

Privacy Terms: [TikTok](#), [Dubsmash](#)

I decided to do TikTok and Dubsmash. I recently saw an episode of “explained” on Netflix that explained how dance crazes start. Both companies are social media platforms where users create, upload, share, and/or interact with content on their mobile applications(usually in the form of videos lasting seconds to no longer than a minute). The episode mentioned Dubsmash, a precursor to TikTok, and how many users create content on Dubsmash but is “stolen” and made famous by other influencers on TikTok, thus raising the ethical dilemma of who really owns original dance content and can dance be copyrighted. Besides the point, both platforms have similar uses of user information.

Both TikTok and Dubsmash collect and store user information in their servers, mostly to create a sort of profile of who you are. A lot of the data deals with content shared on the platform, but some data can come from connected servers (if, for example, you decided to link your FaceBook with either site), apps on your phone, web searches and other histories, and ads from other websites you visited prior to going on their app. Device information is also collected, including SIM card, IP addresses, GPS, contacts, and so on. Both platforms also analyze any content stored on their servers to study images, videos, and audio to discern identifiable characteristics from the content (like distinguishing objects from people).

One interesting thing to note is that if Dubsmash is ever purchased or changes hands to another company, they do not guarantee what happens to your data after that point. TikTok does not mention anything in their Privacy Policy. In addition, both companies disclose that private messages sent to users on the apps are also monitored with the pretense of keeping their platforms safe from illegal activities. One surprising fact about TikTok is that they can collect and store payment information; Dubsmash does not include this in their policy.

Both services share user data with third-parties. While both parties claim they do not sell user information, they still work with third-party companies to collect information and target users with different ads depending on how they interact with the platform. In addition, they claim that while they may work with companies outside of the US, they are not responsible with how user data is used in those countries. This is worrisome because if

there is a data breach at one of those outside companies, it would be difficult to do anything about one's sensitive information. The company absolve themselves and the companies overseas could be difficult or impossible to reach and/or brought to justice.