Podcast Orange – Episode 6

Personal data : can we trust our smartphones ? 2/2

By : Spintank
To : Orange
20 January 2020

Introduction

- Nate :

"My fiancée and I both had wedding ads the day after we got engaged, before we had told anyone. We bought the ring in the spur of the moment and never looked anything related up."

- Melissa :

I visited a friend who was setting up security cameras at her house. I have never used the internet to look at anything remotely linked to home security, yet less than an hour after discussing how to set up the cameras, I had a Facebook ad for home security cameras.

- Justin :

[Tested this and settled the debate at a bar with some friends]... As I had not bought, searched for, or even thought about a new bed in several years and I couldn't remember seeing a mattress ad online ever, we started talking about beds and mattresses and guessing keywords, like slipping 'California king' and 'buy a mattress online' into the conversation, while intermittently scrolling facebook.
"Two mattress ads in five minutes. None before that conversation."

- **Joe :**

These witness accounts can be read on the BBC in an article from 2017. And you've surely heard this being discussed by friends and family. Perhaps you've had a similar experience with ads appearing on Facebook or other applications just after discussing something specific in your daily life.. So, are our smartphones listening to us? Are we each carrying our own little spy around in our pocket? That's the subject for today. Welcome to the Memo, the podcast that probes the big digital topics. Hello Chloé!

- Chloé :

Hello Joe !

- Joe :

"Is my telephone listening to me" is a question that comes up very frequently on the net- you can come across it in many articles, forums, videos..

- Chloé :

Yes, and just like the witnesses we've just heard from, we often experience troubling coincidences, like this youtuber who did their own test in a live video… He said the words "dog toy" several times, placing them randomly in what he was saying. And after only a few minutes, while he was still speaking, he was given adverts for a brand of dog toy! He showed us everything live on his screen.

- Joe :

So we're right to be worried?

- Chloé :

Well, not so fast.. This video was widely criticised by experts on the subject who said he wasn't being very rigorous. On their blog, cybersecurity experts Kaspersky said the video wasn't made in good enough conditions to constitute proof. Why? Because the youtuber was broadcasting live- therefore sending the words he was saying directly to Google- which Google clearly used to send him targeted ads. So we can see from this that the algorithm for Google's targeted ads is very quick, that's clear, but it doesn't prove that the company is listening to us.

- Joe :

How can we prove it then?

- Chloé :

The Kaspersky experts did it: they placed a telephone in the middle of a table where several people were talking and purposefully dropped in the phrase "flood control system" several times. Nobody was searching this word online, neither before nor during the experience. And of course, there was no broadcasting on youtube at the same time. The result: Nothing. No ads for flood control systems.

- Joe :

And I see Facebook has also denied listening to its users' phone conversations.

- Chloé :

Yes, but what's interesting is to understand why. I've just read an article from 2017 in Wired, the American site specialised in digital. The author Antonio Garcia Martinez worked at Facebook at the time when the company was launching monetisation and targeted-ads. His first argument is that he says it's technically impossible. Permanently listening to the conversations of 150 million daily users- and that's only in the United States- would demand 33 times the data storage capacities of what's currently available. On top of that, it would slow our phones up enormously, so we would have already noticed.

- Joe :

But surely these companies dream of having the possibility to do that? Listening to all our conversations, finding out our deepest desires...

- Chloé :

Antonio Garcia Martinez is even less enthusiastic about that. He says that out of the enormous volume of text that would come from saving all our daily conversations, only a miniscule amount of it would be interesting. And to know that, he said they looked into it at Facebook… in a test they called the “Chorizo project”. They took all the data they had on users, and ran it through their targeting algorithm; all their posts, shares, links- and they realised that less than 10% had any value for the algorithm. So we often have this false idea that what we say is of any interest- the former Facebook employee says we are making a “narcissistic” error.

- Joe :

So in that case, how can we explain all these advertising coincidences?

- Chloé :

I read an article on the American news website Vox. The journalist reminds us that platforms like Facebook are capable of harvesting a lot of information from us, including information that we haven’t voluntarily submitted. This information mainly comes from other users. Do you remember when you signed up and Facebook asked you for permission to go into your address book to find potential contacts to add as friends? The information which has the most value is not what we like, nor where we are, or what we click on, but who we know. And if a friend buys something, someone about the same age as you… there’s a big chance you’re going to want the same thing.

- Joe :

And it’s the same on other platforms?

- Chloé :

Yes.. Tristan Harris, who we’ve already talked about in another of these podcasts, used to work at Google. At a talk he gave at Californian thinktank the Milken Institute, he recalled that Google had made “phantom profiles” of users. “It was a sort of voodoo doll,” he said. “I accumulated all your clicks and likes, which made this voodoo doll act more and more like you. All I had to do was to *simulate* the conversation that the voodoo doll could be having- I didn’t need to record you at all.

- Joe :

Really? But some of those mysterious ad stories are very difficult to unravel.

- Chloé :

There’s also an exercise the Reply All podcast team attempted at studio Gimlet in the United States. One woman said that her son had received troubling ads on his mobile. She was just telling him over the phone that her perfume had been taken from her at customs when she arrived at the San Francisco airport. He immediately received ads for a nearby perfumer on Facebook.

What was the explanation? Well, it started when she looked up her perfume online and the page probably contained a little tracker, known as a “Facebook Pixel” and which allows the social network to know what you do outside its pages. Then Facebook is capable, by clocking your location and your previous locations, to know where you will be in the following days- or even the very same day. So Facebook knew she was going to visit her son.. etc etc.

So we can’t prove that Facebook isn’t listening to our conversations.. but we’re sure they don’t actually need to.

- Joe :

But can other applications listen to my phone conversations?

- Chloé :

Well, yes. There’s a company called Alphonso that integrates into various mobile applications, including games. The New York Times revealed this two years ago. So Alphonso doesn’t actually listen to your conversations, but picks up certain signals from films in the cinema or on television- and that means it knows what you’ve watched. And that information is interesting to advertisers.

- Joe :

The other worrying subject at the moment are connected speakers- How easily we accept that they are always ready to work- that means of course that they’re permanently listening to us.

- Chloé :

Yes and no. Because the applications that make these speakers work only have the capacity to pick up the words they’re listening out for. That’s what former Facebook employee Antonio Garcia Martinez says anyway in his Wired article. As soon as they hear “Hello Alexa” or “Ok Google”, they start recording what you are saying. They script everything virtually and your question is then treated by the virtual assistant.

- Joe :

But we’ve also been hearing recently that connected speakers can be listened to by human beings..

- Chloé :

Yes, Belgian media VRT was able to get hold of some recorded sound from Google. Other publications also implicate Amazon and Microsoft in these practices. The recordings were listened to by humans- because an algorithm needs to be guided manually in order to learn. The task of these listeners was to say whether the machine was making a mistake or not. The journalists noted that on little more than a thousand recordings, 153 should not have been recorded, because the “OK Google” command hadn’t been said. They included things like professional conversations.. or even sexual situations..

- Joe :

How did the platforms react when they learned that?

- Chloé :

Right now you have the possibility to delete the recordings used by these platforms. Google announced on a blog in September that it wouldn’t save what you said to your Google home assistant by default anymore.

- Joe :

And just a little advice- you can easily see which applications on your telephone have access to your microphone- if you're still worried, feel free to withdraw their access! Thanks everyone for following this episode of the Memo, our second edition dedicated to exploring the issue of personal data. We'll return soon with a look into 5G! Until next time, goodbye.

Resources:

BBC : https://www.bbc.com/news/technology-41802282

Kaspersky : https://www.kaspersky.fr/blog/smartphones-eavesdropping/12070/

Wired : https://www.wired.com/story/facebooks-listening-smartphone-microphone/

Vox : https://www.vox.com/the-goods/2018/12/28/18158968/facebook-microphone-tapping-recording-instagram-ads

Milken institute : https://youtu.be/ueEaiZFwKto

Reply All : https://gimletmedia.com/shows/reply-all/z3hlwr/109-is-facebook-spying-on-you

New York Times : https://www.nytimes.com/2017/12/28/business/media/alphonso-app-tracking.html?_r=1

VRT News : https://www.vrt.be/vrtnws/en/2019/07/10/google-employees-are-eavesdropping-even-in-flemish-living-rooms/