corporate interests and committed advocates. But Americans will be served better by an imperfect national standard based on a consensus developed by progressive and conservative states than by today's data Wild West.

The United States should strike its own balance—and it just might. For all the domestic political discord, there is a bipartisan consensus that China poses threats that must be managed. Skepticism of unchecked data collection by Big Tech platforms is also widely shared. The new Congress, with some determination from key members, could finally protect U.S. citizens' privacy, shore up cybersecurity—from industry to infrastructure—and, in the same stroke, frustrate present and potential threats from China.

FURTHER READING

Sacks, Samm, and Peter Swire. "A Framework for Assessing U.S. Data Policy Toward China." *SSRN Electronic Journal*, SSRN: 4601794, June 2023. **http://dx.doi.org/10.2139/ssrn.4601794**.

Sacks, Samm, Krystal Chen Zeng, and Graham Webster. "Moving Data, Moving Target." DigiChina. Stanford University, October 25, 2024. **https://digichina.stanford.edu/work/moving-data-moving-target/**.

Oliver, John, host. "TikTok Ban: Last Week Tonight with John Oliver (HBO)." YouTube, November 21, 2024. Video, 27:22. **https://www.youtube.com/watch?v=5CZNlaeZAtw**.

Samm Sacks is a senior fellow at Yale Law School's Paul Tsai China Center and a cyber policy fellow at New America. She is writing a book (Chicago, forthcoming) on the geopolitics of data privacy and cross-border data flows. Sacks launched the industrial cyber business for Siemens in Asia and worked as an analyst and Chinese linguist with the U.S. government. She also led China technology analysis for the political risk consulting firm Eurasia Group.

Graham Webster leads the DigiChina Project at Stanford University's Center for International Security and Cooperation. As a senior fellow and lecturer at Yale Law School, he was responsible for the Paul Tsai China Center's U.S.-China Track 2 dialogues and led programming on cyberspace and high-tech issues. He wrote for CNET News on technology and society from Beijing, worked at the Center for American Progress, and taught East Asian politics at NYU's Center for Global Affairs.