NSA Data Collection Efforts - What They're Doing and Who They're Watching

June 7, 2013 - Over the past few days we've been watching the various news stories about the NSA's data collection activities with some interest. The revelations aren't really new. Ever since the passage of the Patriot Act, we've known that the government is listening to phone calls and monitoring internet traffic. But what is newsworthy about the most recent revelations is the scope of the monitoring. The bottom line is that the NSA has taken the attitude that everyone is a suspect until they can prove otherwise. And so far, it would appear that the federal courts agree with the approach. Below, we'll tell you what the NSA's data collection efforts look like, who they are monitoring, and what (if anything) you can do about it.

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);
 })();
```

What forms of communication are being monitored by the NSA?

The NSA is running multiple data collection efforts. These include a program to monitor telephone calls and one to monitor internet traffic. The program for the internet is known as PRISM. There is no known code name for the telephone monitoring program.

What data is the NSA collecting in these programs?

The telephone data being collected is meta-data. That means that according to the government, the NSA isn't listening to phone calls. They are simply looking at which telephone numbers people are calling and how long they are on the phone. The stated goal of the program is to establish communication patterns by sifting through tens of millions of call records. The hope is that this type of data analysis will lead the government to find people involved in terrorist plots.

The internet monitoring program appears to be all inclusive. PRISM apparently looks at every sight you visit, every email you send and pretty much anything that you do online.

Who is the NSA monitoring?
The shore answer is, "everyone."

The telephone program was revealed late last week when a secret court order was leaked. The order which was issued by a judge sitting on the Foreign Intelligence Surveillance Act (FISA) court ordered Verizon Communications to turn over all telephone records for every single one of their 120 million customers to the NSA. The order covered the last three months but it has since been revealed that similar court orders have been issued every three months for the past seven years.

While the order was specific to Verizon, it is difficult to imagine that other cellular carriers haven't been receiving similar orders over the same time frame. Bottom line is that any cellular call you've make in the past seven years is knows to the government.

The PRISM program allows the FBI and the NSA to tap directly into the internet servers of Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple. It is rumored that DropBox is also going to join the program. According to information obtained by the Washington Post, Google, Microsoft and Yahoo traffic make up approximately 98% of the traffic being analyzed.

In the case of Google, CNET is reporting that search traffic as well as Gmail, Google Drive files, stored photographs and video communications (stored and live) are being monitored.

Are these programs legal?

If you think that these programs are unconstitutional, you are not alone. But the federal courts have made it almost impossible to challenge them.

Congress and the White House have enacted two laws that specifically allow the programs; the Patriot Act and the Foreign Intelligence Surveillance Act (FISA).

Since most programs under each of these acts are considered "secret" by the government, it is almost impossible for someone to prove that they have been hurt by either program. Federal courts require that you show that you have been injured in some way in order to file a law suit. They refer to this as "standing." If you haven't been injured, then you don't have "standing" to sue. And you can't claim that simply because you are an American citizen a violation of the Constitution by the government injures you. In short, the courts have created a Catch22 in which the government appears to be able to operate with impunity.

Is there any way to protect my phone and internet records from government snooping?
Possibly.

You can protect your cell phone calls by using paid services such as Seecrypt or SilentCircle. At present, neither of these services have any back-doors that would allow the government to monitor your call traffic.

In the case of your internet traffic, you may be able to thwart monitoring efforts but it will take some time on your part. There are privacy programs such as TOR or VPN services which can protect your IP address and help you remain anonymous. But you would also need to change your current passwords and probably need to cancel any online mail accounts such as Gmail.

What is the federal government saying about these programs?

They are saying, "trust us." But that may be a real leap.

NSA and FBI officials have openly lied in testimony to Congress about the very existence of these two programs. And even though the NSA is stating that it isn't listening in on phone calls, there is every reason to believe that this is also a lie.

Shortly after the Patriot Act was enacted, there were several reports from whistle blowers that several phone companies were installing call monitoring systems on behalf of the federal government. There have been no reports of such systems being removed. Additionally, it was widely reported that the NSA was scanning telecommunications networks for conversations in which certain key-words were used. Use of those key words would bring about more monitoring of specific calls and/or the individuals making them.

Have these programs made us any safer?

According to reports over the past few days, the federal government was able to use the telephone program to stop a terrorist attack but no details were revealed.

With that said, neither of these programs were involved in stopping or solving the Boston Marathon bombing, the Underwear Bomber, the Shoe Bomber or the Times Square Bomber. All of these were stopped or solved by tips or intervention from the general public. To date, there have been absolutely no details of any crimes stopped or solved through the telephone or PRISM programs.
byJim 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 me on Twitter:

Follow ACCESS