Understanding the Security and Privacy Concerns of TikTok

One PPG Place, Suite 1700
Pittsburgh, PA 15222
(412) 697-5200
www.schneiderdowns.com

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

Understanding The Security and Privacy Concerns of TikTok

In today's digital society, our personal lives are often chronicled through the lens of our camera phones and posted on social media platforms for our friends and followers to see.

While social media offers a great channel way to share experiences and memories with those who cannot be there in person, these platforms also lead to security and privacy concerns. Specifically, the usage of TikTok (the "Platform") has received ample attention from privacy advocates and security experts alike.

It is important to note that TikTok is a social media platform that, like other similar applications, is intended to share data and information with a large network of users. However, the full extent of what is being shared is often misunderstood.

Our intent here is not to dissuade use; rather, it is to educate users on what information they are actually sharing on TikTok, with whom that information is being shared, and why the Platform is often regarded as a security risk.

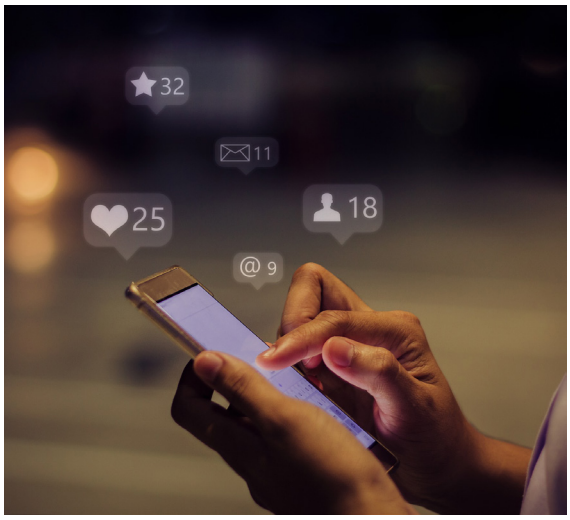
TikTok – What Are You Actually Sharing?

TikTok was first launched internationally by parent company ByteDance in 2017, and as of Q3 of 2022, it has upwards of 1.5 billion active monthly users. TikTok expects that it will exceed 1.8 billion users by the end of 2022. With that, the prevalence of the Platform is evident. What is not, however, is the understanding of what information is being collected on the backend.

TikTok's Privacy Policy outlines what information "may" be gathered from its users, and what is described therein is generally expected from a social media provider. For example, some information that is gathered upon registration is the user's age, username and password, email or phone number, name and profile image.

However, it is reasonable to assume that most users are not aware what the Platform collects beyond basic profile information. It is also worth noting that users agree to these Terms of Service and policies upon registration to TikTok. In addition to profile information, TikTok will collect any user-generated information that is uploaded within a user's account, regardless of whether the post is saved or shared. This includes comments, photos, livestreams, audio and video. Additionally, the Platform can access (with permission) your device's clipboard and collect any text, images or video that may be present.

TikTok can also access and collect information from any other login sources or those that are linked to a user's profile. This can include Google, Facebook, Twitter or any other service used to authenticate users to TikTok. Furthermore, third-party services such as advertising partners, data providers and analytics providers can be leveraged by TikTok to collect information about its users.



Listed in the Privacy Policy as information that is "automatically collected," specific device information is also obtained from users. Notably, device IP addresses, mobile carriers, "identifiers for advertising purposes," device system and model types, installed applications and file names, keystroke patterns, connected audio devices (i.e., speakers or smart home devices) and location data. The Platform will even access and collect information on audio settings and the device's battery state.

Perhaps the most concerning issue from a security and privacy perspective is that TikTok collects audio and video information that can be used to pinpoint locations and specific demographics. Through analysis of audio and video context, TikTok can use collected data to identify "the objects and scenery that appear" or use "the existence and location within an image of face and body features and attributes" to identify users or the locations in which the content was created.

The stated reasoning for this is to enable effects on the video, moderate content, classify demographics and recommend content and advertisements. However, there could be additional uses of facial and environmental recognition not explicitly listed. TikTok may also generate and collect text of any words spoken in user content.

What Is Done with User Data on TikTok?

According to TikTok's Privacy Policy, the Platform does not sell personal information to any third parties, but will share personal information with "service providers and business partners to help [them] perform business operations." All this information may also be shared with organizations within the corporate group of ByteDance, the China-based parent company of TikTok.

Any collected information can then be used to customize content seen on the Platform, help TikTok assess and understand user activity (even across devices used by that account), interpret additional information about users (age, gender, interests) and advise on algorithms used to moderate what users see.

Other social media platforms arguably follow similar models of information collection and sharing. So, the question is, why is TikTok often singled out for it?

The combination of what information is collected, the algorithms used to moderate user content, and the presence of ByteDance is what causes concern among professional security and privacy communities.

Furthermore, all keystrokes logged within TikTok's app and browser means that they have access to every password, credit card number, and other sensitive user data that is typed. Taxonomies of user data and behaviors are being chronicled and catalogued, to be exploited for financial gain or blackmail.

TikTok And National Security

In November 2022, FBI Director Christopher Wray testified to Congress that the FBI has national security concerns regarding the use of TikTok in the U.S. Director Wray cited that ByteDance being a Chinese company is concerning, primarily because this includes "the possibility that the Chinese government could use it to control data collection on millions of users, or control the recommendation algorithm which could be used for influence operations if they so choose, or to control software on millions of devices."

Generally speaking, the concern is that TikTok can be used to influence American perception through data collection and content moderation.

The ability to moderate user content (i.e., controlling what users see) is typically justified by platforms for advertising or safety reasons. It can be argued that this is the case for TikTok as well, but the issue is that TikTok is used for more than just watching videos. A recent Forbes article cited that the number of U.S. adults who regularly access TikTok as a news source rose from 3% in 2020 to 10% by November 2022. Additionally, Pew Research found that 26% of all U.S. adults under the age of 30 routinely get their news updates from TikTok.

Overall, the amount of TikTok users who refer to the Platform as a regular news source rose from 22% in 2020 to 33% in 2022. It is important to note that other social media platforms have not seen such growth in this regard. In other words, TikTok is increasingly becoming a news source and with that comes the potential for a foreign entity to effectively control what news is being shared in the U.S.

From an IT risk advisory and cybersecurity perspective, we can appreciate these concerns, especially with the parent company being located outside of the United States. TikTok's Terms of Service and Privacy Policy pay little attention to security, privacy and confidentiality, with the only mention of security in either document simply noting that "reasonable measures" to protect information are implemented, but security is not guaranteed.

Also, user information may be transmitted and stored in data centers that are outside of the U.S. With that, data can be stored anywhere and is accessible to anyone. The fact that user data is can be stored and viewed by agencies not listed naturally merits consideration from a risk management mindset.

We know how fulfilling and fun sharing your experiences with friends and family on social media can be, just be mindful of what else you may be agreeing to share when signing up.

About Schneider Downs Cybersecurity

The Schneider Downs cybersecurity practice consists of expert practitioners offering a comprehensive set of information technology security services, including penetration testing, intrusion prevention/detection review, ransomware security, vulnerability assessments and a robust digital forensics and incident response team. In addition, our Digital Forensics and Incident Response teams are available 24x7x365 at 800-993-8937 if you suspect or are experiencing a network incident of any kind.

To learn more, visit our dedicated Cybersecurity page or contact the team at cybersecurity@schneiderdowns.com.

Want to be in the know? Subscribe to our bi-weekly newsletter, Focus on Cybersecurity.