



Identifying the Next TikTok: Which Apps Could Washington Target Next?

September 13, 2024 **Joel Thayer** *American Foreign Policy Council*

Related Categories: Cybersecurity and Cyberwarfare; Democracy and Governance; Public Diplomacy and Information Operations

In the first Cold War, the United States and Soviet Union clashed repeatedly through satellite states and proxies. Today, America finds itself locked in great power competition with the People's Republic of China (PRC). The digital age has reshaped this conflict in ways that make this second cold war categorically different from the first. The PRC has infiltrated numerous aspects of America's communications networks. With the promise of cheap labor, Beijing stole American intellectual property. With the promise of cheap equipment, it took control of multiple U.S. routers, backhauls, cell sites, and mobile devices. With the promise of cheap laughs, it captured Americans' attention and siphoned data.

Congress has responded in bipartisan fashion, passing most recently the Protecting Americans from Foreign Adversary Controlled Applications Act (the Act). The Act specifically mentions ByteDance and TikTok, which means that they and their subsidiaries are required to divest. However, the law's scope is not limited to just TikTok and ByteDance. The Act broadly applies foreign ownership restrictions to apps operating within the United States. In so doing, it follows legal frameworks that America has implemented in separate contexts like telecommunications services, broadcasters, banking, and energy, to name a few.

Likewise, the TikTok bill is bigger than TikTok. It could prove to be a useful tool to rid America's networks of insidious malware. What follows is an outline of the Act's substantive provisions, and an analysis on how the Act's framework can apply to other Chinese-based applications posing similar national security issues as TikTok and ByteDance. Specific attention is given to WeChat and Temu.