While awaiting TikTok's fate, we must protect our data

Chicago Tribune · 5 Apr 2023 · By Sheldon Jacobson Sheldon Jacobson is a professor in computer science at the University of Illinois at Urbana-Champaign. A data scientist, he applies his expertise in data-driven, risk-based decision-making to evaluate and inform public policy.

Few, if any of us, live in a place like Mayberry, the fictitious town in North Carolina that provides the bucolic setting for the 1960s television program "The Andy Griffith Show." Before we leave our homes, we secure our doors and windows. When leaving our vehicles, we lock their doors. We install complex security systems to protect our property against intruders.

Yet when we enter the cyberworld, we act like it is a version of Mayberry. We tend to act nonchalantly with our personal information. We rely on companies and their websites to protect our data, no matter how sensitive it may be. We use our smartphones in a manner that often exposes our personal information to cybercriminals and bad actors.

Few companies intentionally misuse or expose their clients' personal data. In spite of all the safeguards deployed, security breaches occur with regularity. An enormous cybersecurity industry has surfaced, with revenues on the order of hundreds of billions of dollars annually.

The current debate over TikTok focuses on the app's use of Americans' personal information. The primary driver of such concerns is that the majority stakeholder of TikTok, ByteDance, is based in China. The fear is that the Chinese government will access such personal information and use the platform for targeted messages fomenting social unrest and angst.

Lawmakers worry that such actions pose a threat to our national security. Several countries have banned TikTok on government devices and computers. Yet the cyberworld has few borders, and those that exist can be circumvented with some technical acumen.

The TikTok controversy reflects ongoing tensions between the United States, the world's dominant superpower, and China, a superpower wannabe. Like two heavyweight wrestlers locked in a hold, each is attempting to gain an advantage that can flip a neutral stance into a position of strength.

Their struggles cover a wide swath of issues, including microchip manufacturing; the role of Taiwan; intellectual properties, with economic and trade implications; and rare earth metals that are needed for national defense and numerous technologies.

The U.S. government would like to see TikTok owned by one or more U.S. companies. ByteDance is 60% owned by non-Chinese investors, including U.S. investment firms. China does not support such a full transfer of ownership, no matter how large the sale price would be.

The RESTRICT Act, a measure recently introduced in the U.S. Senate with bipartisan support, would limit foreign influence by tech companies, with TikTok clearly in its crosshairs. However, giving the Department of Commerce the power to take such actions is different from achieving the desired result.

In reality, the types of data TikTok is collecting may not be that dissimilar to the data collected by other social media companies that are U.S.-owned. The concern is that data collected by a company based in China has national security implications, based on the relationship that the U.S. has with China.

Of course, a simple solution for all users is to assume that any data they share on the internet is being seen and used by cybercriminals and foreign nations. This would require a massive change in how people in the U.S. use the internet and social media.

Cybersecurity companies always indicate that the greatest vulnerability of any cybersystem is the user and their unwillingness or inability to follow sound cybersecurity protocols. With social media, users freely share information that is akin to providing a key to their home and information on when they will be away.

The TikTok debate will continue. The best protection that any person can take on TikTok, or any social media site, is guarding personal information and taking responsibility for doing so. Assuming that a company will handle all cybersecurity issues and keep such information private is risky, and even naive.

With regard to TikTok, if the Department of Commerce is successful in closing down access to the website in the U.S., what tool will people gravitate toward? Alternatives already exist that can fill this void. The question is why these other tools are not being used to the same degree as TikTok, which now has 150 million U.S. registered users.

The freedoms that Americans enjoy also expose people to personal risks. When such risks threaten national security, they no longer are personal. The RESTRICT Act, much like the Patriot Act, recognizes such risks. Whether TikTok is a real risk or a false alarm remains to be seen. It is likely something in between. Over time, more will be revealed.

Until then, everyone has a responsibility to act responsibly on the internet, not only for their own personal security but also for the security of the nation.