GlobalResearch
Center for Research on Globalization

Cell Phone Users Beware: How to Protect Yourself from Government Spying

By Washington's Blog
Global Research, June 24, 2013
Washington's Blog

Region: USA
Theme: Intelligence, Police State & Civil Rights

Unless You Know About This Spying Method, You Might Say Something Which Could Get You In Hot Water

Given that the NSA is tapping into your phone calls and spying on your Internet activities, you might have switched to a search engine which is more privacy-conscious.

You might have started using encrypted communications. After all, NSA whistleblower Edward Snowden and the leading electronic privacy group – the Electronic Frontier Foundation – say that encryption helps to protect privacy. On the other hand, Tech Dirt points out that the NSA might consider you suspicious if you encrypt information, and so hold onto your data until they can decrypt it.

The above are all issues about which you are at least somewhat aware.

But there is a giant type of snooping which you probably don't even know about. Specifically, ABC News reported in 2006:

> **Cell phone users, beware. The FBI can listen to everything you say, even when the cell phone is turned off**. A recent court ruling in a case against the Genovese crime family revealed that the FBI has the ability from a remote location to activate a cell phone and turn its microphone into a listening device that transmits to an FBI listening post, a method known as a "roving bug."
>
> Experts say the only way to defeat it is to remove the cell phone battery.
>
> **"The FBI can access cell phones and modify them remotely without ever having to physically handle them,"** James Atkinson, a counterintelligence security consultant, told ABC News. "Any recently manufactured cell phone has a built-in tracking device, which can allow eavesdroppers to pinpoint someone's location to within just a few feet," he added.
>
> ***
>
> According to the recent court ruling by U.S. District Court Judge Lewis Kaplan, **"The device functioned whether the phone was powered on or off, intercepting conversations within its range wherever it happened to be."**
>
> ***

> "The courts have given law enforcement a blank check for surveillance," Richard Rehbock, attorney for defendant John Ardito, told ABC News.
>
> ***
>
> "Big Brother is upon us...1984 happened a long time ago," he said, referring to the George Orwell futuristic novel "1984," which described a society whose members were closely watched by those in power and was published in 1949.

Fox News covered the story as well:

CNET noted the same year:

> The U.S. Commerce Department's security office warns that "a cellular telephone can be turned into a microphone and transmitter for the purpose of listening to conversations in the vicinity of the phone." An article in the Financial Times last year said mobile providers can "remotely install a piece of software on to any handset, without the owner's knowledge, which will activate the microphone even when its owner is not making a call."
>
> ***
>
> Because modern handsets are miniature computers, downloaded software could modify the usual interface that always displays when a call is in progress. The spyware could then place a call to the FBI and activate the microphone–all without the owner knowing it happened.
>
> ***
>
> A BBC article from 2004 reported that **intelligence agencies routinely employ the remote-activiation method. "A mobile sitting on the desk of a politician or businessman can act as a powerful, undetectable bug," the article said, "enabling them to be activated at a later date to pick up sounds even when the receiver is down."**

Given that the American and British intelligence agencies are trying tap every single communication, some rogue agency or contractor might be tapping your phone ... even when it's off.

Indeed, even *private* hackers might be listening in. Specifically, private parties without security clearance may be activating your microphone or camera without your knowledge.

Indeed, commercially-available, off-the-shelf software allows people to spy on you:

Your iPhone, or other brand of smartphone is spying on virtually everything you do (ProPublica notes: "That's No Phone. That's My Tracker") ... and sending the information to private companies.

And CNET pointed out 7 years ago:

> Malicious hackers have followed suit. A report last year said Spanish authorities had detained a man who write a Trojan horse that **secretly activated a computer's video camera and forwarded him the recordings**.

So the single most important step to protect yourself from government – or private – spying is to remember that your conservations might not be private when your cellphone is nearby … even if it is turned off.

Note: If you have a microphone in your car, that might also open you up to snoopers. As CNET points out:

> Surreptitious activation of built-in microphones by the FBI has been done before. A 2003 lawsuit revealed that the FBI was able to surreptitiously turn on the built-in microphones in automotive systems like General Motors' OnStar to snoop on passengers' conversations.
>
> When FBI agents remotely activated the system and were listening in, passengers in the vehicle could not tell that their conversations were being monitored.

And Fox news notes that the government is insisting that "black boxes" be installed in cars to track your location.

And see this.

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: **Washington's Blog**