Privacy and Search Warrants in the Digital Age

September 18, 2021 - Not so long ago, if the police wanted to know where you were at a specific date and time, they would have to do some investigating. By that, I mean they would actually have to make some phone calls to your friends and acquaintances. Go out and knock on a few doors. Interview a few people. After that, they might be able to establish where you were and what you were up to. But that's all changed now. All they have to do is contact Google, Apple or any one a number of other companies and get a data dump on you. And the information they get could put you in a world of hurt even if you haven't done anything wrong.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];

s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

Let's just say you are out riding your bike one day and your cell phone pings off of a tower that is close to a crime scene. That's exactly the scenario that was reported in The Guardian that ensnared a man in Gainesville, FL early last year. The police were looking for a burglary suspect and they got a search warrant for tracking data from Google. And just because he was out riding his bike and near the house that was burgled, he had to pay for an attorney to deal with a legal issue that he never should have been involved in in the first place.

Warrants and subpoenas for this type of information are very problematic. If the police want to search your home, they first need to establish a solid reason for that search. That's called probable cause. But a sweeping subpoena for information to a tech company is something different. One minute you're minding your own business and the next, the police are knocking at your door because you just happened to be in the area of a crime. Frankly, if you think about it, it isn't anybody's business what you're doing at any given time. But because the police were able to gather information that you were near the crime, you may now be a person of interest to them. And they may actually be able to use the information they received through that tech company to establish probable cause in the eyes of a court. That could lead to a lot of other issues for you; none of them good.

The fact is that this is happening more and more. The phone that we all carry around with us is now being used by companies to track our movements. And the government can easily access that data by simply issuing a subpoena. That's something that the 4th Amendment was designed to prevent and it isn't the way investigations are supposed to work.

In an ideal world, the police would have to operate the same way they did before cell phones were common. They would go to the scene of a crime, gather evidence and then develop a suspect pool. Then they would have to establish probable cause for any search, and only then could the get search warrants that would be limited to those suspects. But with a subpoena to big-tech, they're doing just the opposite. They get a list of names that happened to be in the area of a

crime, but to which they have no other links. Then they force the people on that list to prove that they weren't the perpetrators. No probable cause needed or, put another way, guilty until proven innocent.

If you want to see the type of information that a big tech company has on you, just take a look at Google. Log into your Google account and go to https://myaccount.google.com/data-and-privacy. If you take a look around, you'll be able to find maps that show your travels. These can go back years and this is only one company. Google is far from the only company gathering this data on you.

Weather applications rely on your location data to provide accurate information. Apple, Facebook and a wide variety of others also gather this information. Weather or not you like it, you are being tracked everywhere you go.

There are ways that you can protect your privacy but they are limited and inconvenient. You leave your phone at home. No tracking when that happens but not a real option for most people; especially if you use your phone for business. You can buy a burner phone that you use when you're out of the house, and have another one that you use when home. Again, not real convenient and for many, not an option.

The bottom line here is that you really shouldn't have to worry about any of this when you go about your day. Unfortunately, there really aren't any laws to protect any of us from this type of tracking and government overreach and congress has shown little interest in changing these practices. Therefore, everyone needs to be aware that this is going on and, whenever possible, limit the amount of data that we allow applications on our phones to collect on us.
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS