techradar pro

Are our phones listening to us?

By Dmitry Bagrov 12 days ago Internet

Our smartphones may not be listening but plenty of data is being collected about us online

Image Credit: Pixabay

Are our mobile phones spying on us? It's a hot topic right now and there has been much discussion about it. Are they listening to our every conversation, creeping us out by serving us with ads for things straight after we've just discussed them with wives, husbands, children, neighbours?

Many of us have tested our phones. We discuss the house decorating that you're doing and shortly afterwards are served paint ads. Or we discuss the summer holiday and then we're served adverts from hotel companies. And then conclude that our phones must have been listening.

The belief is that a group of Data Satanists got together and, having sacrificed a goat or two, devised a way to individually spy on everyone in the world that has a phone to do bad things. Or at least to sell us things in real time, virtually as we think of them.

- Facebook paid users to install a VPN that spies on them
- Chrome will soon make it harder for websites to spy on you
- Hackers used Apple tech to put malicious apps on iPhones

But the truth is, just because something is possible, doesn't mean it's viable. Our phones are very unlikely to be listening to us and then responding individually, as appears to be the case sometimes.

So, what is going on?

Receiving an advertisement for something we have just discussed proves precisely nothing, certainly not that our phones are "listening" to us and answering us with adverts.

Was the phone connected to a Google account? Did the person getting the ads read any emails or articles about decorating, or holidays? If they did - and it was done using a browser that had access to their Google account, there is, in fact, no need for their phone to listen to them. All that needs to be done for advertisers to try to sell them stuff, is to analyse their cookies.

The fact is, that if Facebook and Apple were to conduct a global snooping exercise, targeting us individually, there'd be huge technical issues and both companies would go bust simply through the sheer amount of traffic they'd have to handle. Far more valuable and cost-efficient for Facebook is digital footprint analysis.

Isaac Asimov, renowned for writing fiction that often predicted future trends, imagined a science called "psychohistory", which combined various statistics to predict how large groups of humans would behave in the future. The idea was that, while it's almost impossible to predict what one person will do in the future, due to too many possible variables, the laws of statistics can be used to predict what very large groups of people will do. Asimov illustrated the principle with the analysing the behaviour of gas. While a scientist can't predict what one gas molecule will do, he/she can predict what a large amount of gas is going to do when exposed to a specific environment in a specific space.

So it is with the data that is collected on us today. Those collecting it are not concerned with us as individuals. They want to know what all of us, broken down into categories, are going to do, think or want. We're still too unpredictable and expensive to target singly. Rather, data is being collected, in various ways, that feeds into greater knowledge of behaviour of different crowds.

Digital footprints are bigger than single conversations

The size of our digital footprints, even without the mythical audio snooping, is phenomenal. People scroll through Facebook and Instagram feeds, like, share, send messages, stay on some posts for a longer time than others, click on notifications as soon as they see them, indicating an interest in the topic and so on. We google information, read the news, write emails, and visit web sites. And most of all, we make purchases online and offline. Yes, that's right – offline is key too – because, yes, along with online-only vendors, Visa and Mastercard also sell your data, along with the owners of loyalty card programs.

Those clever Data Satanists created predictors that understand the optimal time to show different types of people advertising, and what sort of advertising this should be to maximise the chance of selling things to them.

So, Peter, a highly-paid manager, bought a car three-and-a half years ago. Recently, Peter paid several bills from the local garage, but did not extend his car insurance. Two of Peter's friends, who were with him in the same geolocation at the time he was (no doubt waiting for a fourth person to fill a tank), at this moment googled "BMW X5" and "Audi Q7". Peter comes home and sees an advertisement for the "Mercedes GLS", which he talked about with friends later in a bar.

Oh My God! Facebook has been eavesdropping on him! No, not directly eavesdropping, but collating information gleaned from Peter's complex digital footprint, largely based on cookies.

It would make no economic sense to develop technology to listen to conversations, then parse and match keywords in that conversation, particularly given that advertisers pay around 10 pence every time someone clicks through from a served advertisement. We can assume that advertisers are not tracking us in this way.

Image Credit: Shutterstock

What should we be worried about regarding data collection?

Certainly, not the serving up of a few targeted ads, giving us the opportunity to either buy, or not buy, according to our wishes.

Far more concerning, is the use of recognition technology, which is also based on data, which blurs the lines between convenience and consent. Convenience technology has vast potential for abuse. This year, China's first facial recognition payment-based shopping street opened. More will be coming. So seamless is paying in this way, that the consumer doesn't have to do anything much. China is also talking about widespread payment for public transport in this way.

While globally we are still in a largely wild west unregulated environment with regard to data collection, it is worrying that we could slip into systems not where we were being annoyed by targeted ads, but where we buy things, or agree to things, without knowing that that's what we've done. Where the marketers are so sure they know who we are and what we want and what our spending power is, that they go ahead and sell us things without troubling us for specific consent. And that is when the line is crossed, and it could be hard to put the genie back in the bottle.

Dmitry Bagrov, Managing Director at DataArt
Soutce: https://www.techradar.com/news/are-our-phones-listening-to-us