# TikTok Not the Problem: Data Privacy Is

Paul S. Wang, Sofpower.com

May 13, 2023

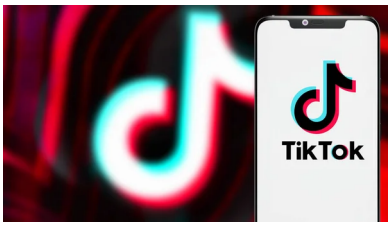
TikTok is a popular short-form video app that has raised concerns about its potential threat to US national security, as highlighted by both the Trump and Biden administrations. The controversy revolves around data security and privacy concerns.

In this article, we will delve into what TikTok is and explore the concept of privacy protection, which is crucial for everyone in the digital world, particularly for computational thinkers.

This post is part of our *Computational Thinking* (CT) blog where you can find many other interesting and useful articles.

## What is TikTok?

TikTok is a short-form videos app and social media platform, very popular, especially among young people. TikTok supports 1080x1920-pixel short videos. Initial success was built on rapid-paced 7-15 second videos. Over the last few years, the platform extended its maximum video length all the way to 10 minutes.



It is available for free download and install on most devices including smartphones, tablets and desktops. But it is usually used on smartphones. You can watch many video clips, engage with what you like, skip what you don't. There's something for everyone. The app also provides great and easy-to-use tools for creating original videos, adding special effects, filters, music, and more.

## Popularity of TikTok

TikTok and its Chinese counterpart Douyin (抖音) are owned by parent company ByteDance (字节跳动). Douyin was launched in late 2016 and, according to Wikipedia, had 100 million users within a year, with more than one billion videos viewed every day.

TikTok, an international version of Douyin, was launched in 2017. After merging with Musicaly.ly (another Chinese company), TikTok became available globally. TikTok and Douyin are managed and operated by two independent companies, the former by TikTok Inc. registered in the US (located in LA) the latter registered in China. They also do not offer exactly the same features.

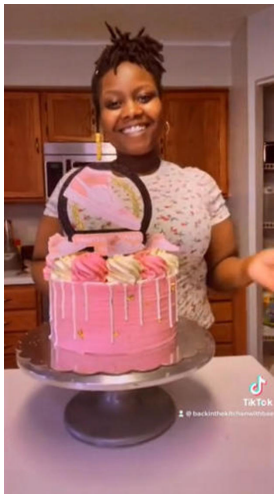

(*image: Influencer Marketing Hub*)

A December 2021 Forbes article had the title "*TikTok Surpasses Google, Facebook As World's Most Popular Web Domain.*" This is quite a feat considering that the Google domain includes Search, Maps, Translate, Photos, Flights, Books, and News, among others and still people visited TikTok more than all these other services combined.

With (1) a great recommendation engine based on its proprietary algorithms– rivaling and overtaking those of Amazon, Netflix, and Youtube; (2) a set of super easy-to-use video creation tools; and (3) over 1 billion active monthly users; TikTok became very popular and successful in a very short time.

CBSNews.com reported this interview:

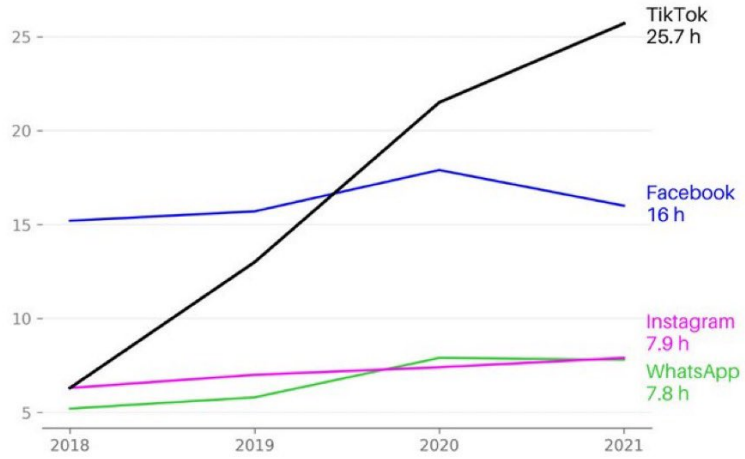
> *Baedri Nichole, founder of a bakery in Columbus, Ohio, said of TikTok, "It's taught me how to do e-commerce, how to get into shipping. and more than anything, I also use it to find my next customer. Prior to getting on TikTok, we were struggling even to turn a profit."*
> *And now? "We've seen at least a 300% increase in profit," she said.*




*Baedri marketing her bakery business* (image: tiktok)

From wallaroomedia.com: "*The Top 1000 advertisers are drastically increasing their spending on TikTok. Ad impressions there cost 50% less than on Instagram Reels, 33% less than on Twitter, and 62% less than on Snapchat.*"

Moreover, as the next chart shows, since 2021, user engagement with TikTok has overtaken that of other major social media.




*Average monthly hours spent per user* (image: thenetworkec.com)

Given its enormous popularity, why does TikTok repeatedly face bans in the US? The main reason seems to be concerns about data privacy and security, especially because TikTok's parent is a Chinese company.

But can banning TikTok or forcing its sale to a US company really solve the data privacy issue?

## Data Collection and Protection

In the digital age we live in a global village where information travels at the speed of light and is constantly being collected, stored, shared, and analyzed by companies, governments and giant corporations, including Facebook, Google, Amazon, Walmart, Microsoft, Apple, Youtube, TikTok, Uber, and Lyft, as well as government agencies (see the next section on who collects what).

The data collected are huge and relate to every aspect of our activity, behavior, preference, and lifestyle. Data are generated and saved in databases, mostly without our noticing or consent. Such data sets are then used for *data mining* to discover hidden insights for various purposes.

*Data Mining*

Here is a well-known example of data mining. In 1992, Karen Heath discovered within retail sales data, not through sophisticated data mining techniques but simple SQL database queries, the now famous *beer and diaper correlation*—men between 30-40 years in age, shopping between 5pm and 7pm on Fridays, who purchased diapers were most likely to also have beer in their carts. Thus, retail outfits should place beers next to diapers to increase sales.

Today data mining is used widely. For example in healthcare, data mining enables more accurate diagnostics, more effective treatments. In addition it can also suggest more effective, efficient and cost-effective management of health resources. Also it help detect fraud and irregularities.

Such data collections are very valuable and must be protected well against loss, theft, and misuse. Of course everyone is and should be concerned about personal information falling into the wrong hands. **Without adequate privacy protection of sensitive personal data we are laid bare online and there is no place to hide**.

However, if we keep everything about us secret, we won't enjoy many of the advantages and conveniences the digital world can provide. For example, your current location is used for travel navigation and for finding near-by stores and services. Your age, sex, interests, and even web browsing history can lead to better recommendations for goods and services.

To safeguard our privacy, we first need to know how our data are collected.

## Who and Where

Computing hardware such as desktops, laptops, and smartphones, as well as operating systems, web browsers, email apps, texting/chat apps, navigation apps, and audio/video/camera apps, along with individual websites, all have the capability to collect and use our personal data. This data may also be stored locally or in the cloud, and shared with others.

For instance, email apps may collect your contact information including names, email addresses, phone numbers, and addresses. Smartphones can track your location, travel history, and phone calls. Browsers can keep a record of the websites and pages you visit. Search engines may remember the details of every search query you make, including the time and place. Websites may store your authentication information, such as usernames, passwords, and email addresses, while e-commerce sites can track your purchasing history and interests.

Furthermore, various service providers such as airlines, hotels, cellphone carriers, credit/debit card terminals, taxi/ride providers, gas stations, parking lots, and toll booths may track your whereabouts. Healthcare facilities like hospitals, doctor's offices, and pharmacies may also collect and share your health information, which may include sensitive data that you would not want to be made public. Similarly, banks, stock/mutual fund companies, and credit unions may collect and use your financial data.

Therefore, it is true that when using the internet, you are inadvertently disseminating information about yourself.

## Data Privacy Laws and Regulations

In the US, there are several federal and state laws that protect *Personally Identifiable Information* (PII), which includes any data that can be used to identify an individual.

The most important federal law is the Privacy Act of 1974. It regulates the collection, use, and dissemination of PII by federal agencies, and provides individuals with certain rights to access and amend their own records.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 sets national standards for protecting the privacy and security of people's medical records and other health-related information.

The Gramm-Leach-Bliley Act (GLBA) of 1999 requires financial institutions to safeguard nonpublic personal information of customers, such as

credit scores, and banking information. In addition, there are several state laws that protect PII.

Overall, these laws and regulations aim to ensure that personal information is properly collected, used, and safeguarded, and that they have certain rights to access and control their own information.

In the European Union (EU), personal data protection is governed by the General Data Protection Regulation (GDPR). which provides a comprehensive framework for protecting the privacy and rights of individuals in the EU. The law applies world-wide as long as the PII belongs to EU citizens or residents.

The GDPR provides a unified and consistent framework across all member states of the EU. Whereas the US data protection laws tend to be sector-specific and often vary from state to state.

Overall, the GDPR is generally considered to be more comprehensive and stringent than the data protection laws in the US. The GDPR places a greater emphasis on individual rights and places stricter requirements on organizations that collect and process personal data.

## Protect Your Own Privacy

Think relying on governments or laws is not enough? You are not alone. Here are some steps you can take to protect your privacy:

- Guard your PII. Be cautious sharing personal information such as full name, date of birth, Social Security number, home address, and phone number.
- Use strong passwords and two-factor authentication and a password manager.
- Update your operating system, web browser, email agent ASAP.
- Consider using a virtual private network (VPN) which encrypts your internet connection to protect your online activities from prying eyes.
- Be careful when using shared computers and public Wi-Fi. Do not conduct sensitive business on them.

- Before you download and install an app, you can and should learn exactly what data it collects and its data privacy and protection practices. Normally, you can find detailed information in the app's user agreement to which you must first give your consent before successful installation. For example, TikTok provides that information in its data safety section.

- Examine and manage permissions to apps on your smartphone and other systems. Deny access permissions when appropriate; similarly for the privacy settings on your social media accounts and other online services.

- Consider using privacy-focused tools such as browser extensions that block ads and trackers, encrypted messaging apps, and privacy-enhancing search engines.

Thus you can take proactive measures to protect your personal information and enhance your privacy online.

## Summary

In the digital age, information and data are collected by various platforms, including TikTok, Facebook, and Google. These data collections can be used for both beneficial and harmful purposes.

TikTok, like other social media platforms, has similar data collection and privacy policies. However, due to its popularity, TikTok has raised concerns about data collection, privacy protection, and potential threats to US national security. It is important to carefully consider the evidence provided by the government in terms of protecting national security and to exercise personal caution when using TikTok or any other app.

Governments should create and enforce sensible laws and regulations to address people's privacy concerns. Meanwhile, individuals, especially those who are computational thinkers, should proactively protect their own privacy as relying solely on laws and regulations may not be the best defense.