DAY 2

Check Your Smartphone's Privacy Settings

Smartphone apps can run in the background of your phone, gathering all kinds of private data about you, from your location to your contact list. It's a good idea to audit these permissions so apps don't gain access to data you don't want them to. This won't delete any data app-makers have already gathered, but it will at least prevent them from getting more. It takes only a couple of minutes to do.

If you have an iPhone:

1. Open up "Settings" and then go to the "Privacy" menu. Here, you'll find a list of different privacy permissions, like location, contacts and more.

2. Go through each option and disable access to any app where it doesn't make sense. For example, a game you downloaded to fill time on the bus doesn't need access to your location, the mic or your photo library. In some cases, you can disable access at the cost of functionality, as with Instagram, which works perfectly fine without location access, but you will lose out on some features by disabling it.

3. **Note:** On the "Location" menu, be sure to scroll all the way down to "System Services" and disable options like "Location-Based Apple Ads," which captures your geographic location for ads in Apple News and "Popular Near Me," which tracks where and when you use apps for those same marketing purposes.

4. Finally, scroll down and tap Advertising, then enable "Limit Ad Tracking," to opt out of the interest-based ads generated from the App Store search history and Apple News reading history.

If you have an Android phone:

1. On stock Android (it may be different on your phone), head to the Settings menu and open the Apps menu.
2. Tap the gear icon, then tap “App permissions.” You will find permissions for location, microphones, contacts and more.
3. Tap each and disable apps you don’t trust or don’t think need access to the data it’s requesting.

Have you completed this?
Mark this task complete

Bonus

You can disable some of Google’s data collection from the My Activity page. There, click “Activity Controls” and disable options like “Location History,” “YouTube Watch History” or “Device Information.” Google will still keep anonymized information about you, but at least you can minimize what it has. If you use Google’s products, like Gmail, Keep or Docs, Google will continue to collect and store all that data.

Why Am I Doing This?

Companies like Google and Apple generally have consistent privacy and security policies, and while they do collect data, at least you know it’s happening. Third-party apps and services often don’t have this same level of transparency. Nearly every time you install an app, you’re granting it some sort of data access. The majority of these permissions are for basic functionality — a photo editing app won’t work without access to the photo library — but sometimes those apps will collect data without your knowledge. For example, Path uploaded users’ address books, and dozens of apps abuse location permissions for ad tracking.

Now that you understand the risks, it will be easy to keep an eye on permissions as you install new apps. If you ever run into an app that seems to overreach, it’s usually best to delete it unless you really need it.