Don't Ban TikTok

by

Phil Rasmussen

For the past month there has bee a lot of discussion in Congress and elsewhere about banning TikTok in the US. Some members of the far left believe that to ban it is an assault on the First Amendment (Freedom of Speech). The conservatives and middle-of-the ground politicians believe the social media application is a security risk to the nation.

Regardless of your stance with regard to TikTok, banning it, in one sense, is not the answer. The concerns with TikTok include:

- Gathering data on TikTok users
- Pushing social, political, and economic agendas favorable to the Chinese Communist Party
- Targeting the youth of the free world (US, Europe, etc.) with communist propaganda
- Acquiring classified military, political, and economic data on government, business, and industry computer networks.

These four concerns alone should be paramount in every person's mind who uses ANY social media platforms. It is well known that "Big Tech" gathers, extrapolates, and routes the data it gathers on its users to push "content" that the tech industry believes the users need or want. Much of the data collected is sold to companies for marketing purposes. We also know that the data collected is used to censor those who do not agree with the social, political, or economic viewpoints of various tech industries.

All of the social media platforms collect three types of data – analytics, personal, and espionage (corporate and political).

Analytics

While analytics covers the entire spectrum of data collection, it is typically aimed at collecting **Performance Data**. This type of data includes:

- Amount of website traffic/site visits/page views
- Number of searches for keywords
- Content viewed
- Number of followers
- Number of subscribers

- Number of websites linking to your website
- Number of comments and/or likes on posts
- Website performance (speed, bad coding, dead links, etc.)

Personal

The most common personal data that most people realize is collected include:

- Name
- Age
- Race
- Gender
- Phone number(s)
- Physical location
- Email address
- Driver's license number
- Social security number
- Credit card usage and information
- Other identifiable information

What people do not realize is that there are **52,000 unique attributes** that social media platforms use to classify their users. Read again that number of unique identifiers are to classify **YOU** if you use ANY social media.

Espionage

Espionage is nothing more than spying. It can be out in the open (overt) or it can be secretive/hidden (covert). We generally think of espionage as between different countries or governments. However industrial and commercial espionage, like political espionage, has existed since the time civilization began.

Through online comments, purchases, sites visited, social media collects and extrapolates your data attributes in order to target you directly (with ads, coupons, content, etc), or supplies the analysis of your date to foreign and domestic governments, industries, businesses, and educational institutions. The more benign targeting is to direct your buying and spending habits. On the other hand, the most dangerous targeting is to brainwash you with regard to political agendas and rearranging our social environment.

As mentioned at the beginning of this commentary, banning TikTok is not the answer. The accessibility to the data collected by ALL social media platforms needs to be examined. While the government is in the throes of banning TikTok on all government

computer systems, there is no talk about banning any of the other platforms. Regardless of who owns, develops or maintains a social media platform, ALL platforms should be banned on government computer systems. They are ALL a security risk to the political, economic, and social environments of our nation.

But banning the platforms on government systems is only one part of the solution to protect our nation and its citizens. The second step is to insure that there is no way that these platforms or the organizations they sell their data to, can use the date to manipulate individual, social, or political thought and outcomes.

To carry out this second part, it is necessary to eliminate a platform's ability to:

- collect personal information
- push content

All social media platforms should be able to track specific data such as those listed in the Analytics section above. All other data collection should be prohibited as it essentially comes under the heading of spying/espionage!

Email your congressional representatives and ask them to put a stop to Big Tech's data collection and/or sale of personal data.