THE RV LIFESTYLE

CELLPHONE PRIVACY? WHAT'S THE BIG DEAL!

FEBRUARY 9, 2017 | MARGO

Part 1

If you are wondering what the big fuss is about keeping the government from accessing your cellphone data without a warrant,
read on . . .

If your privacy is important to you (at least what can be controlled by you), a piece of black tape is already over the camera on your computer. How about your cellphone?

Smartphone ownership is at an all-time high, and microphones are an essential hardware feature on every phone. What does it mean for your privacy?

Is Your Phone Listening to Your Conversations

To review the permissions you have already granted to apps, like Google:

On a Samsung, Motorola, or other Android-based phone, go to **Settings** > *Privacy and Safety* > **App Permissions**. On an iPhone iOS, go to **Settings** > *Privacy*. Both have an entry for *microphone*, which lists all the apps that have access. If you see something suspicious, investigate.

With services like Siri or Google Assistant, your phone is always listening for a keyword, but that is processed locally. It does not start recording your audio until it hears "Ok Google" or "Hey Siri." At that point, it records and uploads an audio file. You can turn these features off quite easily; for example, on Android, go to **Settings** > *Google* > *Search* **&** *Now* > **Voice.** Turn "Ok Google" detection **off**.

Read more…

Tired of Products Pushed In Your Face

Kim Komando, a leader in gathering high-tech information to share with the consumer, stated that back in March 2015, AT&T surprised everyone when it added a new option to its GigaPower fiber Internet service: **privacy**. Yes, for just $29 more a month AT&T promises it WON'T sell your search and browsing history to advertisers. How generous.

While there's still some doubt about how private your information is even after you pay the $29, at least AT&T is being honest about how it finances operations. The truth is, the major cellphone carriers are more than happy to sell your information to advertisers and serve you targeted ads over their networks.

Options You Can Control

iPhone

If you're an iPhone user, you need to go into **Settings**, and then tap *Privacy*. Scroll all the way down to **Advertising**.

You'll see a button labeled says, "*Limit ad tracking*." If it's not showing a green color, slide the button so that it shows green. This will stop ad companies from tracking what you do with your phone and serving up targeted ads.

Right underneath that setting, by the way, you'll see the "*Reset Advertising Identifier*" option. Tapping on that will zero out the anonymized identifier linked to your personal data on Apple's servers.

In other words, to trackers you'll appear to be a new user. This can make it more difficult (but not impossible) for advertisers to build up a profile on how you browse.

Android

To turn off the Google "AdID" system, you do not go to your Android phone settings, but your **Google Settings** app. You might have to look under your full list of apps to find it.

Once you are in *Google Settings*, tap the **Ads** link and then tap "*Opt out of interest-based ads*." You can also see your advertising ID and tap "*Reset advertising ID*" to make a new one. This will make you look like a new user to advertisers.

Windows Phone

To turn off Personalized ads in Windows Phone, go to Microsoft's ad opt-out page and under "Personalize ads whenever I use my Microsoft account" click "Off."

You will need to be signed in with a Windows account to do this. Make sure you sign in with the same account you use on your Windows Phone. This also turns off personalized ads for Internet Explorer in Windows 8.

Ads aren't the only way you're tracked on your phone. Google and Apple might be tracking your searches.

The Future of Tracking

Of course, carriers are working on ways to track you that you can't stop. Verizon and AT&T have experimented with "supercookies" that let any website know who you are when you visit.

AT&T eventually dropped the idea when customers complained, but Verizon still does it.

You can opt out at https://www.verizonwireless.com/myprivacy/, so Verizon won't track your information or show you targeted ads. However, Verizon does still add the supercookies to your browsing, which can give away your identity to websites or hackers.

One solution is to use Wi-Fi instead of your cellular signal for browsing, but that isn't always possible. Click here to learn more about Verizon's supercookie problem and how you can protect yourself.

Tracking and selling your information is not just a problem with cellular carriers, though. There are ways every ad company can track where you go online.

You should also know that Facebook shares your information with advertisers as well.

For the rest of the story…

Non-Tracking Search Engines

Here are some options for search engines that do not allow tracking:

- DuckDuckGo

- Ixquick's Startpage

To surf anonymously everywhere — at the cost of slower browsing speed — try the Tor Browser Bundle. Be careful here as the US Government is watching this site for terrorist action.

Try Ghostery.com software to be aware of who is tracking you and exercise some controls on access.

Downsides to Privacy

As you make your cellphone and computer as safe as you can, the downside is the limits that Google and other browsers put on your search requests. Some websites reject your request if their ads do not appear. If using Ghostery software, you can pause it just to access that site.

*Tune in next time for **Part 2 of Cellphone Privacy**. Find out exactly what information about you is available to the world.*