Government Spooks Can Use the Mic and Camera on Trump's Phone Even When He Thinks It Is Turned Off

After reading this article, you might not ever view your electronic devices the same way again.

Last year, Hollywood released a biographical political thriller based on the life of Edward Snowden that had one particularly creepy scene. In that scene, a government spook used a program to remotely activate the microphone and camera on a laptop, and by doing so he was able to watch a woman as she got undressed. Sadly, as you will see below, this kind of thing is happening constantly.

Any digital device can potentially be accessed and used to spy on you even if it appears to be turned off. And this is why Donald Trump needs to be so careful right now, because the intelligence community wants to take him down and they can literally use any digital device in his possession to try to gather dirt on him.

We have a "deep state" that is absolutely obsessed with watching, tracking and monitoring the American people, and something desperately needs to be done about this unconstitutional surveillance. Now that Trump has become greatly upset about how the government was tapping into his phone calls, maybe something will finally get accomplished.

In an article that I just published on *The Most Important News*, I talked about the NSA's brand new two billion dollar data storage facility in Utah that can store up to five zettabytes of data. Secret "electronic monitoring rooms" embedded within the facilities of major communications

companies across the United States send an endless flow of digital information to this facility, and most Americans have no idea that this is even happening. The following comes from Wired:

> *Before yottabytes of data from the deep web and elsewhere can begin piling up inside the servers of the NSA's new center, they must be collected. To better accomplish that, the agency has undergone the largest building boom in its history, including installing secret electronic monitoring rooms in major US telecom facilities. Controlled by the NSA, these highly secured spaces are where the agency taps into the US communications networks, a practice that came to light during the Bush years but was never acknowledged by the agency. The broad outlines of the so-called warrantless-wiretapping program have long been exposed—how the NSA secretly and illegally bypassed the Foreign Intelligence Surveillance Court, which was supposed to oversee and authorize highly targeted domestic eavesdropping; how the program allowed wholesale monitoring of millions of American phone calls and email. In the wake of the program's exposure, Congress passed the FISA Amendments Act of 2008, which largely made the practices legal. Telecoms that had agreed to participate in the illegal activity were granted immunity from prosecution and lawsuits.*

Whistle-blowers have come forward again and again to warn us about what was happening, but they have largely been ignored. One of the most prominent whistle-blowers was former NSA employee William Binney:

> *Binney left the NSA in late 2001, shortly after the agency launched its warrantless-wiretapping program. "They violated the Constitution setting it up," he says bluntly. "But they didn't care. They were going to do it anyway, and they were going to crucify anyone who stood in the way. When they started violating the Constitution, I couldn't stay." Binney*

> *says Stellar Wind was far larger than has been publicly disclosed and included not just eavesdropping on domestic phone calls but the inspection of domestic email. At the outset the program recorded 320 million calls a day, he says, which represented about 73 to 80 percent of the total volume of the agency's worldwide intercepts. The haul only grew from there.*

Can you imagine recording 320 million phone calls a day?

And that was at the beginning of the program—I can't even imagine what the number must be these days.

But even if you aren't using your phone government spooks can still potentially be listening to you. The following comes from a CNN article entitled "How the NSA can 'turn on' your phone remotely":

> *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.*

Unfortunately, these tactics are not just used against "terrorists".

The truth is that these tactics are employed against anyone that the NSA is interested in, and in fact they could be listening to you right now.

Thanks to Edward Snowden, we have learned quite a bit about how the NSA takes over digital devices…

> *The latest story from the Edward Snowden leaks yesterday drives home that the NSA and its spy partners possess specialized tools for doing exactly that. According to The Intercept, the NSA uses a plug-in called GUMFISH to take over cameras on infected machines and snap photos.*
>
> *Another NSA plug-in called CAPTIVATEDAUDIENCE hijacks the microphone on targeted computers to record conversations.*
>
> *Intelligence agencies have been turning computers into listening devices for at least a decade, as evidenced by the Flame spy tool uncovered by Kaspersky Lab in 2012, which had the ability to surreptitiously turn on webcams and microphones and perform a host of other espionage operations.*

So what can you do to prevent this from happening?

If you have external webcams and microphones, you can unplug them when they are not in use.

If you have a built-in camera, some have suggested covering the camera with a sticker.

And of course pulling out the battery entirely will prevent someone from taking over your phone when you are not using it.

But at the end of the day, it is going to be really hard to keep government spooks out of your electronic devices completely. They have become extremely sophisticated at using these devices to get what they want, and they will literally go after just about anyone.

For example, just consider what they did to former CBS reporter Sharyl Attkisson. In **her recent book,** she details a campaign of digital harassment that sounds like something out of a spy novel. The following comes from *The Washington Post*:

> *The breaches on Attkisson's computer, says this source, are coming from a "sophisticated entity that used commercial, nonattributable spyware that's proprietary to a government agency: either the CIA, FBI, the Defense Intelligence Agency, or the National Security Agency (NSA)." Attkisson learns from "No. 1" that one intrusion was launched from the WiFi at a Ritz Carlton Hotel and the "intruders discovered my Skype account handle, stole the password, activated the audio and made heavy use of it, presumably as a listening tool."*
>
> *To round out the revelations of "No. 1," he informs Attkisson that he'd found three classified documents deep inside her operating system, such that she'd never know they were even there. "Why? To frame me?" Attkisson asks in the book.*

If they can do all of that to Sharyl Attkisson, they can do it to Donald Trump too.

Trump needs to understand that the deep state is trying to destroy him, and everything he says and does is being monitored.

So until Trump can completely clean house at all of our intelligence agencies, he is going to have to be extremely careful 24 hours a day.

And let us hope that Trump is ultimately victorious in his struggle against the deep state, because the future of this nation is literally hanging in the balance. {eoa}