America is Now Officially an Orwellian Totalitarian State: The Complete Interactive Guide To How The NSA Spies On Everything You Do

By Zero Hedge

Global Research, April 07, 2014

Scoop new Zealand

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

With all the hoopla about missing airplanes, renewed wars of the cold variety, and rigged markets, it is easy to forget that America is now officially a totalitarian state of the Orwellian kind, where the population has – *involuntarily* – ceded all of its privacy in exchange for… something. Because it certainly isn't security. So we are happy to provide a reminder of just this, especially since as BusinessWeek notes, it gets harder to keep track of all the bizarre ways the National Security Agency has cooked up to spy on people and governments. This may help.

> Data in Motion
>
> NSA's spies divide targets into two broad categories: data in motion and data at rest. Information moving to and from mobile phones, computers, data centers, and satellites is often easier to grab, and the agency sucks up vast amounts worldwide. Yet common data such as e-mail is often protected with encryption once it leaves a device, making it harder—but not impossible—to crack.
>
> Data at Rest
>
> Retrieving information from hard drives, overseas data centers, or cell phones is more difficult, but it's often more valuable because stored data is less likely to be encrypted, and spies can zero in on exactly what they want. NSA lawyers can compel U.S. companies to hand over some of it; agency hackers target the most coveted and fortified secrets inside computers of foreign governments.
>
> Where the Data Goes
>
> Much of the data the NSA compiles from all these efforts will be stored in its million-square-foot data center near Bluffdale, Utah. It can hold an estimated 12 exabytes of data. An exabyte is the equivalent of 1 billion gigabytes.
>
> *And some of the specific methods the NSA uses to spy on US citizens and the occasional offshore "terrorist":*
>
> - Call Recorder – The agency can intercept and store for up to a month 100 percent of a foreign country's telephone calls, which can be sorted and played back.
> - Clone Phones – Foreign targets' cell phones can be surreptitiously

swapped for an identical model with built-in listening and data collection devices.

- Fake Shops – Diplomats at the 2009 G-20 summit in London were tricked, with the NSA’s help, into using an Internet cafe that had been rigged to send data to British intelligence.
- Travel Trackers – The NSA has several ways to follow the movements of intelligence targets as they get off planes, drive across borders, or move around a city, including an implant that directs a cell phone SIM card to send geolocation data via text message.
- Special Delivery – Spies intercept computers that foreign targets buy online, fit them with devices that send data to the NSA, and box them back up for normal delivery.
- X-Ray Vision – Radar waves beamed into a room can detect what is being typed on a keyboard or displayed on a computer screen.
- Credit Cards – The agency tapped into the network of Visa and major banking systems to collect troves of transaction data.
- Satellites – The NSA infiltrated German satellite communications used in remote locations such as drilling platforms—and by the country’s diplomats.
- Gamer Spies – Agency employees join World of Warcraft and Second Life communities, hunting for criminal networks and recruiting informants. They’ve also infiltrated Microsoft’s Xbox Live network.
- Cell Towers – Base stations mimicking cell towers siphon location data from targets’ phones. Agents can also intercept mobile calls with a shoe-box-size receiver.
- Submarines – The agency can collect worldwide Internet traffic with a modified nuclear submarine that taps undersea fiber-optic cables—allowing spies to vacuum data from millions of users.
- Secret Selfies – Malware planted in an iPhone can secretly activate its camera and microphone, turning it into a listening device. Malware for Windows mobile phones enables complete remote control of the handset.
- Fake Rocks – Transmitters hidden inside rocks and other objects can receive information from NSA taps implanted in nearby computers even if they’re “air gapped” machines or networks that aren’t hooked up to the Internet—among the hardest of all digital targets.

The Stasi is spinning in its grave… with jealousy. The full interactive presentation can be found after the jump:

Average:
4.954545
Your rating: None Average: 5 (22 votes)

The original source of this article is Scoop new Zealand

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: Zero Hedge

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

For media inquiries: publications@globalresearch.ca