



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

Par [Washington's Blog](#)

Mondialisation.ca, 11 février 2016

[Washington's Blog](#) 10 février 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](#).

Articles Par : [Washington's Blog](#)

Avis de non-responsabilité : Les opinions exprimées dans cet article n'engagent que le ou les auteurs. Le Centre de recherche sur la mondialisation se dégage de toute responsabilité concernant le contenu de cet article et ne sera pas tenu responsable pour des erreurs ou informations incorrectes ou inexactes.

Le Centre de recherche sur la mondialisation (CRM) accorde la permission de reproduire la version intégrale ou des extraits d'articles du site [Mondialisation.ca](#) sur des sites de médias alternatifs. La source de l'article, l'adresse url ainsi qu'un hyperlien vers l'article original du CRM doivent être indiqués. Une note de droit d'auteur (copyright) doit également être indiquée.

Pour publier des articles de [Mondialisation.ca](#) en format papier ou autre, y compris les sites Internet commerciaux, contactez: media@globalresearch.ca

[Mondialisation.ca](#) contient du matériel protégé par le droit d'auteur, dont le détenteur n'a pas toujours autorisé l'utilisation. Nous mettons ce matériel à la disposition de nos lecteurs en vertu du principe "d'utilisation équitable", dans le but d'améliorer la compréhension des enjeux politiques, économiques et sociaux. Tout le matériel mis en ligne sur ce site est à but non lucratif. Il est mis à la disposition de tous ceux qui s'y intéressent dans le but de faire de la recherche ainsi qu'à des fins éducatives. Si vous désirez utiliser du matériel protégé par le droit d'auteur pour des raisons autres que "l'utilisation équitable", vous devez demander la permission au détenteur du droit d'auteur.

Contact média: media@globalresearch.ca