# How to assess application security before installing on iPhone

We have been browsing and clicking to install the apps we need on our phones 'unconsciously'. But now Apple offers a new tool that allows you to mitigate that risk.

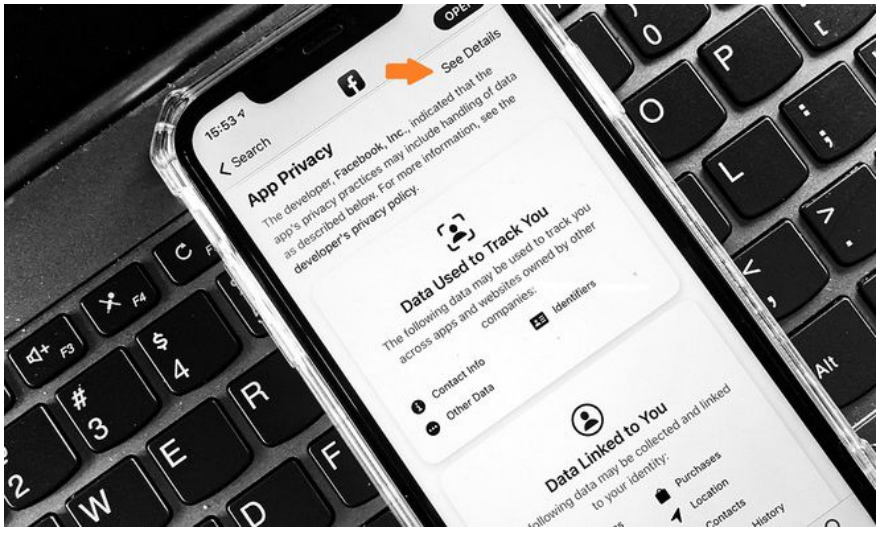
From the end of 2020, the App Store app store will start offering a 'App Privacy' label for all listed app categories. Through this information, you can get a more accurate view of how apps are tracking you, as well as make a decision about whether or not to download them via the How To Geek page:

## Why did Apple suddenly turn to privacy monitoring?

With the launch of iOS 14 last year, Apple started to focus more strongly on the privacy aspect of its smartphone and its apps. This is also one of the ways that Apple wants customers to differentiate their products from competitors, through surveillance and protection of interests (including privacy) for its customers. .

Until recently, the way iPhone and iPad apps could track you or use your personal data weren't entirely transparent with users. In addition to enforcing multiple security solutions for the iPhone, Apple implemented a dedicated label for digital privacy of apps. Now, you only need to take a look to temporarily evaluate the security performance of your application to make a decision with them.

## How to check the privacy details of an app on the App Store

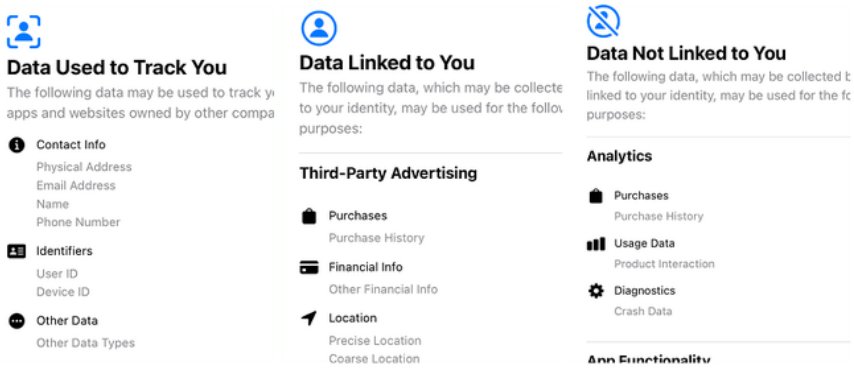


First, open the App Store on your iPhone and find the app you want to check or install. Then, click on the app's name to open a detailed description and scroll down to the App Privacy section just below the Rating & Reviews section. Clicking App Privacy will see a privacy summary that the app developer has reported to Apple (and made public to users). Here are the three main categories and the meaning of information in the App Privacy labeling of an app on the App Store:

1. **Data Used to Track You** (data used to track you): Information used to track you on apps and websites owned by companies other than Apple, thereby helping advertisers Ads build a personalized profile based on a user's online behaviors to allow them to show specific advertising content to each person.
2. **Data Linked to You** (data linked to you): Information collected and linked to your personal identity, for example Facebook will know your real name and some specific information that it does. collected in the application's database.
3. **Data Not Linked to You** (data not linked to you): Information that is collected but not used to associate with your online identity. In other words, data is collected but not used to build a user's personalized profile.

Each application uses data in different ways, so you may not see the full three items above in the detailed description of App Privacy. For example, the Facebook app's App Privacy label won't have a 'Data Not Linked to You' entry, but the Signal app only has this entry in its privacy description.

There are special cases like Facebook where the list of data it collects to track you extends much longer than many other apps, which may be one of the reasons that Facebook is not satisfied when Apple goes public about the behavior of this app. But that's how Apple wants to differentiate itself from the competition: Protect user interests and privacy.




If you find some sensitive information and permissions for an app on the App Store that doesn't work for you, the first option you can avoid is to not install the app and try to find apps. a more suitable replacement. For example, you can use Signal instead of WhatsApp if you're concerned about data linking to track users.

The second option is to ask the developer to create a less privacy-invasive version, although the odds on the likelihood of success of this option are low and take time. With the new application's privacy policy managed and publicized, we can expect that under pressure from Apple, the app industry will pay more attention to user data security. As for Apple, they are 'shooting' an arrow that hits both targets: Making a difference with their opponents and protecting their users.