**The TikTok threat**

Mel Gurtov

Thursday, Apr 27, 2023

High-tech spying is in the news because of the one-sided, hypocritical debate in Congress on whether the popular app TikTok is actually a tool for Chinese government data collection on American users. The sensitivity of the issue has to do not only with rivalry with China but also the fact that the US government has recently been the target of hackers.

In November 2021 President Biden banned use of Pegasus, a powerful Israeli-made surveillance tool, by all US government agencies. His order came in the wake of two developments: hackers who used Pegasus to break into the phones of some State Department employees, and investigative journalism that revealed use of Pegasus by many governments, democratic as well as autocratic, to break into the cell phones of political opponents and human rights activists.

As the New York Times has just found, not all US agencies have apparently gotten the message; an unnamed government agency is said to be using the nearly undetectable surveillance device in Mexico. Meantime, the phones of 50 more US government employees have been hacked.

The US case against TikTok, however, sidesteps two matters: the US government’s own spying on citizens under cover of law, and the questionable political motives that seem to dictate the specific effort to kill TikTok.

Congress members are far more concerned about the US government as victim of spying than as perpetrator. We’ve just been reminded of that with the top-secret documents hacked by an Air Force reservist that revealed US spying on various allies as well as on Russia.

That spying is widely considered legitimate, but Congress members prefer to forget the long history of government spying on unsuspecting citizens, a history that goes well beyond the Cold War. Various agencies – Homeland Security, the FBI, the Department of Justice, the State Department – have monitored social media to report on ‘national security’ dangers.

Leaders of Black Lives Matter, left and right political parties and resistance groups, immigrants from Muslim and socialist countries, environmental activists – the list of targeted groups is long. To that list should be added the mainstream social media – Facebook, Twitter, Google – that have given government agencies access to users’ personal information and communications. Their data collection probably exceeds TikTok’s, but somehow they are not considered national security threats.

Legislation passed with strong bipartisan support in Congress has cemented the government’s right to invade privacy, most recently to combat terrorism. The Foreign Intelligence Surveillance Act (FISA) of 1978 permits electronic and other means of surveillance of US citizens suspected of being “agents of foreign powers.” A FISA court, consisting of 11 federal district judges appointed by the chief justice of the Supreme Court, considers applications to carry out surveillance and may issue warrants based on probable cause.

FISA has been amended several times – the USA Freedom Act (2015) is the latest version – but has been challenged as an unconstitutional violation of personal liberty. That’s because catching terrorists was used to justify creation of a huge data base that went well beyond counterterrorism.

The Freedom Act puts some limits on metadata collection, but still has provisions for warrantless surveillance, for instance against whistleblowers such as Edward Snowden. Courts have rarely ruled against US government intrusion, usually when national security is the justification.

But then there’s the 2013 case in which the Supreme Court, in a 5-4 ruling, decided that Amnesty International lacked standing to challenge FISA. The case was brought against James Clapper, then director of national intelligence.

To judge from the virulence of the rhetoric, TikTok is one of China’s biggest threats to US national security. Congress members actually seem to believe that killing off TikTok would be a major victory over a malevolent foreign power – a way to “protect Americans from the technological tentacles of the Chinese Communist Party,” as House Speaker Kevin McCarthy put it. TikTok is owned by Bytedance, a Chinese technology company, but its CEO claims the company does not share data with the Chinese government, has independent management, and is willing to store its US data in the US.

Now I have to say that I have never used TikTok, nor do I even know anyone who does. But the roughly 150 million Americans who use it swear by it; TikTok has become an icon of US culture.

A number of countries, including the European Union, Denmark, New Zealand, and India, have restricted government use of TikTok or banned it altogether. But I have yet to see evidence that TikTok is channeling Chinese propaganda or amassing anyone’s personal data to be offloaded to Beijing.

Yet Congress members, and the Biden administration, are determined either to ban TikTok or force its sale, which the Chinese government opposes on the grounds that would harm investments in the US. The political lineup against TikTok mirrors the bipartisan consensus in Congress that is hostile to most anything Chinese-made or owned.

Allowing TikTok to continue operating but ensuring that its database resides in a US server such as Oracle would seem to be a reasonable answer for those who insist TikTok is a security threat. At one time the administration supported that idea.

But now we learn that Biden has “endorsed a bipartisan Senate bill that would give the Commerce Department the clear power to ban any app that endangered Americans’ security.”

That’s the authoritarian solution, but it would probably satisfy the China hawks, who love the prospect of turning public attention away from America’s real security issues. Their posturing on TikTok may fool some people, but far from strengthening national security, it reveals how insecure government leaders are when dealing with China.

The article was originally published as: ‘TikTok and US National Insecurity’. Courtesy: Counterpunch.org