**HOW THE 'SMART HOME' COULD ALLOW YOUR HOUSE TO SPY ON YOU AND BE MANIPULATED BY HACKERS?**

It’s the stuff of horror films: an intruder in your house, impossible to find but undeniably somewhere, watching you at your most private moments. Or perhaps it’s the plot of a thriller, where you are recruited into international crime without even knowing it, at the behest of smart criminals.

If the worst fears about the prevalence of weakly secured smart home gadgets materialise, those terrifying situations could become all too real. As we fill our homes with internet-enabled and smart devices, we are opening ourselves up to attacks that exploit houses themselves – and we might not even realise they are happening.

Everything from washing machines to baby monitors is being hooked up to the internet by companies convinced that features such as remote control and artificial intelligence will make our lives easier and safer. But they could also endanger the very people using them.

The government has now published a voluntary code of practice for manufacturers of smart home devices in an attempt to stop them being used for cyber crime by hackers and even nation states.

GOOGLE NEST DOOR BELL…

Google’s new Nest Hello is a video doorbell that aims to be smarter than the rest with constant recording, face and object recognition.

The Hello is a direct replacement for a wired doorbell, working with an existing chime and requiring constant power, making it one of the high-end options for smart doorbells.

That need for power restricts where you can put it, unlike some more flexible options such as the battery-powered [Ring Video Doorbell 2](https://www.theguardian.com/technology/2018/feb/01/ring-video-doorbell-2-review-deal-with-doorsteppers-from-your-own-sofa), but enables some much more powerful features.