

Search Engines Now Being Served with Keyword Search Warrants by Feds

October 7, 2021 - In what can only be termed a fishing expedition, it has come to light that the federal government served Google with a recent search warrant for "keywords" used in searches. The revelation came from an accidentally revealed court document that was discovered by Forbes. Keyword search warrants are issued secretly by the government in an effort to develop a list of suspects who conduct internet searches using specific terms. They are also dangerous because they have the potential to ensnare innocent people in criminal investigations.

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);  
})();
```

In the case discovered by Forbes, the government was trying to develop a list of people who might have been involved in a sex trafficking and missing persons case in Wisconsin. So the keywords they wanted information on included the victim's name, her mother's name and her address. Any searches for that information that were logged by Google that occurred over a time frame of a little more than two weeks in 2019 were fair game. And any information that Google possessed on the people conducting the searches was also to be turned over. And Google has a lot of information on your search history.

Tens of millions of Americans used a multitude of Google products. Android phones run on a Google-built operating system and they can track your whereabouts. And since virtually everyone is logged into Google any time Android is used, that means Google knows exactly who conducted a specific search. The same can be said for those on PC or MAC who use a Chrome browser. Most users of Chrome are logged into Google all of the time, so any search you conduct can be tracked back to you.

It isn't hard to come up with a scenario here that has the potential to entrap perfectly innocent people. Let's just take a hypothetical bank robbery in which the police have no suspects. If you were searching for the address of the bank that was robbed a couple of days earlier, you could find the police knocking at your door to ask you why. What was the interest in that particular bank location? Or let's say you're looking for a new apartment to live in. You set an appointment to see one in a couple of days and then look up the address on Google Maps. But prior to your appointment there is a rape... or a murder that takes place in the building. You could find yourself being questioned.

These warrants are sweeping and dangerous to our privacy and our liberty. And it isn't just Google that has received them. Yahoo and Microsoft are also known to have been served such warrants so it is reasonable to think that other search engines are getting them too.

Use of internet search engines is really a necessity in today's world. But being caught up in criminal investigations isn't something that anyone should suspect will happen when they conduct a search. Anyone interested in protecting their privacy does have some options though. You can use a VPN (virtual private network) which will route your traffic through servers around the world prior to routing it to the search engine. You can also use a browser that protects your privacy, such as TOR, which will do much the same thing.

Either way, the job of protecting your privacy is clearly on your own shoulders. It doesn't appear that Google has fought any of the keyword search warrants they have received, so as a consumer, you are on your own.

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