TIP SHEET

MANAGING YOUR PRIVACY WHEN USING SMART DEVICES

Today, it's not just computers or even phones that connect to the internet: chances are that you have one or more "smart" devices in your home.

Whether it's a video doorbell, a speaker with a built-in voice assistant, or even "smart socks" for your baby, these things all have one thing in common: they use data to operate. Sometimes that data is personal, so you should know how to manage it.

What kind and how much *data* is collected, though, is at least partially up to you. Here are some steps you can take to manage your privacy when using smart devices.

Keep privacy in mind when shopping. Different devices collect more or less information than others. For instance, some smart doorbells only store video *locally* (on a hard drive or memory card) instead of uploading it to the cloud. (Remember that it's not just our privacy we have to worry about: we should be respectful of *other people's* privacy, too.) Remember to check for these features, including what data storage options are available like deletion and encryption.

Reading the privacy policy should be an important part of your decision, too. The privacy policy tells you what information the company collects, what they'll do with it and what rights and options you have to control that.

> The website Terms of Service, Didn't Read (tosdr.org) summarizes and rates terms of service and privacy policies.
>
> You can also review the privacy policy yourself before you decide what to buy. This is easiest to do on a laptop or desktop computer, where the text is easier to read and you can use CTRL-F to look for key words.

- Look for: the word "collect," as in "information we collect" or "how we collect and use your data." Be ready to open a new tab and look up any words you might not recognize or you're not totally sure you know, like "biometric" or "geolocation."
- Look for: the word "partners", "share", or the phrase "third parties." That tells you what *other* companies your information may be shared with (or sold to).
- Look for: the phrase "how we use." This will explain the different things the company will use your information for. It can be hard to know what effect that might have on you – for example, information about your health from a wearable device might affect how much you pay for insurance – so if this part of the policy isn't clear or you're not comfortable with it, consider buying a different option.
- Look for: the words "rights" or "choices." This should explain your privacy rights under the law (make sure to read the section for the place you live) and may tell you how you can ask to see what's been collected or have it deleted, or to opt out of some of the ways that the company collects and uses your data.

Get to know the app. Because most smart devices don't have screens, they almost all have an app that you install on a phone or tablet. The app is how you change the different settings on the device. A lot of the things suggested below involve changing those settings, so it's a good idea to get familiar with the app and how you use it.

However, installing the app also gives the company that makes the device access to certain information on your phone or tablet. Some apps collect information when you're using them, and others even collect data when you're using other apps on the same device. Here's how to stop that:

- If you have an iPhone or an iPad, choose "Ask App Not to Track" when you install the app. If you have apps for smart devices that you've already installed, go to Settings, then Privacy & Security and then Tracking. Find the app and toggle "Allow Apps to Request to Track" to Off.
- If you have an Android device, install the app DuckDuckGo. Go to Settings and then enable App Tracking Protection.
- If you use a laptop or desktop computer to control your device, make sure your browser has an extension like Privacy Badger or Ghostery installed that blocks data collection.

Anybody who gets access to the app can change settings on the device, too, so think about installing apps for smart devices on a tablet or an old phone that doesn't leave the house. That way you don't have to worry about someone who finds or steals it getting access to the device.

Review privacy settings. Once you're familiar with the app, find the privacy settings. These will usually be an option inside the main Settings section, but if you have trouble finding them you can use a search engine to look for "privacy settings" plus the name of your device ("Alexa privacy settings," for example.)

Different devices have different privacy settings. Here are some options you should look for. (If you're shopping for a smart device, try to find out which of these a device offers.)

- Turning off data collection and sharing. Almost all smart devices send some information to the company, and companies use that data for a lot of different things: to improve how the service works, for instance, or to send specific ads. You may be able to opt out of having your data collected or used for these purposes. For instance, on an Alexa device go to Alexa Privacy and then select Manage Your Alexa Data. You can also opt out of receiving personalized ads on Amazon **here**.
- Deleting your history. Smart devices often record what you've done with them in the past, such as the specific things you've said to a smart speaker using the wake word (more on that below). You may be able to review what's been saved, delete some or all of it, and pause history to keep it from recording things in the future by selecting "Don't save recordings" or something like that.
- Changing the password and wake word. Most smart devices come either with no password or a default password, so make sure to set a strong one. (See our short video at http://www.tiny.cc/goodpassword for quick tips on how to make a good one.)

    - Smart speakers also have a "wake word" that tells it to start listening to you. To make sure that it doesn't "wake up" by accident, change the wake. (Not all smart speakers let you change the wake word. Other ones give you a limited range of wake word options, so pick the one that's the best fit.) If you speak a language other than English, you may be able to set your speaker to hear and respond in that language instead.
- If it is possible to buy anything using the device, make sure that option is turned off too. (That way other members of your household can't buy anything by accident.)

If the device is linked to your account with a company such as Google, Apple or Amazon, you may also be able to change some settings in your main account: for instance, if you don't want your Amazon smart speaker to play targeted ads you can turn off "interest-based ads" on the Amazon Advertising Preferences Page. (It will still play ads, but they won't be based on your personal information.)

Create a guest account on your WiFi. Keeping the device off your main WiFi account also limits what it can collect. Your internet provider may have come with an app that lets you change your router settings. If so, it should have an option to create a guest network. If there isn't an app, contact your internet provider to ask for help.

Turn off microphones and cameras when you don't need them. Many smart devices that have microphones or cameras have either physical switches or options in the app to turn them off (for example, Alexa devices have a visible Mute button on the top, and will indicate via a red light when the device is muted. You'll get the same outcome by simply saying "Alexa stop recording")

Cover cameras when you're not using them too. Most smart devices that have cameras have a light that turns on when the camera is active, but to be on the safe side you should put a sticky note or something similar over any smart device whose camera doesn't need to be running all the time.

Don't forget about extra apps. Some smart devices have extra apps or "skills" that let it do different things. Some of these are made by different companies than the one that made the device, and may collect different information or use it for different things. Make sure to only download them from the device's official store, and check the privacy policy before installing a new app or skill.