Bose Connect Privacy Evaluation

Prepared by: Brian Semrau on 4/20/2017

Edited on 4/21/2017 to fix a typo and a grammar error

Table of Contents

Introduction

On 4/18/2017, Kyle Zak filed a class action lawsuit against Bose Corporation, claiming that Bose was spying unsuspecting users through their Bose Connect app. As an owner of a set of Bose QC35 noise canceling headphones and a cyber security researcher, this case intrigued me. I love my Quiet Comfort headphones – they block out almost everything around you (and can be very useful for ignoring co-workers if necessary). I hadn't personally used the Bose Connect app prior to this, but as soon as I heard about the case, I downloaded it and checked it out. It was interesting… I changed my auto-powerdown setting to 1 hour (before they were set to stay on even when inactive – I had just been too lazy to download the app and change that setting prior to this), and then closed out the app. At no point during that time did the Bose Connect app ask for any PII (Personally Identifiable Information); however, I had already registered my headphones with Bose for the warranty, so it was possible that the app looked up the serial number and automatically tied it to me. Reading the case against Bose, I was furious. There were plenty of accusations, but neither in the case (or any article I could find about the case) was there any proof offered to support the claims. Because of this, I thought it was just someone looking to make a quick buck. As a security researcher and someone pursuing a career in Cyber Forensics, I felt that it was time to put these accusations to the test and run a very simple test to find out if my headphones were spying on me. While I had a bias in favor of Bose in this matter, as a researcher, I do my best to set my opinions aside and only look at the facts when I draw my conclusions The specific points that I sought to draw conclusions on were as follows:

- Does Bose Connect collect information on the end-user's listening habits and send said information to third parties as the lawsuit claims?
- Does Bose Connect send PII with the listening habit information?
- If Bose Connect is doing either of the above, does it collect user consent prior to doing so?

Process

One of the easiest ways to test whether or not a app, program, website, or any other such service running on a local device (such as a phone) is sending information to another party is to watch the network traffic. The best way to make sure you can see what type of information is flowing (even if it is encrypted) is to setup an interception proxy. PortSwigger Web Security makes a freemium interception proxy called Burp Suite. Within Burp, I can intercept and read all traffic – while some premium features such as saving my project data are disabled in the free version, I can still see all traffic that flows. In order to successfully have Burp intercept all traffic without raising any red flags to applications, I have to install Burp's root certificate as a trusted certificate authority on my device. This tells my device that Burp is authorized to respond for whatever server my device tries to send information to. Once this certificate is trusted on my device and I have configured my network settings to use my computer running Burp as a proxy server, all traffic going out of my device goes to Burp, which takes the traffic, and resends it to the real destination. Once the real destination responds, Burp relays that traffic back to my device. All traffic going through Burp is logged for my review.

Once I setup my device (a Samsung S7 Edge) with Burp, I tested it by visiting Google. Since Google uses HSTS (which tells browsers to *always* force a trusted and secure connection – even if the user tries to override it), my device would not allow me to connect if the browser believed that there was ***anything*** suspicious about the server it was connecting to. I connected right into Google and verified I could see all traffic from that visit in Burp. I then cleared all received data in order to prevent the possibility of that data being mistaken for data received during my test.

After verifying everything was working properly, I connected my headphones to my phone. No traffic flowed during this time. After that I opened the Bose Connect app. As soon as I did that, a number of traffic flowed between https://downloads.bose.com, https://bose-downloads.s3.amazonaws.com, https://e.crashlytics.com, and https://settings.crashlytics.com. Data was also sent to other URLs, but it did not contain any data, it seemed to only be a probe to see if the URL would respond with any data back, and none of those URLs did respond back.

Once I saw this data stopped flowing, I pressed the home key to return to my home screen, but still keep Bose Connect running in the background. I then started my Pandora app. A song was still in the cache from when I was listening to it earlier in the day, so I let that play for a few seconds then skipped forwarding by using the shortcut on my headphones. Of course I could see plenty of data flowing back and forth for Pandora, but the one site that caught my eye was https://api.segment.io. This was one of the data mining services that was mentioned in the lawsuit. Prior to seeing this, I had just assumed that if data had been collected by segment.io, it was because of either another service (such as a cloud music service) was sending it, or the user had spyware or other malware on their device that was sending the traffic to segment.io. Since I knew my device was free of malware and I wasn't aware that Pandora send data to segment.io, I felt that I needed to check this out. Sure enough, when I looked at the traffic, it was sending data to segment.io from the Bose app – and the data was regarding what I was listening to! I let my Pandora play for a while, turning the volume up and down from my headphones, skipping a track again, and then finally pausing the track. While I had originally planned to try multiple music services, I felt as if I had gathered enough data with just this one.

Once I determined I had collected the data that I needed, I turned off the proxy so no further traffic would be logged, I reconfigured my phone to stop sending traffic through the proxy, and removed the certificate that I installed for the proxy. I then continued to open the Bose app and read the privacy policy. I then reinstalled it from the Google Play store to see if I was prompted to accept the privacy policy when I first opened the app.

Data found

Upon inspecting the traffic from the URLs that the Bose Connect app communicated with, here is the information that was sent to each one:

https://settings.crashlytics.com:

- A request for the settings that crashlytics should use, included ways to identify the Bose Connect "account" with crashlytics.

https://e.crashlytics.com:

- Encrypted data that is most likely debugging information about app handling events.

https://downloads.bose.com:

- What looks like requests to know how to interact with the headphones

https://bose-downloads.s3.amazonaws.com:

- What looks like requests for what information to display

https://api.segment.io:

- What type of device it was (mobile, desktop, etc)
- App build versions
- App name (Bose Connect)
- What appears to be a way to identify what "account" to associate the data with
- An "anonymousId" (probably a unique ID to tie listening habits to a single person for analytics without revealing the PII)
- Information about the programming libraries it is using
- The timezone
- Screen resolution
- The android userAgent (Dalvik or Art – in this case Dalvik)
- The operating system version
- The specific hardware versions and builds
- The language settings
- A unique identifier for the phone
- Brand of phone
- Model of phone
- Name of phone build (in this case "hero2qlteatt")
- Whether or not the phone was on WiFi or Cellular (in this case WiFi)
- The carrier (even though I was on WiFi)
- Whether or not the network was over Bluetooth
- Whether or not the network was over Cellular
- What appears to be the amount of time I was listening to the headphones
- What appears to be the firmware version of the headphones

- What appears to be the serial number of the headphones
- What appears to be the product ID of the headphones
- Artist of media playing
- Album of media playing
- Title of media playing
- Timestamp
- Message sent timestamp
- Type of event (track changed, now playing, etc)

Here is a sample of one of the raw data packets:

```
POST /v1/import HTTP/1.1
Content-Type: application/json
Authorization: Basic MFRmaUpreHVBY3NCTGpXTFRRWjZkcW1VMmQycmZJdzc6
User-Agent: Dalvik/2.1.0 (Linux; U; Android 7.0; SAMSUNG-SM-G935A Build/NRD90M)
Host: api.segment.io
Connection: close
Content-Length: 3994
```

{"batch":[{"messageId":"e25b406f-e356-47da-82c3-
1bf68af85ed5","type":"screen","channel":"mobile","context":{"app":{"build":27,"name":"Bose
Connect","namespace":"com.bose.monet","version":"4.0.0"},"traits":{"anonymousId":"4673b852-00de-
405b-a62f-20bd0d324a7f"},"library":{"name":"analytics-
android","version":"3.4.0"},"os":{"name":"Android","version":"7.0"},"timezone":"America/Chicago","scr
een":{"density":3.0,"width":1080,"height":1920},"userAgent":"Dalvik/2.1.0 (Linux; U; Android 7.0;
SAMSUNG-SM-G935A Build/NRD90M)","locale":"en-
US","device":{"id":"4bcf7d38e03ba106","manufacturer":"samsung","model":"SAMSUNG-SM-
G935A","name":"hero2qlteatt"},"network":{"wifi":true,"carrier":"AT&T","bluetooth":false,"cellular":fals
e}},"anonymousId":"4673b852-00de-405b-a62f-20bd0d324a7f","timestamp":"2017-04-20T19:58:45-
0500","integrations":{"All":true},"category":null,"name":"Privacy
Policy","properties":{"Duration":163.702,"Product Id":"0x400C","Current Firmware
Version":"1.2.10","Serial Number":"072546Z63293816AE"}},{"messageId":"a9f42ea7-e062-42b8-8fcb-
3359b5ce7123","type":"track","channel":"mobile","context":{"app":{"build":27,"name":"Bose
Connect","namespace":"com.bose.monet","version":"4.0.0"},"traits":{"anonymousId":"4673b852-00de-
405b-a62f-20bd0d324a7f"},"library":{"name":"analytics-
android","version":"3.4.0"},"os":{"name":"Android","version":"7.0"},"timezone":"America/Chicago","scr
een":{"density":3.0,"width":1080,"height":1920},"userAgent":"Dalvik/2.1.0 (Linux; U; Android 7.0;
SAMSUNG-SM-G935A Build/NRD90M)","locale":"en-
US","device":{"id":"4bcf7d38e03ba106","manufacturer":"samsung","model":"SAMSUNG-SM-
G935A","name":"hero2qlteatt"},"network":{"wifi":true,"carrier":"AT&T","bluetooth":false,"cellular":fals
e}},"anonymousId":"4673b852-00de-405b-a62f-20bd0d324a7f","timestamp":"2017-04-20T19:58:45-
0500","integrations":{"All":true},"event":"Now Playing Event","properties":{"Event
Name":"Source","Event Value":"Primary"}},{"messageId":"1df0110e-a5a8-4f45-bd3f-
51e0ab3ee4f0","type":"track","channel":"mobile","context":{"app":{"build":27,"name":"Bose
Connect","namespace":"com.bose.monet","version":"4.0.0"},"traits":{"anonymousId":"4673b852-00de-
405b-a62f-20bd0d324a7f"},"library":{"name":"analytics-

```
android","version":"3.4.0"},"os":{"name":"Android","version":"7.0"},"timezone":"America/Chicago","scr
een":{"density":3.0,"width":1080,"height":1920},"userAgent":"Dalvik/2.1.0 (Linux; U; Android 7.0;
SAMSUNG-SM-G935A Build/NRD90M)","locale":"en-
US","device":{"id":"4bcf7d38e03ba106","manufacturer":"samsung","model":"SAMSUNG-SM-
G935A","name":"hero2qlteatt"},"network":{"wifi":true,"carrier":"AT&T","bluetooth":false,"cellular":fals
e}},"anonymousId":"4673b852-00de-405b-a62f-20bd0d324a7f","timestamp":"2017-04-20T19:58:45-
0500","integrations":{"All":true},"event":"Now Playing Event","properties":{"Event Name":"Track Info
Changed","Event Value":{"Artist":"Straight No Chaser","Album":"Six Pack EP","Song Title":"The Man
Who Can't Be Moved"}}},{"messageId":"57d5de70-030f-41b9-84c2-
ee366e3d1920","type":"screen","channel":"mobile","context":{"app":{"build":27,"name":"Bose
Connect","namespace":"com.bose.monet","version":"4.0.0"},"traits":{"anonymousId":"4673b852-00de-
405b-a62f-20bd0d324a7f"},"library":{"name":"analytics-
android","version":"3.4.0"},"os":{"name":"Android","version":"7.0"},"timezone":"America/Chicago","scr
een":{"density":3.0,"width":1080,"height":1920},"userAgent":"Dalvik/2.1.0 (Linux; U; Android 7.0;
SAMSUNG-SM-G935A Build/NRD90M)","locale":"en-
US","device":{"id":"4bcf7d38e03ba106","manufacturer":"samsung","model":"SAMSUNG-SM-
G935A","name":"hero2qlteatt"},"network":{"wifi":true,"carrier":"AT&T","bluetooth":false,"cellular":fals
e}},"anonymousId":"4673b852-00de-405b-a62f-20bd0d324a7f","timestamp":"2017-04-20T19:59:03-
0500","integrations":{"All":true},"category":null,"name":"Device
Connected","properties":{"Duration":18.019,"Product Id":"0x400C","Current Firmware
Version":"1.2.10","Serial Number":"072546Z63293816AE"}}],"sentAt":"2017-04-20T19:59:07-0500"}
```

When I looked at the privacy policy for Bose, I noticed that it stated (paraphrased) that they will collect non-identifying information about you and send it back to their systems as well as third parties including crashlytics and segment.io. It also stated that in order to use the app, you agreed to these terms and conditions. When you install the Bose App (at least on Android), the first thing it does when you open it is ask for the permissions that it requires to work. It does not mention anything about the privacy policy. I accepted these permissions and moved on. By this time, I had already turned off my headphones, so it prompted me to reconnect them. I turned them on and it automatically detected them. It did not ask me to accept the privacy policy, and automatically opened to the screen where it showed what song I had last been playing. I checked the Google Play store; and it does not show the privacy policy for the app on the Play store, nor does it prompt you to accept when you download the app.

Conclusion

Based on the transmitted data that I found, I now believe there is much more to this lawsuit than I originally thought. As stated before, I sought out to find data on 3 points:

- Does Bose Connect collect information on the end-user's listening habits and send said information to third parties as the lawsuit claims?
- Does Bose Connect send PII with the listening habit information?
- If Bose Connect is doing either of the above, does it collect user consent prior to doing so?

Based on the data that I found, I do believe that the end-user's listening habits are logged and sent to a third party data mining service; however, I do not believe that any information is sent to this third party data mining service that could directly link the listening habits (identified by a unique but anonymous identifier) to an actual person. That being said, if this data mining service was able to use other data collected from other apps or services to link the Quiet Comfort serial number or other identifying numbers surrounding the phone to an actual person, they could then link all of the previously documented listening habits to that person.

Had the users been prompted to review the privacy policy and accept it prior to using the app, then I believe Bose would have every right to use the data in this way. I am a firm believer that users need to be more careful about EULAs and privacy policies that most blindly accept. The main issue that I see with this data collection is that the user is never prompted to accept the policy, instead, if they want to see what data is collected, they have to hunt within the app to find it. They are not aware that this data is being sent before it already has. Yes – it's a condition of using the app to accept the privacy policy, but how are the users supposed to know that if they aren't told that prior to using the app?

All in all, I believe that while this issue that is coming to light ***is*** concerning and needs to be fixed, I do not believe that it would have stopped me from purchasing my headphones if I had known about this issue ahead of time. As I said before, prior to this controversy piquing my curiosity, I hadn't even downloaded the app much less used it. Now that I've set my "idle" timer on the headphones, and finished running my tests I will be uninstalling the app and will continue to happily use my headphones as I did before.

Follow up

This report was prepared by an independent security researcher: Brian Semrau. For any questions or follow up comments, please contact brian@bscc.support.

For anyone wishing to verify the data, traffic that was intercepted and related to the Bose Connect app (Pandora traffic is not included for security reasons) during this test can be downloaded from:

https://bscc.support/files/bc_privacy/bose_connect_captures.zip

(Please note that the traffic received is formatted in a XML file. This still contains all of the information from each of these sites – including sites that were excluded from the report above due to my belief that they did not hold any relevance. The only sites that have been excluded are those that I was able to verify did not originate from the Bose Connect app.)