The good and bad of location tracking

June 29 2018, by Larry Magid, The Mercury News

Credit: CC0 Public Domain

Two recent news stories about cellphone location services recently caught my eye. One was a positive development and the other quite negative, until it was at least partially fixed.

The positive story is that Apple's iOS 12 operating system for iPhone will enable users to "automatically and securely" share their location data with 911 call centers and first responders. The negative story revealed that cellphone carriers were selling real-time customer location information to data brokers who sold that information to law enforcement and others, without necessarily going through those annoying and time consuming formalities such as court orders. In response to the controversy, the major carriers are stopping the practice.

LOCATIONS DISCLOSED WITHOUT CONSENT OR COURT ORDER

In a letter to AT&T president Randall Stephenson, Sen. Ron Wyden (D-OR) said that he "recently learned that Securus Technologies, a major provider of correction facility telephone services, purchases real-time location information from major wireless carriers and provides that information, via a self-service portal, to the government with nothing more than a pinky promise." Wyden also went after Verizon, T-Mobile and Sprint. So far, Verizon, AT&T and Sprint have announced that they will no longer provide this information to these third parties.

According to Wyden, law enforcement agencies could obtain this data simply by uploading an "official document" to a Securus web portal but said that senior officials from Securus "have confirmed to my office that it never checks the legitimacy of those uploaded documents."

In addition to these illegitimate sales to law enforcement, there is also the not-so-theoretical risk of hacking. Motherboard reported that a hacker broke into Securus servers and stole "2,800 usernames, email

addresses, phone numbers, and hashed passwords and security questions of Securus users, stretching from 2011 up to this year." And, as Krebs on Security reported last month, LocationSmart, another data aggregator with access to these phone location records, "has been leaking this information to anyone via a buggy component of its Web site—without the need for any password or other form of authentication or authorization."

LOCATION DATA CAN SAVE LIVES

The positive story about smartphone location data is also important and worth celebrating. Last week, Apple announced that it's working with emergency technology company RapidSOS to "quickly and securely" share iPhone callers' location data with 911 centers. Cellphone carriers have long been able to provide some location data to 911 centers even before there were smartphones. But iPhones and Android devices have far more location data than those old flip phones, including what can be gleaned from GPS and Wi-Fi access points. There are also efforts underway to pinpoint specific locations within buildings.

In a press release, Apple said that "Approximately 80 percent of 911 calls today come from mobile devices, but outdated, landline-era infrastructure often makes it difficult for 911 centers to quickly and accurately obtain a mobile caller's location." RapidSOS currently offers its RapidSOS Haven Emergency app for both Android and iPhones.

DO-IT-YOURSELF NON-EMERGENCY LOCATION SHARING

Even if you don't have a 911-level emergency, there are other reasons to use your mobile device to share location data. One is to let others know when you are likely to arrive at a location, such as a meeting or dinner appointment.

Another is piece of mind for parents, spouses/partners and other close family and friends. I'm a bit of a worry-wart and there are times when I've used technology to locate my wife and other family members with their permission and knowledge, including when they're traveling abroad. It's not about stalking but reassurance that they're OK.

I've heard from parents who insist that their children share their location via their smartphone in exchange for giving them more freedom to be out on their own.

Google Maps has a "Share location until you arrive" feature that allows people to follow your progress during a specific trip. The free Glympse app for smartphones allows you to share your location for a specified period of time—up to four hours, a limit that prevents the app from being abused by stalkers.

Apple's Find My Friends app lets you permanently share your location with friends, though you can terminate or suspend location sharing at any time.

There are also ways to track your car. My wife and I each have an Automatic Pro ($129.95 with no monthly fee) in our car which can track the car's location, automatically call for help after a crash and provide diagnostic information. It can be removed or disabled, but when it's working, it can share your location with anyone allowed to access your account.

Another option is using Apple's Find My iPhone feature or Google's Find My Device. In general, I don't recommend sharing your password, even with close friends, but it could be appropriate as a way for parents to track their children (ideally with the kids' knowledge) or even between close partners with the understanding that you should change your password if you have any reason to believe someone may be misusing

the information. There are also "find my friends" style apps for Android that you can use to share your location with others and unshare at any time.