MARCH 3, 2017 | MARGO

Part 2

To live the RV lifestyle to it's fullest potential, smartphones are a necessity these days. We use them to stay in touch, search the Internet for nearby gas stations or food, and check the weather. For many of us, our smartphone is the connection to that other world that we choose to venture into now and then.

Smartphone Downsides

Like any tool, the smartphone has its downside. Similar to the problems we deal with using a computer, digital data can so easily be subverted. Learning how to protect ourselves is part of the price we pay for the convenience.

My last blog post alerted you to unauthorized use of the cellphone's microphone and how to prevent that. Also mentioned were ways to keep advertising to a bare minimum and where to find non-tracking search engines.

But . . . what about information you willingly give to Google and other ad-producing entities. Let's take a look at some of the permissions you may be giving them without realizing the long-term effect on your everyday life.

Many people today have their whole life habits, family and friends, business contacts, calendars, and wishlists turned into data on their smartphones. Yes, it is alarming what information about you can be downloaded by almost anyone.

Listed here are only the permissions given to Google. All of the apps and widgets on your smartphone also have certain access given to them. It is an all or nothing plan.

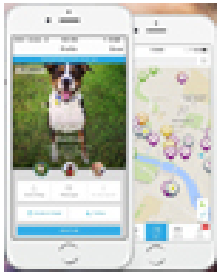
Access List

Google Android has access to:

- Read your web bookmarks and history, write web bookmarks and history
- Directly call cell phone numbers, read phone status and identity, reroute outgoing calls
- Read instant messages, read your text messages (SMS or MMS), receive, send and write text messages
- Set an alarm, control the flashlight
- Take pictures and video
- Record audio, change audio settings
- Locate your phone approximately and precisely
- Modify your contacts, read call log, read contacts, write to call logs
- Activity recognition: modify contact card, read calendar events
- Add voicemail
- Modify or delete the contents of your USB storage, as well as read the contents
- Disable your screen lock
- Add or remove accounts: access contacts in Google accounts, create accounts and set passwords, find accounts on the device, read Google mail, read Google service configuration, use accounts on the device, view configured accounts, and access Youtube usernames

- Modify secure system settings
- Read sensitive log data
- Retrieve system internal state
- Change network connectivity: connect/disconnect Wi-Fi, control Near Field Communication, download files without notification, full network access, receive data from Internet, view network connections, view Wi-Fi connections
- Access Bluetooth setting, pair with your bluetooth devices
- Make apps always run, retrieve running apps, run at startup
- Draw over other apps
- Allow Wi-Fi Multicast reception, control vibration, prevent phone from sleeping
- Read sync settings, sync statistics, toggle sync on and off.
- Install shortcuts, interact across users, modify system settings, read subscribed feeds, retrieve app ops stats, send sticky broadcast, write subscribed feeds

Some apps, like *BarkHappy*, a site that finds and adds dog friendly places on the map, require this strange access.



- Device ID & Call Information: Allows the app to determine the phone number and device IDs, whether a call is active, **and the remote number connected by a call**.

Wow! That is a long list. Next time you install an app, take the time to read to the bottom of the page before you hit the “install” button. If you are appalled at the privacy invasion, maybe you should re-evaluate the value of the app compared to the information given away. Better safe than sorry, that is MHO.

Think Long-Term

Yes this, my friends, is why the discussion about smartphone access without a warrant has become so heated. This is why the tech companies worldwide have lined up against government access without your permission.

Breaking News! Microsoft is suing the U.S. government for preventing the company from notifying users when their data has been handed over to authorities. The company says it has had to keep quiet about 2,500 requests over the last year and a half.