Your headphones aren't spying on you, but your apps are

April 26 2017, by David Glance

Bose headphones. Credit: Bose Corp Media

Lawyers in the U.S. are claiming that headphone and speaker company Bose, is secretly collecting information about what users listen to when they use its bluetooth wireless headphones.

Edelson, the lawyers acting on behalf of customer Kyle Zak of Illinois, claim that information about what Zak has been listening to through his Bose headphones was being collected without his knowledge or explicit consent every time he used a Bose companion mobile app called Bose Connect. The app allows customers to interact with the headphones, updating software and also managing which device is connected at any time with the headphones. If the headphones are being used to listen to something, details about what is being played will show up in the Connect App.

This information is then collected by Bose and sent to third parties, including companies like Segment, who facilitate the collection of data from web and mobile applications and make it available for further analysis.

The lawyers are contending that Bose's actions amount to illegal wire tapping and that the information being collected could reveal a great deal of personal information about customers. Allegedly, Kyle Zak would not have bought Bose headphones if he had known that this information would be collected and he further claims that he never gave his consent for this information to be collected.

Bose has denied the allegations and pointed to the privacy policy in the Connect App that is explicit about the fact that it collects de-identified data for Bose's use only and does not sell identified data for any purpose

including "behavioral advertising". Bose also points out that what a customer listens to on the headphones is only visible to Bose if the customer is using the Connect App and has it open and running.

Given the app's limited functionality, it is really unclear why anyone would use the Connect App for this purpose on a continuous basis.

Most software uses tracking

The majority of apps installed on a phone will be collecting data about its usage and sending it back, de-identified, for analysis. This data may well be aggregated without giving any detail about any individual user. So, it would not be possible for example to say whether people who use an app every day are more likely to use particular features. Of course, some companies do collect this level of detail.

So what is this tracking data used for?

Developers use this information to track a range of things including statistics about usage of the app. Companies usually track how many daily and monthly active users they have and how many users stop using the app after opening for the first time.

Developers are also interested to find out if the app experiences problems, like crashes for example. They are also interested in what features of the app do customers use, what sequence did they use them and for how long.

A range of companies, including Apple and Google provide means of collecting anonymous statistics from users. The data is sent back to a server and made available for analysis. This type of tracking is very different from the tracking that is done for advertising purposes. In this case, information is collected that is identifiable and used to personalise

ads to be delivered either directly through the app, or through other services.

Hidden privacy statements are not enough

Privacy statements for apps, websites and other software should make it clear, and before the user starts using the app, what information the software is collecting, who it will be shared with, and for what purposes. Most software however, does not do this. Companies simply skip showing a user the privacy statement and make reference to the fact that the statement can be accessed somewhere on a website or in the app, at a later time.

Another problem with a great number of privacy policies, is that they are written in legal language and do not make explicit what information is being collected and for what purpose.

It is not only the companies that treat privacy as an afterthought. Customers also struggle with understanding the basics of their rights to privacy and what a privacy statement actually does. In 2014, Pew Research found that 52% of Americans surveyed wrongly believed that simply having a privacy policy at all meant that companies kept confidential all the information they collected on users.

In another survey, only 20% of users who read any part of a privacy policy felt they fully understood what they had read.

Ironically enough, the website of legal firm Edelson does not feature a clear link to its privacy policy. Its privacy statement is buried in a "Disclaimer" which helpfully says: "PLEASE READ THE FOLLOWING TERMS OF SERVICES & LEGAL NOTICES ("THIS AGREEMENT") CAREFULLY BEFORE USING THE EDELSON.COM WEBSITE". Somewhat hard to do if you have to visit

the site to get to it.

Privacy should be treated as a fundamental driver of design in software. This situation has been changing, especially as companies have focused on protecting customers' privacy, not from the companies themselves, but from law enforcement agencies, secret services and the government in general. Perhaps also, the threat of legal action by companies like Edelson, will prove another incentive to do the right thing.

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

Provided by The Conversation

Citation: Your headphones aren't spying on you, but your apps are (2017, April 26) retrieved 24 April 2024 from https://phys.org/news/2017-04-headphones-spying-apps.html