The Whole POINT of the "Internet of Things" ("IoT") Is So Big Brother Can Spy on You

By Washington's Blog

Global Research, February 11, 2016
Washington's Blog 10 February 2016

The government is already spying on us through spying on us through our computers, phones, cars, buses, streetlights, at airports and on the street, via mobile scanners and drones, through our credit cards and smart meters (update), television, doll, and in many other ways.

Spying in the U.S. is worse than under Nazi Germany, the Stasi, J. Edgar Hoover … or Orwell's 1984.

Yesterday, U.S. Intelligence Boss James Clapper said that the government will spy on Americans through the internet of things ("IoT"):

> In the future, intelligence services might use the [IoT] for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials.

Yves Smith has the definitive comment on Clapper's statement:

> Oh, come on. The whole point of the IoT is spying. The officialdom is just trying to persuade you that it really is a big consumer benefit to be able to tell your oven to start heating up before you get home.

Personally, I'm a tech geek, and love the latest gadgets and toys. But I don't want my dishwasher or refrigerator sending messages to me … let alone the intelligence agencies. Despite all of the hype about IoT, I don't know *anyone* who does.

We've previously noted that the CIA wants to spy on you through your dishwasher and other "smart" appliances. As Slate notes:

> Watch out: the CIA may soon be spying on you—through your beloved, intelligent household appliances, according to Wired.

> In early March, at a meeting for the CIA's venture capital firm In-Q-Tel, CIA Director David Petraeus reportedly noted that "smart appliances" connected to the Internet could someday be used by the CIA to track individuals. If your grocery-list-generating refrigerator knows when you're home, the CIA could, too, by using geo-location data from your wired appliances, according to SmartPlanet.

> "The current 'Internet of PCs' will move, of course, toward an 'Internet of Things'—of devices of all types—50 to 100 billion of which will be connected to the Internet by 2020,"Petraeus said in his speech. He continued:
>
> Items of interest will be located, identified, monitored, and remotely controlled through technologies such as radio-frequency identification, sensor networks, tiny embedded servers, and energy harvesters—all connected to the next-generation Internet using abundant, low cost, and high-power computing—the latter now going to cloud computing, in many areas greater and greater supercomputing, and, ultimately, heading to quantum computing.

And see these comments by John Whitehead and Michael Snyder.

The Guardian notes:

> Just a few weeks ago, a security researcher found that Google's Nest thermostats were leaking users' zipcodes over the internet. There's even an entire search engine for the internet of things called Shodan that allows users to easily search for unsecured webcams that are broadcasting from inside people's houses without their knowledge.
>
> While people voluntarily use all these devices, the chances are close to zero that they fully understand that a lot of their data is being sent back to various companies to be stored on servers that can either be accessed by governments or hackers.
>
> ***

Author and persistent Silicon Valley critic Evgeny Morozov summed up the entire problem with the internet of things and "smart" technology in a tweet last week:

Update: The highest-level NSA whistleblower in history (William Binney) – the NSA executive who created the agency's mass surveillance program for digital information, 36-year NSA veteran widely regarded as a "legend" within the agency, who served as the senior technical director within the agency, and managed thousands of NSA employees – read this post, and told Washington's Blog:

> Yep, that summarizes it fairly well. It does not deal with industry or how they will use the data; but, that will probably be an extension of what they do now. This whole idea of monitoring electronic devices is objectionable.
>
> If forced to buy that stuff, I will do my best to disconnect these monitoring devices also look for equipment on the market that is not connected in any way

Postscript: As security expert Bruce Schneier points out, the entire concept of the IoT is wildly insecure and vulnerable to hacking.

The original source of this article is Washington's Blog

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: Washington's Blog

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

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca