GlobalResearch
Center for Research on Globalization

The Whole POINT of the Internet of Things Is So "Big Brother" Can Spy On You

By Washington's Blog
Global Research, March 16, 2017
Washington's Blog 15 March 2017

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

The government is already 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 (see this), television, doll, and in many other ways.

The CIA wants to spy on you through your dishwasher and other "smart" appliances. Slate reported in 2012:

> 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.

Last year, 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 commented at the time:

> 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.

The Guardian notes:

> As a category, the internet of things is useful to eavesdroppers both official and unofficial for a variety of reasons, the main one being the leakiness of the data.
>
> ***
>
> There are a wide variety of devices that can be used to listen in, and some compound devices (like cars) that have enough hardware to form a very effective surveillance suite all by themselves.
>
> ***
>
> There's no getting around the fundamental creepiness of the little pinhole cameras in new smart TVs (and Xbox Kinects, and laptops, and cellphones), but the less-remarked-on aspect – the audio – may actually be more pertinent to anyone with a warrant trying to listen in. Harvard's Berkman Center for Internet and Society observed that Samsung's voice recognition software in its smart TVs had to routinely send various commands "home" to a server where they were processed for relevant information; their microphones are also always on, in case you're trying to talk to them. Televisions are also much easier to turn on than they used to be: a feature creeping into higher-end TVs called "wake on LAN" allows users to power on televisions over the internet (this is already standard on many desktop PCs).
>
> ***
>
> A cyberattack on toymaker VTech exposed the personal data of 6.4m children last year; it was a sobering reminder of the vulnerability of kids on the web. But technology waits for no man. Mattel's Hello Barbie doll works the same way the Nest and Samsung voice operators do, by passing kids' interactions into the cloud and returning verbal responses through a speaker in the doll. HereO manufactures a watch for kids with a GPS chip in it; Fisher-Price makes a WiFi-enabled stuffed animal. Security researchers at Rapid7 looked at both and found that they were easy to compromise on company databases, and in the case of the watch, use to locate the wearer.

In a separate article, the Guardian pointed out:

> Just a few weeks ago, a security researcher found that Google's Nest thermostats were leaking users' zip codes 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:
>
> In case you are wondering what "smart" – as in "smart city" or "smart home" – means:
>
> Surveillance
> Marketed
> As
> Revolutionary
> Technology
>
> > In case you are wondering what "smart" – as in "smart city" or "smart home" – means:
> >
> > Surveillance
> > Marketed
> > As
> > Revolutionary
> > Technology
> >
> > — Evgeny Morozov (@evgenymorozov) February 1, 2016

And in the wake of the CIA leaks showing that the agency can remotely turn on our tvs and spy on us using a "fake off" mode so that it looks like the power is off, Tech Dirt wrote in an article called CIA Leaks Unsurprisingly Show The Internet Of Broken Things Is A Spy's Best Friend:

> The security and privacy standards surrounding the internet of (broken) things sit somewhere between high comedy and dogshit.

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

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 – reviewed an earlier version of 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.

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: Washington's Blog