Even sex toys can be connected to the internet – and hacked

April 10 2017, by Kate Devlin

Credit: CC0 Public Domain

Your photos aren't safe online. Repeated incidents of celebrities having their internet accounts hacked and intimate pictures distributed across the web have made this clear. Yet one company decided to put a camera into a sex toy and connect it to the internet. And, predictably, a security firm now claims it has found a way to hack and intercept the vibrator's video stream.

This follows the recent case of another smart vibrator manufacturer, Standard Innovation, agreeing to pay an out-of-court settlement of CAD$4m (£2.4m), after it emerged that the company was harvesting data from its devices. The case was started by two unnamed female users who realised that the device was collecting and relaying data on how often it was used, the vibration settings selected and – eyebrow-raisingly – its temperature, all linked to each user's email address. This meant the firm could build a rather detailed and personal profile of an individual's sexual activity.

Such data collection is becoming more common thanks to the growth of the Internet of Things, which is essentially a way of describing devices that can send and receive data online, from fitness trackers to smart fridges that tell you when you've run out of milk. With the spread of this technology, concerns over what personal information is being collected – and who can access it – are only going to become more important.

The device in the Standard Innovation case was a sex toy called the We-Vibe, a vibrator that can be controlled from an app via Bluetooth. Smart sex toys can act just like fitness trackers, recording the activity of their users. But the activity they track is a little more sensitive. And connecting any device online creates a risk it can be hacked.

The particular vulnerability of the We-Vibe was revealed back in 2016 when two independent hackers speaking at the DEF CON conference showed that a third party could take control of the vibrator. On the surface this might seem like an amusing idea but, after two seconds of consideration, it obviously becomes a complete violation. They also broke the news that the We-Vibe was sending data every minute it was being used.

There's actually nothing that suspicious about technologies collecting data for market research. It's commonplace for manufacturers to monitor how their products are used. Being able to spot patterns and trends in data means being able to improve the quality of your product in response to user requirements. For example, fertility calculators that gather and analyse users' menstrual cycle data can pinpoint with great accuracy whether the user is fertile or not. The more information the algorithm has, the more accurate it can be.

But there are three potential issues around this kind of dating sharing. First, there is the question of whether the company has permission from the user. Explanations of exactly what data is being collected and what will happen to it are often buried in lengthy terms and conditions that users rarely read in full, even if they can understand them.

Second, in a world of big data, even supposedly anonymous data is no guarantee of real anonymity. With every connected click we make, we leave a trail of digital footprints that can be pieced together to identify us.

And third, there's the issue of what's going to happen to that data in the long term. Your data might be securely stored and supposedly unidentifiable to others, but what happens when the companies who created your devices are merged, or acquired, or simply go out of business? In most cases you face the possibility of your information being lost, migrated or discarded, all adding to the lack of user control.

On top of this, while individual countries have their own data protection laws to govern these issues, there are still grey areas over which local rules apply to multinational companies – and uncertainty over the ability to enforce them.

And even if a company follows all the rules the data could still be stolen. Details of how many steps you walk each day probably aren't that interesting to hackers (though might have value to your health insurance supplier) but most people probably wouldn't want the intimate information collected by We-Vibe made available – and therein lies the potential for blackmail. This problem is even more obvious with something like a camera-equipped vibrator.

But the threat of having a personal video stream hacked is only one short-term issue. Companies such as married dating site Ashley Madison have had entire databases of customer information stolen and published. And it doesn't take a criminal hacker for this to happen. Data loss can occur when companies' computer systems fail or even when staff leave hardware lying around.

Consumers must be assured that their information is safe. That could be a choice about which company they trust, or which product they use. Users should have control, from the features of the technology they choose, to where their data ends up. Digital abstinence isn't the necessarily the answer, but when it comes to smart sex tech, corporate voyeurism is a huge turn-off.

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

Provided by The Conversation

Citation: Even sex toys can be connected to the internet – and hacked (2017, April 10) retrieved 8 May 2024 from https://phys.org/news/2017-04-sex-toys-internet-hacked.html