theguardian

The government just admitted it will use smart home devices for spying

Trevor Timm

Many consumers are wholly unaware that the smart devices making their home more custom and responsive are making data that can be hacked or collected

Tue 9 Feb 2016 15.29 EST Last modified on Tue 9 Feb 2016 15.39 EST

If you want evidence that US intelligence agencies aren't losing surveillance abilities because of the rising use of encryption by tech companies, look no further than the testimony on Tuesday by the director of national intelligence, James Clapper.

As the Guardian reported, Clapper made clear that the internet of things – the many devices like thermostats, cameras and other appliances that are increasingly connected to the internet – are providing ample opportunity for intelligence agencies to spy on targets, and possibly the masses. And it's a danger that many consumers who buy these products may be wholly unaware of.

"In the future, intelligence services might use the [internet of things] for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials," Clapper told a Senate panel as part of his annual "assessment of threats" against the US.

Clapper is actually saying something very similar to a major study done at Harvard's Berkman Center released last week. It concluded that the FBI's recent claim that they are "going dark" – losing the ability to spy on suspects because of encryption – is largely overblown, mainly because federal agencies have so many more avenues for spying. This echoes comments by many surveillance experts, who have made clear that, rather than "going dark", we are actually in the "golden age of surveillance".

Privacy advocates have known about the potential for government to exploit the internet of things for years. Law enforcement agencies have taken notice too, increasingly serving court orders on companies for data they keep that citizens might not even know they are transmitting. Police have already been asking Google-owned company Dropcam for footage from cameras inside people's homes meant to keep an eye on their kids. Fitbit data has already been used in court against defendants multiple times.

But the potential for these privacy violations has only recently started reaching millions of homes: Samsung sparked controversy last year after announcing a television that would listen to everything said in the room it's in and in the fine print literally warned people not to talk about sensitive information in front of it.

While Samsung took a bunch of heat, a wide array of devices now act as all-seeing or all-listening devices, including other television models, Xbox Kinect, Amazon Echo and GM's OnStar program that tracks car owners' driving patterns. Even a new Barbie has the ability to spy

on you – it listens to Barbie owners to respond but also sends what it hears back to the mothership at Mattel.

Then there are the rampant security issues with the internet of things that allow hackers – whether they are criminal, government or something in between – to access loads of data without any court order, like the creeps who were eavesdropping on baby monitors of new parents. 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.

While Clapper's comments are generating new publicity for this privacy worry, the government has known about the potential to exploit these devices for a long time. The then CIA director David Petraeus made clear that intelligence agencies would use the internet of things to spy on people back in 2012, saying:

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.

As Wired put it, Petraeus was expressing excitement the CIA would soon be able spy on you through your dishwasher.

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 - February 1, 2016

While internet-connected devices are not going away – it's a certainty they will only get more prevalent – it's important that companies make them as secure as the end-to-end encryption the FBI director loves to complain about, and that we press the government to enact strict new rules to prevent our privacy from being invaded thanks to the weakest link among televisions or dolls or thermostats that line billions of homes around the world.