

TikTok, Privacy, and National Security

Petra Mitchell

Introduction to Media Theory

Dr. Andrew Iliadis

March 5, 2021

In an age of social media and digital communication, one is able to easily share information for anyone in the world to see, but navigating the line of what to share or not share comes with more difficulty. Human beings have a natural desire to connect with others and the rise in virtual ways of connecting has only encouraged and supported this desire in people. This connection, however, comes with some level of permanence to the information one chooses to put on social media. Once one chooses to post a picture, add a friend, like a post, send a direct message, create a video, or even simply sign up for a social media app, they are on some level sharing that information with someone. If an account is made private, that information may be viewable only by people they chose, while public accounts can be viewed by anyone, but public or private- the social media company itself is able to view and collect any of this seemingly personal information that one agrees or chooses to share.

These ideas of privacy and privacy ownership on social media are particularly notable on the short-form video sharing platform known as TikTok. Compared to other popular social media platforms, TikTok is unique in its more recent popularity with the Gen Z population, and unlike Facebook, Snapchat, or Twitter which are American-owned companies, TikTok is owned by the Chinese company ByteDance. This ownership alone has prompted many questions and concerns over information shared within the app and if it presents a potential threat to personal privacy and even national security. The concept of privacy in itself can be complicated to navigate, especially as “Organizations, populations, and governments differ widely on how best to handle such issues, and countless factors shape their preferences and views” (Gupta & Brooks, 2013).

When having fun making videos, sharing posts with friends, and interacting with new people, it becomes easy to forget that TikTok is automatically collecting data on one’s messages, location, device information including apps, IP address, keystroke patterns, as well as user

metadata, and much more (Private Policy, 2020). Information like this can be used in a variety of ways and once aware of its collection, people want to know what companies like TikTok are doing or are capable of doing with this information. It is important to also note that users do give permission for TikTok to collect such information. Like most media apps, in the act of creating an account, users are agreeing to both the terms of service and privacy policy of the platform even if they don't actually read them; a survey from 2017 found that 91% of people consent to such agreements without reading them, and that percentage only increases in younger populations (Guynn, 2020). The complexities of TikTok information ownership and social media privacy, in general, can be tied into and broken down by Sandra Petronio's communication privacy management theory. This theory, also known as CPM, can help in the understanding of private information on social media platforms and why the security of personal information on TikTok has been called into question.

Theory

Communication privacy management theory is "a description of a privacy management system that contains three main parts" including privacy ownership, privacy control, and privacy turbulence (Griffin, Ledbetter, & Sparks, 2019). Privacy ownership also includes privacy boundaries or the distinct separation of what one considers something to be private or public. In the context of social media and TikTok, as soon as someone chooses to share a piece of information, that information is no longer in the sole ownership of that person. This is because the agreed terms of the platform include that person allowing for the collection of such information by the company. The decision of whether or not to share information falls under privacy control. CPM argues that "disclosure is the process by which we give or receive private

information” and by extension, disclosure of private information is what strengthens relationships (Griffin, Ledbetter, & Sparks, 2019; Petronio & Venetis, 2017).

When privacy doesn't go the way one may want or expect, there is experienced privacy turbulence. Another argument of CPM is that “individuals believe they own their private information and have the right to control said information” which helps explain why users of social media platforms like TikTok have a desire to keep their information within their own control (Petronio & Venetis, 2017). Communication privacy management theory is also a rule based theory, meaning that privacy information is often controlled by the use of one's personal or implied rules for privacy. When sharing information with another person, or in this instance with a social media company, there are new collective privacy boundaries as multiple parties become co-owners of the same private information (Griffin, Ledbetter, & Sparks, 2019). In connection to TikTok, this collective boundary when sharing your information is presented to a user and stated in the company's privacy policy. People believe they have a right to their information but often neglect to appropriately focus on the collective boundaries of their information that they have already, and legally, agreed to.

Example

In August of 2020 former president of the United States Donald Trump signed an executive order “forcing ByteDance to sell TikTok's US operations” or otherwise banning it from the U.S. (Tillman, 2020). In order to understand why such an order was signed, one must first understand a brief history of the politics of TikTok leading up to this. With a dramatic rise in downloads and American users of TikTok beginning in October 2019, around the same time as trade conflict between the U.S. and China, U.S. officials began to warn against the use of TikTok. By July, former Secretary of State Mike Pompeo stated that there was consideration of

banning the app and warned that “your private information is in the hands of the Chinese Communist Party” (Fowler, 2020).

The overarching question here is whether or not TikTok could hand over user data to the Chinese government if demanded to do so and if this app is then a threat to American national security, but TikTok has repeatedly denied this (Graham, 2020). Both in claim by TikTok and in the privacy policy of the platform, user data is said to be stored outside of China and is thus not able to be ‘handed over’ to Chinese government (Graham, 2020). In the midst of this dispute, TikTok users seemed to split into distinct groups either advocating for the deletion of the app or for the executive order to be retracted and shared their thoughts on the issue under the hashtag: #TikTokBan. Around this time TikTok, with the support of many TikTok creators, filed a lawsuit against the Trump Administration in allegation that banning transactions with their parent company “infringes due process protections, goes beyond the purview of sanctions rules, and provides no evidence that TikTok is a national security threat” (Tillman, 2020). On September 20th under a new executive order by Trump, TikTok was removed from all app stores, however, the ban was blocked by a judge following the legal action taken, and though there were efforts by the administration to appeal this block- the app is no longer banned. The company is still majority owned by the China-Based parent company ByteDance, but TikTok has since made efforts to distance itself and shifted operations to be U.S. based and “isn’t even available directly in China” (Fowler, 2020).

Synthesis

This example, though dealing more with ideas on a greater scale of national privacy and security, can still be evaluated through concepts of communication privacy management theory. The conflict of the event can be seen through CPM as an extreme version of privacy turbulence.

There are two parties involved and a situation in which one party (the American people or more specifically American government) has doubts that the other party (TikTok and ByteDance) would abide by the collective privacy boundaries (privacy policy and terms) that they have stated and claim to hold.

Arguments of CPM that individuals believe they have rights to own and control their private information can also be expanded to this example. Even with no evidence suggesting that the information TikTok has could be exploited, the American government believes that America or an American company should have rights to own and control the private information and user data of TikTok. CPM has five factors that play into how privacy rules are thought and established and one of these factors is culture (Griffin, Ledbetter, & Sparks, 2019). In this example, TikTok, having come from a China based company, has roots from a different culture compared to that of those in the U.S. and thus could potentially hold a difference in their privacy rules and values. The end result of TikTok moving operations to the U.S., and the U.S. government no longer challenging the platform, is also reflective of the CPM idea of a mutual privacy boundary. Agreed upon by both parties on some level, the current standing and operation of TikTok is no longer a pressing threat or major cause of doubt to personal or national privacy.

References

- Fowler, G. (2020, July 13). Perspective | Is it time to delete TikTok? A guide to the rumors and the real privacy risks. The Washington Post.
<https://www.washingtonpost.com/technology/2020/07/13/tiktok-privacy/>.
- Graham, J. (2020, August 7). TikTok and privacy: What's the problem? Perhaps the video-sharing app gathers too much data. USA Today.
<https://www.usatoday.com/story/tech/2020/08/06/tiktok-any-worse-privacy-and-data-mining-than-facebook/3311726001/>.
- Griffin, E., Ledbetter, A. M., & Sparks, G. G. (2015). *A first look at communication theory*. “Communication Privacy Management Theory of Sandra Petronio” (pp.145-157) New York, NY: McGraw-Hill.
- Gupta, R., Brooks, H. (2013). Using social media for global security (1st ed.). Indianapolis, IN; John Wiley & Sons. Retrieved from
<https://learning-oreilly-com.libproxy.temple.edu/library/view/using-social-media/9781118442319/9781118442319p01.xhtml>
- Guynn, J. (2020, January 29). What you need to know before clicking 'I agree' on that terms of service agreement or privacy policy. USA Today.
<https://www.usatoday.com/story/tech/2020/01/28/not-reading-the-small-print-is-privacy-policy-fail/4565274002/>.
- Petronio, S., & Venetis, M. (2017, July 27). Communication Privacy Management Theory and Health and Risk Messaging. Oxford Research Encyclopedia of Communication.
 Retrieved 5 Mar. 2021, from

<https://oxfordre.com/communication/view/10.1093/acrefore/9780190228613.001.0001/acrefore-9780190228613-e-513>.

Privacy Policy. (2020, December 20) TikTok.

<https://www.tiktok.com/legal/privacy-policy?lang=en>.

Tillman, M. (Ed.). (2020, September 22). TikTok US ban: Everything we know about Trump's TikTok US 'ban'. Pocket.

<https://www.pocket-lint.com/apps/news/153872-tiktok-ban-us-trump-timeline-explained>.