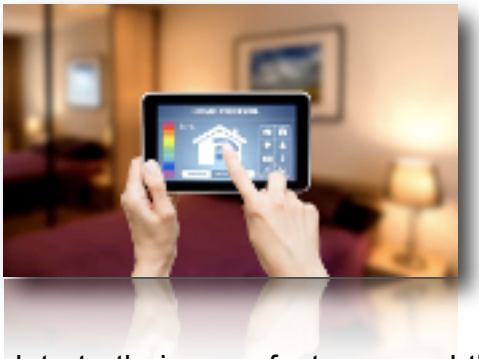
The Guardian International edition

Alex Hern
@alexhern
Friday 1 June 2018

# UK homes vulnerable to 'staggering' level of corporate surveillance

## Smart home appliances send data to manufacturers and third parties, Which? warns



The findings by the consumer organisation Which? have alarmed privacy campaigners. Photograph: scyther5/Getty Images/iStockphoto

British homes are vulnerable to "a staggering level of corporate surveillance" through common internet-enabled devices, an investigation has found.

Researchers found that a range of connected appliances – increasingly popular features of the so-called smart home – send data to their manufacturers and third-party companies, in some cases failing to keep the information secure. One Samsung smart TV connected to more than 700 distinct internet addresses in 15 minutes.

The investigation, by Which? magazine, found televisions selling viewing data to advertisers, toothbrushes with access to smartphone microphones, and security cameras that could be hacked to let others watch and listen to people in their homes.

The findings have alarmed privacy campaigners, who warn that consumers are unknowingly building a "terrifying" world of corporate surveillance.

> "Smart devices are increasingly being exposed as soft surveillance devices that owners have too little control of," said Silkie Carlo, the director of Big Brother Watch. "People are now being subjected to invasive and unnecessary corporate snooping on an unprecedented scale.
>
> "The very notion of a smart home is one of ambient surveillance and constant recording, which will without doubt lead people to modify their behaviour over time. If this current direction is continued, we will become a society of watched consumers subjected to the most granular, pervasive and inescapable surveillance. It is a terrifying thought."

Which? bought more than £3,000 worth of smart home equipment and set it up in a lab to monitor how much data was being collected and transferred. As well as the manufacturers, more than 20 other companies were on the receiving end of data transfers including social networks, third-party monitoring services, advertising and marketing data brokers.

Just one device – a Samsung smart TV – connected to more than 700 distinct internet addresses after being used for 15 minutes. If the viewer accepts Samsung's privacy policy, the company gains the right

to monitor what is being watched and when. It uploads some of that data to Samsung's advertising platform, Which? says, "suggesting it is used for marketing". Another Samsung device, the company's Smartthings hub, sits at the heart of the smart home and has a privacy policy that allows aggregated information to be shared with "advertisers and/or merchant partners".

Other devices didn't transmit much data but unnecessarily asked for it anyway, creating the possibility of breaches down the line. A Philips bluetooth toothbrush, for instance, links up with a smartphone app to monitor brushing habits, frequency and technique. But the app also asks for location information, which Philips said was used only to find a local company store, and microphone access – Philips said this wasn't used at all.

Some devices collected only the data they should, but then failed to keep it secure. Which? tested a security camera, sold under the IeGeek brand, and found a security flaw in the app that meant the company could access usernames and passwords for other cameras. If they had misused that access, they could have seen live video feeds from other people's homes, and even talked to those users. That flaw was fixed by IeGeek, but Which? has since found others that are still live.

Alex Neill, the managing director of Which? home products and services, said the investigation showed the downside of a digital home.

> "Smart home gadgets and devices can bring huge benefits to our daily lives, but our investigation shows they can collect vast amounts of data about us," he told the Guardian.
>
> "Companies should be clear about how they are collecting and using data and ensure consumers feel in control about what they are sharing — without having to trawl through impenetrable terms and conditions."

While users may be comfortable trading their data for free services, or for a better quality of product, Which? suggested that it may be worth thinking twice about intrusive monitoring connected to paid products – particularly when "dumb" devices are frequently cheaper, and just as useful.

> "Not all data collection is bad," the organisation concluded. "In fact there can be real benefits for those who want a more personalised service or some extra features. However, you need to know what you're getting into when you choose to buy an internet-connected product over a traditional 'dumb' one.

With services such as Facebook and Gmail, you're getting a free resource in exchange, at least partially, for access to your data.

> "With products that you've purchased, however, there's even more onus on companies to be transparent over what information they're collecting, and how it is being used."

In a statement, Samsung said:

> "Samsung takes consumers' privacy and data security very seriously and is in compliance with all the EU directives and regulations of member states on personal data privacy. We

> have also taken extra steps given the implementation of the General Data Protection Regulation (GDPR), in order to ensure our compliance with the regulation.
>
> We will continue to work on strengthening and improving our policies, procedures, organizational structures and systems to ensure our customers have more control over their personal data and to guarantee a high level of data protection."

Which?'s research comes days after Google[1] made a new push into the smart home market, launching a video doorbell in the UK that uses facial recognition technology to identify friends and family when they're at the front door.

The Nest Hello, from the search firm's smart home division, is a £229 wifi-connected doorbell that uses a wide angle camera to pump video footage of visitors to connected smartphones. A bundled AI system can analyse video from the front door automatically, alerting residents to suspicious visitors while welcoming loved ones and residents.

The device may raise privacy fears, analysts warned.

> "Facial recognition on smart home cameras is not something new but the Nest Hello will likely raise awareness among consumers that could spark a deeper debate about the implications of such technology being deployed by people's front doors," Ben Wood, chief of research at CCS Insight, said. "This could be a major challenge for Google[2] given the broader unease around privacy at present."

Which? has also been carrying out a policy study to understand the public's attitudes to data collection and use. The report, to be published on 5 June, will raise important questions about how to build consumer confidence in the data ecosystem following the introduction of GDPR, it says.

---

1 https://www.theguardian.com/technology/2018/may/31/nest-hello-google-launches-facial-recognition-data-doorbell-uk-privacy-concerns-amazon-ring

2 https://www.theguardian.com/technology/google