Amazon, Facebook and Google don't need to spy on your conversations to know what you're talking about

January 16 2019, by Jason Nurse

Credit: AI-generated image (disclaimer)

If you've ever wondered if your phone is spying on you, you're not alone. One of the most hotly debated topics in technology today is the amount of data that firms surreptitiously gather about us online. You may well have shared the increasingly common experience of feeling creeped out

by ads for something you recently discussed in a real life conversation or an online interaction.

This kind of experience has led to suggestions that tech firms are secretly recording our private conversations via smartphones or other internet-connected devices such as smart TVs, Amazon Echo or Google Home. Or that they are reading our private messages even when they are supposedly encrypted, as with Facebook's WhatsApp. If this were proven to be true, it would reveal a huge conspiracy that could do untold damage to the tech industry – which makes it seem somewhat far-fetched. But recent revelations about the degree to which Facebook users' data has been shared certainly won't help to convince people that the big firms aren't spying on them.

Yet, there is another, more compelling reason for the incredibly relevant ads you see. Simply put, tech firms routinely gather so much data about you in other ways, they already have an excellent idea what your interests, desires and habits might be. With this information they can build a detailed profile of you and use algorithms based on behavioural science and trends found elsewhere in their data, to predict what ads might be relevant to you. In this way they can show you products or services that you've been thinking about recently, even if you've never directly searched for or otherwise indicated online that you'd be interested in them.

Firms invest heavily in gathering user data and do so in a number of clever ways. Social networks and other apps offer to store and share our uploaded data for "free" while using it, and the content we access and "like", to learn about our interests, desires and relationships. And, of course, there is our search history, which can reveal so much about our current circumstances that Google data has even been used to spot the start of flu epidemics.

But it gets far creepier. Your personal email inbox is also fair game for tech firms. In 2017, Google said it would no longer analyse email content for the purposes of advertising, but recent reports suggest that other large firms still do this. New tech also provides another data source , be it wearables, smart TVs, other in-home smart devices or the smartphone apps that we have come to love. These can gather data on how you use your smart devices, who you contact, what you watch and for how long, other devices on your home network, or where you go.

It's not just individual sites or devices that monitor your online behaviour. A massive ecosystem of advertisers and supporting companies is dedicated to tracking your activity across the internet. Sites commonly record what pages you look at by saving a small file called a "cookie" to your browser. And your activity across different sites can be matched by looking at your browser's "fingerprint", a profile made up of details such as your screen size, the version of the browser you're using and what plug-in tools you have downloaded to use with it. Then, when you visit another website, an ad firm that has built a profile of you based on your cookies and browser fingerprint can load a "third-party script" to display ads relevant to your profile.

Perhaps even more alarmingly, this tracking does not stop at online data. Tech firms are known to purchase data from financial organisations about user purchases in the real world to supplement their ad offerings. According to some reports, this includes information on income, types of places and restaurants frequented and even how many credit cards are present in their wallets. Opting out of this tracking and onward data sharing is incredibly difficult.

Even where you ask to opt out of this data gathering, your request might not be respected. An example is the uproar caused when it was discovered that Google tracks the location of Android users even when the location setting is turned off. Location data is one of the most useful

for advertising and many firms, including Apple, Google and Facebook, track the location of individuals to use as input into their bespoke algorithms.

Putting the data together

To sum up with a simple example, imagine you have just started to think about where to go for your next holiday. You spend the morning visiting travel agents to discuss the latest deals and then visit your favourite restaurant, a popular Caribbean food chain, in the city. Excited about your potential trip, later that night you watch mostly TV shows on the tropics. The next day, your social media feed contains flight, hotel and tour ads with deals to Barbados.

This is a very real illustration of how data on your location, financial purchases, interests, and TV viewing history can be correlated and used to create personalised ads. While some might welcome holiday deals, it becomes much more worrying when we consider data gathering or ads targeting sensitive health issues, financial difficulties, or vulnerable people such as children.

The future of digital advertising is set to be as scary as it is intriguing. Even with new laws that try to protect people's information, tech firms are constantly looking to push the boundaries of data gathering and algorithm design in ways that can feel invasive. It may yet be proven that some firms aren't being honest with us about all the data they collect, but the stuff we know about is more than enough to build an alarmingly accurate picture of us.

Provided by The Conversation