Mobile App Permissions

Anonymous Messaging App Sarahah to Halt Collection of User Data With Next Update

Sarahah, the anonymous messaging app that shot to the top of app stores earlier this summer, says it plans to remove a feature that uploads users' contacts, including phone numbers and email addresses to the company's servers, in the next update. The app's creator caught flak after The Intercept reported Sarahah was failing to ask for the user's permission before uploading the data.

The app, which allows users to anonymously [unless your email and phone are being shared] compliment or critique friends or co-workers, hit No. 1 on the App Store's list of top free apps in July. The app has been installed between 10,000,000 and 50,000,000 times on Android devices worldwide.

The above cautionary tale highlights the importance of knowing what type of information mobile apps want access to, and whether or not you should decide to give them permission to use it.

Mobile apps can request—or require—access to a broad range of information and resources, including:

- Your location
- Your phone’s hardware such as microphone and camera settings
- Network communications
- Personal information such as your email, phone number, and all your contacts

Android vs. iPhone

There are fundamental differences in how Android and iPhones (iOS) handle permissions. With Android, apps will tell you at the time you install them what permissions they require. It’s an “all-or-nothing” choice. If you are not comfortable with certain required permissions, you cannot disable some and approve others. Android apps will not run unless you give them all the permissions they ask for.

iOS devices (iPhone, iPad) take a different approach. They will not prompt you for a set of permissions at installation. Instead, you can modify the permissions for any app after it’s been installed. Disabling a permission (location service, for example), will not result in the app’s failure or removal.

The trade-off is: Android permissions are more granular, but iOS permissions can be individually modified.

Automatic vs. Manual Updates

Some apps offer the option of performing automatic updates, but from time to time, you will be prompted to perform a manual update. This is because the app developer has modified the permissions required, and now you must decide whether or not to accept them.

Finding Permissions

---

**iOS**

To navigate to specific permissions in iOS, open the Settings app and scroll down to find the app listings.

![Settings Menu]

Touch the app you want to investigate. In this example, we’re using Authenticator.

![Authenticator Settings]

You can see that this app wants to use the phone’s camera. You can disable this permission without breaking the app. There’s another layer here, so we’re going to drill down to see what Notifications includes.
There are a number of options here that govern how the app signals you and whether or not you want it to have access to the display screen when the phone is locked. Again, each one of these can be modified without disabling the entire app.

**Android**

As you know, Android apps prompt you at install for the permissions they require. To check those permissions after installation, open the Settings app, and select Applications in the left panel.

In the right panel, select Application manager.
Select an application. In this example, we’ve selected Chrome.

Scroll down to the Permissions section on the right to see a detailed list of the app’s permissions. This is a good example of how Android permissions are more granular than those available in iOS devices.
More Information
The following links offer additional information and advice on evaluating and reviewing app permissions.

**How App Permissions Work & Why You Should Care [Android]**

**Mobile app permissions: Who does it right?**

**Shining a Light on Mobile App Permissions**

**Understanding Mobile Apps**
[https://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps](https://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps)