Smart homes need to start treating their inhabitants better

April 20 2016, by David Hutchison

Credit: AI-generated image (disclaimer)

We might still be some way from coming home to robots doing the cooking and cleaning for us, but the age of widespread home automation has arrived. More and more people now have "intelligent" versions of devices like thermostats and lighting in their home, that either run automatically or can be controlled from a smartphone.

But the home automation market is very much still in its infancy. There are many newly developed products from a wide range of companies and few of them are compatible with one another. This lack of standards signals a tough time ahead for both manufacturers and consumers. Until the industry addresses some key issues, it looks set to struggle.

Google's recent decision to make some of its home automation products useless does not offer much hope. The company's smart home division, Nest, has come under fire for buying up and shutting down rival business Revolv.

Revolv manufactured hub technology that allowed multiple smart devices from different brands to be controlled from a single smartphone app. Nest bought the company, along with its expertise and staff, to further develop its own "Works with Nest" hub platform. In theory, this move to create greater compatibility between different smart devices in a less crowded marketplace should have been good for the sector.

But then Nest decided to switch off the servers that enabled Revolv's hubs to operate, a move that will leave customers with useless boxes that they paid US$300 (£210) for. This happened despite previous assurances from Nest and the promise Revolv customers were originally given that their products would be supported with a "lifetime subscription".

Credit: AI-generated image (disclaimer)

Don't overpromise

The lessons we should take from this affair are that fledgling vendors (such as Revolv) should never promise a "lifetime subscription", and potential customers should be extremely wary of such promises – if not even as a warning not to buy. Nest will surely have to regain some credibility in the market by compensating owners of Revolv devices, which they have already said they will do on a case-by-case basis.

It's clear that several factors need to be resolved, though perhaps at different paces. This includes establishing appropriate regulations to protect consumers against future "bricked" products like the soon-to-be unusable Revolv hubs.

We also need a more open set of products and services based on a standardised platform that isn't restricted to certain manufacturers. A good example of how this can be done comes from the home entertainment sector where TV and radio broadcasting and now digital streaming systems and services have become fairly ubiquitous via standards. **via standards?**

Standardisation in home automation has already started to happen with the creation of the Zigbee wireless communication protocol by a large number of major manufacturers. But there other more closed wireless home control platforms including Z-Wave that remain popular.

Security and resilience

Another area that needs addressing is security, specifically how to protect devices and the data that they produce from hackers. Companies often pay lip service to security but in reality treat it of secondary importance until hackers get in and steal data or do damage to systems and services. Then the operators and providers pay attention.

Now that IT and communications are at the heart of so many systems in everyday use, they are becoming seen as critical, and are increasingly the target of cyber-attacks. In the future this could include home automation, where hubs, smart energy meters, and security cameras could be remotely accessed by hackers, who could access private data or control devices in the home.

Resilience, the ability of systems to recover and keep offering service, is perhaps even more crucial, and is the subject of new and important research by computer scientists. Resilience is about recognising that systems, even those apparently protected by security, can and will be breached. That doesn't just mean cyber attacks but all sorts of challenges including power failures, hardware and software faults, problems due to system complexity and even people-based errors. Resilience research is about trying to identify the problems and to design mechanisms for getting back to normal operation.

We may also need to see more novel and substantial applications before home automation really takes off. Smart fridges that text you when you run out of milk probably won't be enough.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation

Citation: Smart homes need to start treating their inhabitants better (2016, April 20) retrieved 26 June 2024 from https://phys.org/news/2016-04-smart-homes-inhabitants.html