

How the NSA can 'turn on' your phone remotely

By Jose Pagliery @Jose_Pagliery June 6, 2014: 8:03 AM ET

[Recommend](#) 3.5k



ILLUSTRATION: TIFFANY BAKER/CNNMONEY

The government can't really turn your phone back on. But it can keep the phone from actually turning off.

2K
TOTAL SHARES

1K

505

113

20



NEW YORK (CNNMoney)

Even if you power off your cell phone, the U.S. government can turn it back on.

That's what ex-spy Edward Snowden revealed in [last week's interview with NBC's Brian Williams](#). It sounds like sorcery. Can someone truly bring your phone back to life without touching it?

No. But government spies can get your phone to play dead.

It's a crafty hack. You press the button. The device buzzes. You see the usual power-off animation. The screen goes black. But it'll secretly stay on -- microphone listening and camera recording.

How did they get into your phone in the first place? Here's an explanation by former members of the CIA, Navy SEALs and consultants to the U.S. military's cyber warfare team. They've seen it firsthand.

Related: [Google testing super-secure email](#)

Government spies can set up their own miniature cell network tower. Your phone automatically connects to it. Now, that tower's radio waves send a command to your phone's antennae: the baseband chip. That tells your phone to fake any shutdown and stay on.

A smart hack won't keep your phone running at 100%, though. Spies could keep your phone on standby and just use the microphone -- or send pings announcing your location.

John Pirc, who did cybersecurity research at the CIA, said these methods -- and others, like physically bugging devices -- let the U.S. hijack and reawaken terrorists' phones.

Related: Cybersecurity: How safe are you?

"The only way you can tell is if your phone feels warm when it's turned off. That means the baseband processor is still running," said Pirc, now chief technology officer of the **NSS Labs** security research firm.



Filshere: Why Snowden did the right thing

This isn't easy to accomplish. It's a highly targeted attack. But if you are really concerned about the government's ability to reawaken your phone, here are some things you could do.

Recovery mode. Put your phone on what's known as Device Firmware Upgrade (DFU) mode. This bypasses the phone's operating system. Every phone has a different approach for this.

It's fairly easy (albeit cumbersome) for iPhone users. Plug it into a computer with iTunes open. Hold down the Power and Home buttons for 10 seconds (no less) then let go of the Power button. Wait for an iTunes pop-up. That's it.

For Android users, recovery mode varies by model. Android Magazine has a [great tutorial here](#).

Create a barrier. Use a signal-blocking phone case. You can buy them ([Off Pocket](#), [HideCell](#)) or even [make your own](#) -- assuming you have the patience to do so.

Pull out the battery. Without a power source, the phone can't come back on. This is the best, most surefire option. It's also, annoyingly, no longer a choice on most top-of-the-line smartphones. The iPhone, HTC One and Nokia Lumia don't have removable batteries. Luckily, the Samsung Galaxy and LG G3 still do.

Silent Circle, a company that enables top-end private communication, kept these issues in mind when it co-created the [Blackphone](#). It has a removable battery. It uses PrivatOS, a stripped-down version of Android that reduces tracking.

And because spoofed cell towers can target its antennae too, Blackphone's makers are working with chipmaker Nvidia ([NVDA](#), [Tech30](#)) to develop their own custom, more secure baseband chip.

Related story: The NSA made Obama's BlackBerry

Silent Circle CEO Mike Janke, a former Navy SEAL, said they designed the phone based on revelations that the [NSA can find powered off phones](#) and the [FBI can tap their microphones](#).

You probably don't need to fear that the National Security Agency is using this strategy on your phone, Janke said. Those spies are focused on hunting down a specified list of terrorists and foreign fighters. But he noted that the FBI is using these kinds of surveillance tactics in the U.S. for all sorts of crimes. ■

More from CNN

[Comcast plans data limits for all customers](#)

[China bans Windows 8 from government computers](#)

[Pimco sees another \\$30 billion drain away](#)

[Red Lobster being sold for \\$2.1 billion](#)

[McDonald's under attack on all fronts](#)

[Coping with a \\$15 minimum wage in Seattle](#)

Around the Web

 VerticalResponse

[\[what's this\]](#)



© 2014 Cable News Network. A Time Warner Company. All Rights Reserved. [Terms under which this service is provided to you.](#) [Privacy Policy.](#)