Distant S.K.A.T.E. Privacy policy

For all sign in methods:
App Uses custom email, Facebook and Apple-ID logins to create user for your email.
Application uses Google Firebase products as a backend for data. You can read Firebases privacy policy here https://firebase.google.com/support/privacy. Firebase creates unique identifier for you. This identifier is linked with your email. Only the administrators can see your email and the ID. Other users will never see your email address. We'll send you only email verification and password reset emails. We store your wins, loses, last sign in time and Firebase ID as your user's information. Last sign in time is used to improve the new random game algorithm. You can delete your user and all related data from the settings.

For Facebook sign in:
This chapter is how we deal your data in addition of the above chapter.
While user connects app to Facebook user will be prompted to give access to public profile and friends list. If you grant access to both, Facebook specific ID will be stored to user's information. Facebook ID is used only to acquire corresponding Firebase ID. Only your Facebook friends can see your Facebook name in the game. App gets also list of your friends who has downloaded the app. It is used to let you play game with your Facebook friends. We don't store the friendlist. It is fetched from Facebook every time app starts.
To revert the data collection, you can navigate to settings and press Unlink Facebook button. This will remove stored Facebook ID and delete your Facebook user from our app.

Sent videos:
The tricks must be sent as an video file. Videos are stored in Firebase Storage. Only your opponent can get the link to the video. Videos are deleted after two weeks.

If you have any questions or you want more information, feel free to contact info@distantskate.com.