https://www.theguardian.com/technology/2020/mar/08/how-to-stop-your-smart-home-spying-on-you-lightbulbs-doorbell-ring-google-assistant-alexa-privacy

The Guardian

How to stop your smart home spying on you

Everything in your smart home, from the lightbulbs to the thermostat, could be recording you or collecting data about you. What can you do to curb this intrusion?

Davey Winder

Sun 8 Mar 2020 09.00 EDT

During an interview with the BBC last year, Google's senior vice-president for devices and services, Rick Osterloh, pondered whether a homeowner should disclose the presence of smart home devices to guests. "I would, and do, when someone enters into my home," he said.

When your central heating thermostat asks for your phone number, your TV knows what you like to watch and hackers can install spyware in your home through a lightbulb security flaw, perhaps it's time we all started taking smart home privacy issues more seriously. Just this week the National Cyber Security Centre issued a warning to owners of smart cameras and baby monitors to review their security settings.

You can get a quick overview of privacy options for many smart home devices using the Mozilla "*privacy not included" guide; however if you've already invested in particular technology, all is not lost. A few configuration tweaks could help put you back in control when it comes to balancing device performance with data privacy (and they don't involve wearing anything like the ludicrous-looking "bracelet of silence", which jams smart device microphones, as recently demonstrated by a team from Chicago University).

Is your smart TV watching as you watch telly?

When the FBI, no less, warns users that their televisions could be listening to and watching them, maybe it's time to reflect upon how dumb we are when it comes to smart TVs. Let's face it, most of us buy a big TV with all the internet streaming and programme guide functionality we can afford and kick back in front of it. Beyond the initial tuning in of stations and maybe adjusting the colour to our taste, there's not much configuration tweaking that goes on - which is a mistake when both privacy and security issues are in the picture. TVs nowadays connect to the internet, have web browsers, run apps, and can be controlled by your voice; automatic content recognition (ACR) watches what you see, from TV programmes to games, and the resulting data can target you for personalised advertising and produce viewing recommendations - often across various platforms. You probably agreed to ACR being used when you were setting up your new telly. To disable it - although this varies from TV to TV - head for the general or advanced settings and look for a "viewing information" or "viewing data" option. This will stop some "smart" things like recommendations, and even some voice activation functions, from working properly, so bear in mind that ACR data is anonymised before heading for the off button.

Reduce the smart speaker 'threat surface'

Smart speakers and digital assistants come in many guises; what they all have in common is that, by necessity, they are always listening. Recent research suggests that 59% of smart speaker users have privacy concerns, with unwanted listening and data collection being front and centre.

Of course, only you can determine whether having a voice-controlled "*Star Trek* computer" in your home outweighs those privacy concerns. It is possible, however, to retain the smart performance while minimising the privacy "threat surface". To prevent the Amazon Alexa or Google Assistant account holder from being able to view any requests you've made or questions you've asked, you can tell Alexa to "delete what I just said" and Google Assistant to "delete my last conversation". This does require the account holder to have enabled the "delete by voice" option in their settings, though. If you are the account holder, you can use the "voice match" function for Google Assistant to prevent your results from being available to anyone who simply asks for them. You can manage how Amazon uses your data by opening the Alexa app and heading for Settings | Alexa Privacy and toggling the "help improve Amazon services" option off along with the "use messages to improve transcriptions" setting. Google Assistant users can use the Home app via Settings | More Settings | Your Data to pause collection of any more voice recordings. However, Google warns that this can "limit or disable" more personalised experiences across Google as a result.

Ring the changes for your smart doorbell

A home security surveillance system requires video cameras to record what's going on. When those security cameras are connected to, and accessible from, the internet, questions about who is watching the watcher come to the fore. When those connected cameras can be found in everything from your doorbell to the baby monitor in the nursery, privacy issues cannot be ignored. Amazon-owned Ring is perhaps most famous for its video doorbells and in the US Congress, Amazon is facing questions about the sharing of Ring data (including video footage) with more than 900 police departments.

Moreover, following investigations that found Ring had shared information with the likes of Facebook and Google, the company has said it doesn't sell personal information to anyone and has suspended the use of most third-party analytics services in Ring apps while it works to provide greater ability to opt out in its new Control Center. This already lets users manage privacy and security options such as two-factor authentication, sharing information with third parties for personalised advertising, and managing any shared users. Clicking on the authorised client devices option will show all the devices that can access your Ring account, and therefore your videos. This will show the device and whether it's logged into your account. To remove any you don't recognise, remove all authorised client devices as one and then re-enrol them individually.

Is your central heating a threat to your privacy?

That we are even talking about privacy concerning your thermostat is, frankly, pretty nuts. But fears around central heating technology and privacy are a reality. In the case of the Google-owned Nest thermostat, however, those fears are ill founded. Despite some news reports to the contrary, your Nest thermostat has neither a camera nor a microphone inside. On the other hand, thermostats such as the Alexa-supporting ecobee4, do have microphones. The latter also has a privacy mode that can be activated once the thermostat is installed: tap the microphone

icon at the bottom right of the thermostat screen and select voice control off. You won't then be able to use Alexa to control the thermostat, but nor will it listen continuously for wake words or send recorded messages to Amazon. Both ecobee4 and Nest users can have all their personal information removed upon request, but this deletes their account and disables the remote access and "smart" connected functionality you bought the device for. A Nest thermostat will collect data such as your setup information, environmental data from its sensors, heating and cooling usage.

Shedding light on smart bulb security

Earlier this year, security researchers confirmed that a vulnerability could enable a hacker to launch an attack on your home computer network, and therefore your data, by way of a Philips Hue smart lightbulb. The vulnerability, without getting too technical, was actually in a low-power wireless protocol used to control many different Internet of Things (IoT) smart devices. Philips was quick to issue a new firmware update that fixed the problem before it was publicly disclosed. You can make sure your lightbulbs are protected by opening the Philips Hue app and heading to Settings | Software Update. This will alert you if an update is needed, but to prevent any further checking, you can enable the "automatic update" option on the same page.