IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

KYLE ZAK, individually and on behalf of all others similarly situated, *Plaintiff*, v. BOSE CORP., a Delaware corporation, *Defendant.*	Case No. 17-cv-2928 Assigned Judge: Andrea R. Wood

MEMORANDUM OF LAW IN SUPPORT OF MOTION TO DISMISS SECOND AMENDED CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes and Rules

Legislative Materials

INTRODUCTION

The third time is not the charm. Even on his third effort, Plaintiff's case is still not about wiretapping or eavesdropping. His gripe with Bose is that when he ***knowingly and deliberately installed, opened, and used the Bose Connect App with streaming music services***, Bose collected the track information conspicuously displayed on the app. The parties dispute whether that collection was adequately disclosed. But inadequate disclosure—and not illegal interception—has always been the nature of Plaintiff's claim, which is why the Court properly dismissed his Wiretap and Eavesdropping Act claims. Rather than proceed with his surviving claims (which albeit unfounded, at least reflect his actual grievance), Plaintiff filed a third complaint attempting to resuscitate his dismissed claims. His motivations are transparent—the Wiretap Act authorizes hefty statutory damages, while his remaining claims do not. But stripped of implausible conclusory assertions and arguments for which Plaintiff provides no factual support, the events described in his latest complaint still do not—and cannot—amount to Wiretap and Eavesdropping Act violations. If they did, any app that captures usage data would be subject to Wiretap Act claims so long as the information captured also travels via the Internet. This is not the law.

Plaintiff's Wiretap Act claim must be dismissed for several reasons. Principally, his latest complaint fails to cure the deficiencies that previously led the Court to dismiss that claim. Indeed, while this complaint makes a handful of cosmetic changes and imports legal arguments already presented in his opposition to Bose's previous motion to dismiss, his description of what happened still "make[s] clear that the App is a fully-acknowledged participant in the communication of the Media Information—indeed, receiving and displaying the Media Information is a primary function of the App." Order at 6. Tellingly, there continues to be no allegation that Bose received song title information when Plaintiff was not using Bose Connect—rather, the allegations are that he first

had to connect his Bose headphones and deliberately open the Bose Connect App, which would then conspicuously display audio track information and music controls on his screen. As the Court already recognized, there can be no Wiretap Act violation under such circumstances.

Plaintiff's Wiretap Act claim fails for two additional reasons. ***First***, a cognizable intercept requires the acquisition of a communication transferred by a "system that affects interstate or foreign commerce." *See* 18 U.S.C. § 2510(12). Plaintiff's own allegations—and the generally understood operation of iPhones—make clear that any alleged interception was of Bluetooth communications between the App and his headphones. Such purely local communications are not sent over a system affecting interstate commerce, and thus cannot form the basis for a Wiretap Act claim. The fact that information was separately sent from his iPhone to Spotify over the Internet does not change this. ***Second***, the allegedly intercepted material—audio track information—is not content under the Wiretap Act because it is not Plaintiff's intended message to another. If it were the content of the communication it would be the song itself—music and lyrics. But Plaintiff alleges only that the App collects record information each time he presses the track forward or backward button. This demonstrates that what is occurring is not an interception of a communication, but rather the logging of one.

Plaintiff's attempt to resuscitate his Eavesdropping Act similarly fails. That claim is based on the same alleged conduct, and was dismissed for the same reason, as his Wiretap Act claim. His newest complaint is equally deficient in this regard. And as is plain to see, any capture of information by Bose was not surreptitious as required under the Eavesdropping Act—the App's conspicuous operation, and the displays on Bose's website, clearly show that it receives audio track information. As Plaintiff's latest attempt still fails to allege cognizable Wiretap and Eavesdropping Act claims, these claims should once again be dismissed—this time with prejudice.

BACKGROUND

A. The Bose Connect App

Bose is a Delaware corporation headquartered in Framingham, Massachusetts. Second Amended Complaint ("SAC"), ECF No. 75, ¶ 9. Bose designs, manufacturers, and sells audio equipment, including headphones and speakers. *Id.* ¶ 1. This includes wireless headphones and speakers that can be used with smartphones or similar Bluetooth-enabled devices. *Id.* ¶ 13.

Like countless technology companies, Bose offers a smartphone application that can be used with certain Bose wireless products. *Id.* ¶¶ 13-15. This App, called "Bose Connect," is a companion app that users of compatible products have the option to download and install on their smartphones.[1] The App offers several features. Users can use it to simplify "connecting and switching between devices," adjust the settings on their wireless device, and download firmware updates from Bose. *Id.* ¶ 15. The App also allows users to share audio between two adjacent Bose wireless devices.[2] These features (not to mention the App's name) make clear that Bose created the App to "connect" a user's smartphone to his or her headphones or speakers—allowing the two

---

[1] *See Bose Connect on the App Store* (Feb. 6, 2017, 2:24 PM), http://web.archive.org/web/20170206142401/https://itunes.apple.com/us/app/bose-connect/id1046510029?mt=8. On a motion to dismiss, a court can consider documents that are attached to the complaint, documents that are central to the complaint and are referred to in it, and information that is properly subject to judicial notice. *Williamson v. Curran*, 714 F.3d 432, 436 (7th Cir. 2013); *see also Swartz v. KPMG LLP*, 476 F.3d 756, 763 (9th Cir. 2007) (judicial notice is appropriate "to prevent plaintiffs from surviving a Rule 12(b)(6) motion by deliberately omitting documents upon which their claims are based") (internal quotation marks omitted). Here, the Complaint repeatedly excerpts and cites to Bose's website and the Bose Connect App, as well as to the Bose Connect page in the Apple App Store and Segment's website. *See, e.g.*, SAC ¶¶ 14, 15, 20, 21, 23, 27. To reflect relevant sources as they existed at the time this action was filed, Bose cites to archived versions preserved by the non-profit Internet Archive where appropriate. *See Erickson v. Neb. Mach. Co.*, No. 15-CV-01147-JD, 2015 WL 4089849, at *1 n.1 (N.D. Cal. July 6, 2015) (collecting authorities taking "judicial notice of the contents of web pages available through the Wayback Machine as facts that can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned"); *Hepp v. Ultra Green Energy Servs., LLC*, No. 13-C-4692, 2016 WL 1073070, at *2 (N.D. Ill. Mar. 18, 2016) (taking judicial notice of archived website from Wayback Machine, citing *Erickson*).

[2] *See QC35 Wireless Noise Cancelling Headphones*, Bose (Apr. 9, 2017, 6:29 AM), http://web.archive.org/web/20170409062938/https://www.bose.com/en_us/products/headphones/over_ear_headphones/quietcomfort-35-wireless.html.

devices to communicate with each other, and to exchange relevant information with Bose.

The App also offers an alternate method to remotely control the playback of music being received by a compatible Bose wireless device from the user's smartphone—displaying basic information about the currently playing track (such as artist and song name) and providing an interface to pause, resume, skip tracks, and so on. *Id.* ¶¶ 16, 27. These same controls are also available via buttons on Bose headphones and, of course, through the relevant music app on the device itself. *See id.* ¶ 16, 20. The Complaint does not allege that the Bose Connect App has any functionality, including remote control, when not connected to compatible Bose headphones.

Bose Connect's privacy policy, available through the App, disclosed Bose's collection and transmission of information from the App and the purposes of that collection. The policy stated that Bose and "its service providers may automatically receive and record certain information from your mobile phone," "gather information about [your device's] online activity," and "partner with third parties" to "track and analyze how you use the app . . . during your current session and over time." The policy also disclosed that this collection would be accomplished both through "storing small files on your mobile phone" and "transmission of information to a third-party server."[3]

B. iOS, Apps and Bluetooth Accessories

Plaintiff alleges he downloaded the App from the Apple App Store, indicating that his device is an iPhone. *See* SAC ¶ 39-40. He alleges that he then used the App when listening "to streaming music and audio from various third-party sources, with the audio playing through his Bose wireless headphones." *Id.* ¶ 41. The SAC does not allege that either the App or the Bose headphones access the stream of communications (i.e., the music) sent between the streaming music provider and Plaintiff's iPhone. Rather, it alleges that the App's receipt of song titles is the

[3] *See* Declaration of Jeffrey Landis, dated May 30, 2019 ("Landis Decl."), Ex. 1.

last in a series of discrete steps—"the user's mobile device receives the requested audio materials, and then routes the information to the headphones and the Bose Connect app, where the information about the audio file is then displayed to the user." *Id.* ¶ 27.

This multi-step process described in the SAC accords with the basic technical facts of how iPhone apps and Bluetooth headphones work. Apple maintains public technical documentation for the iPhone's operating system, called iOS, that developers use to create compatible apps. Bluetooth is a technical communications standard, defined through formal "specifications . . . that developers use to create the interoperable devices that make up the thriving Bluetooth ecosystem."[4]

Apple's iOS security documentation explains that:

> All third-party apps are "sandboxed," so they are restricted from accessing files stored by other apps or from making changes to the device. This prevents apps from gathering or modifying information stored by other apps. . . . If a third-party app needs to access information other than its own, it does so only by using services explicitly provided by iOS. System files and resources are also shielded from the user's apps.[5]

In other words, iOS does not allow any third-party app to see or control what another app is doing (e.g., requesting or receiving music from Spotify). iOS does, however, provide a specific service (the "iOS Media Player Framework") through which music player apps can provide song

---

[4] *Specifications*, Bluetooth Technology Website, https://www.bluetooth.com/specifications (last visited May 29, 2019). On a motion to dismiss, a court can take judicial notice of facts that "can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." Fed. R. Evid. 201(b)(2). Apple's technical documentation concerning its own iOS operating system and formal specifications defining the Bluetooth standard both fall within that category, and courts can and do take notice of such materials. *See, e.g.*, *Opperman v. Path, Inc.*, 84 F. Supp. 3d 962, 976 (N.D. Cal. 2015) (taking judicial notice of Apple's "iOS Human Interface Guidelines" and "App Store Approval Process instructions," among other materials); *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1101 n.2 (9th Cir. 2014) (taking judicial notice of current version of publicly-available hypertext transfer protocol (HTTP) specification, RFC 2616); *Sekisui Am. Corp. v. Hart*, 15 F. Supp. 3d 359, 366 n.59 (S.D.N.Y. 2014) (taking judicial notice of publicly-available ISO standards); *Cruz v. Anheuser-Busch, LLC*, No. CV 14-09670 AB (ASX), 2015 WL 3561536, at *8 n.13 (C.D. Cal. June 3, 2015), *aff'd*, 682 Fed. Appx. 583 (9th Cir. 2017) (taking judicial notice of product specifications readily available on manufacturer's website).

[5] *See* Landis Decl. Ex. 2, Apple, iOS Security White Paper (March 2017), at 20.

information *to the operating system*, which can then use that information in various ways such as displaying it on a phone's lock screen or sending it to a connected Bluetooth device.[6]

By definition, Bluetooth-compatible headphones are those that adhere to applicable specifications under the Bluetooth communications standard. Since at least 2003, the Bluetooth specifications have set out standardized formats (called profiles) for sending and receiving information between a smartphone and accessory.[7] For audio signals, the profile is called "A2DP" (Advanced Audio Distribution Profile).[8] For media information and remote control instructions (play, pause, fast forward, etc.), the profile is called "AVRCP" (Audio/Video Remote Control Profile).[9] iPhones comply with these standards and use the AVRCP profile to send song information (artist, album, and song title, etc.) from the phone to connected Bluetooth devices.[10]

Third-party apps like Bose Connect cannot access media information from media apps or the device itself, but iOS provides a protocol for such apps to communicate directly with compatible wireless devices.[11] Bluetooth device makers like Bose use these protocols to create

---

[6] *See* Apple, Bluetooth Accessory Design Guidelines for Apple Products (Release R7) ("Apple Bluetooth Guidelines"), § 2.2.4.7 (as of Jun. 12, 2017, 8:34PM), http://web.archive.org/web/20170612203416/https://developer.apple.com/hardwaredrivers/BluetoothDesignGuidelines.pdf ("An audio app running on an iOS device may use the iOS MediaPlayer Framework APIs to provide metadata about the current audio stream. The iOS device supplies this metadata to the accessory using AVRCP.").

[7] *See* Bluetooth SIG, Archived Specifications, *available at* https://www.bluetooth.com/specifications/archived-specifications/ (listing historical versions of A2DP/AVRCP specifications dating back to 2003).

[8] *See* Bluetooth SIG, Advanced Audio Distribution Profile (A2DP) Specification v1.3.1 (Jul. 14, 2015), *available at* https://www.bluetooth.com/specifications/archived-specifications/ (current version at time of initial complaint filing); Apple Bluetooth Guidelines § 2.2.5 (stating "[e]very accessory that is compatible with an Apple product and supports [A2DP] should meet the requirements of the [A2DP] specification").

[9] *See* Bluetooth SIG, Audio/Video Remote Control Profile v1.6.1 (Dec. 12, 2015), *available at* https://www.bluetooth.com/specifications/archived-specifications/ (current version as of initial complaint).

[10] *See* Landis Decl. Ex. 2 at 32 (listing Bluetooth profiles supported by iOS); Apple Bluetooth Guidelines § 2.2.4 (describing required implementation of AVRCP specification).

[11] There are two frameworks in iOS for third-party apps to create a separate communications channel to talk to Bluetooth devices. *See About External Accessories*, Apple Developer Guides and Sample Code, https://developer.apple.com/library/content/featuredarticles/ExternalAccessoryPT/Introduction/Introduction.html (last updated Feb. 24, 2012) (describing the iOS External Accessory Framework, "a conduit for communicating with accessories attached to any iOS-based device"); *Core Bluetooth Framework*, Apple

custom iPhone apps that communicate with their devices over a separate, secure channel—i.e., apps like Bose Connect "talk" directly to the headphones. The SAC does not allege otherwise.

C. The First Two Complaints and the Court Order

Plaintiff filed his first complaint on April 18, 2017 ("Original Complaint"). ECF No. 1. It alleged simply that Bose Connect collected communications sent from users' smartphones to their wireless devices and was brought on behalf of all users of the App. *Id.* ¶¶ 19, 33. Bose moved to dismiss the Original Complaint on various grounds, including that the alleged interception of communications between Plaintiff's phone and Bose headphones via Bluetooth failed to satisfy the Wiretap Act's interstate commerce requirement; and that either Bose was a party to such communication or there was no second party. *See* ECF No. 20. Rather than oppose that motion, Plaintiff filed a second complaint ("FAC"). ECF No. 24. The FAC sought to recast the allegedly intercepted communications as ones between users and third-party streaming providers, and limited the putative class to only individuals that used the App to remotely control a streaming music app. *Id.* ¶¶ 40, 43. Bose moved to dismiss the FAC on the same grounds. *See* ECF No. 28.

On March 31, 2019, the Court granted in part and denied in part Bose's motion to dismiss the FAC. *See* ECF No. 70 (the "Order"). The Court dismissed Plaintiff's Wiretap Act claim on the ground that he failed to allege facts suggesting Bose is not a party to the relevant communication. *Id.* at 6. In doing so, the Court disregarded his "conclusory allegations" to the contrary and looked at the actual facts alleged: that the App accesses and displays media information from the user's device; that the App functions by displaying media information; and that the App sends a request for a song and processes the music provider's provision of song information in return. *Id.* "These allegations make clear that the App is a fully-acknowledged participant in the communication of

---

Developer Documentation (as of Jun. 6, 2017, 8:01 AM), http://web.archive.org/web/20170606080133/https://developer.apple.com/documentation/corebluetooth (describing the Core Bluetooth framework).

the Media Information—indeed receiving and displaying the Media Information is a primary function of the App." *Id.* The Court, however, offered Plaintiff the opportunity to "allege a set of ***facts*** to suggest that Bose is in fact not a party to the communication." *Id.* at 8 (emphasis added).[12]

D. Plaintiff's Third Attempt to Plead a Wiretap Act Claim

Plaintiff subsequently filed the SAC—his third complaint in this matter—in an attempt to cure the deficiencies identified by the Court in the Order. The SAC does not add any new factual allegations suggesting Bose is not a party to any allegedly intercepted communication. Instead, it merely swaps out " interception" and "transmission" for "redirection" at various places, repeats arguments included in his previous complaint and motion to dismiss opposition, and rephrases selected language that the Court cited in the Order without changing its meaning.

ARGUMENT

"To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). Facial plausibility requires factual allegations sufficient to "draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id*. Labels, conclusions and "formulaic recitation[s]" will not suffice. *Twombly*, 550 U.S. at 555. Broad, conclusory legal allegations masked as fact are likewise insufficient. *Adams v. City of Indianapolis*, 742 F.3d 720, 733 (7th Cir. 2014). Courts also need not give effect to conclusory allegations that are contradicted by actual descriptions of what happened. Order at 6 (citing *McCauley v. City of Chicago*, 671 F.3d 611, 617-18 (7th Cir. 2011)).

[12] The Court dismissed Plaintiff's Illinois Eavesdropping Act claim on the same ground as it dismissed his Wiretap Act claim. *Id.* at 11 ("[The] Illinois Eavesdropping Statute claim fails for the same reason the federal Wiretap Act claim fails."). The Court found that Plaintiff pleaded an Illinois Consumer Fraud Act claim sufficient to survive the motion to dismiss stage (*Id.* at 12-14), and allowed his unjust enrichment claim to proceed noting that it "will stand and fall with the [Illinois Consumer Fraud Act] claim." *Id.* at 15.

I. Plaintiff's Wiretap Act Claim Should Be Dismissed

Plaintiff fails to state a Wiretap Act claim for multiple reasons—all stemming from the fact that, even after three attempts, this is simply not a Wiretap Act case. Rather, Plaintiff's "real issue is with the fact that Bose allegedly collects and discloses the Media Information that it legitimately receives." Order at 7. This falls outside the purview of the Wiretap Act. *Id.*

The current iteration of the Wiretap Act, 18 U.S.C. § 2510 *et seq.*, was designed to "protect against the unauthorized interception of electronic communications." *Ameritech Corp. v. McCann*, 297 F.3d 582, 583 (7th Cir. 2002) (quoting S. Rep. No. 99-541, *reprinted at* 1986 U.S.C.C.A.N. 3555). The Act prohibits "intentionally intercept[ing] [or] endeavor[ing] to intercept . . . any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). The Act includes certain statutory exceptions to its prohibitions. *See, e.g.*, *id.* § 2511(1)(d)-(i). The only conduct plausibly alleged in the Complaint—that the App receives and collects audio track information when connected to Bose wireless devices via Bluetooth—is not prohibited under the Act.

A. The Complaint Does Not Cure the Deficiencies That Previously Caused the Court to Dismiss Plaintiff's Wiretap Act Claim

Plaintiff's Wiretap Act claim fails first because his latest complaint does not allege new or different facts "to suggest that Bose is in fact not a party to the communication." Order at 8. The changes made in the SAC are limited and superficial, consisting of rehashed explanations of old allegations and legal arguments imported from Plaintiff's previous motion to dismiss opposition—both of which the Court has already considered. None of those changes cure the deficiencies that led the Court to dismiss the Wiretap Act claim, and the SAC's Wiretap Act claim should be dismissed for the same reasons stated in the Order.

In an effort to end-run the Order, the SAC rephrases certain allegations without substantively changing any underlying alleged facts. For instance, the Order quoted the FAC's

allegation that the App "accesses and displays" Media Information as a core function. *See id.* at 6, quoting FAC ¶ 26. The corresponding paragraph of the SAC removes the word "accesses," alleging instead that Media Information "is then displayed to the user" on the App. SAC ¶ 27. Similarly, the Order noted the FAC's allegation that the App "sends a user's request for a particular song." *See* Order at 6, quoting FAC ¶ 26. The SAC now alleges the App "causes the user's mobile device to send" a request for a particular song. SAC ¶ 27. Neither of these wording changes affect the Court's conclusion that the App was a known and intended recipient of the communications. Moreover, other allegations undergirding the Order remain unaltered. For example, the SAC still "includes a screenshot of the App functioning on the user's mobile device by displaying the Media Information." Order at 6; SAC ¶ 27. Likewise, the SAC still alleges that the App "processes . . . the music provider's provision of song information in return." *Id.* ¶ 32. And the SAC's bulleted explanation of how the App functions "when used to access and control remote streaming media" merely restates in more words the same description included in the prior complaint. *Compare* SAC ¶ 27 *with* FAC ¶ 26. Such window dressing cannot resurrect Plaintiff's failed claims.

The SAC still "make[s] clear that the App is a fully-acknowledged participant in the communication of the Media Information—indeed [that] receiving and displaying the Media Information is a primary function of the App." Order at 6. However, "a party to the communication" is allowed to intercept an electronic communication. 18 U.S.C. § 2511(2)(d). Because that is the case here, even if interception were adequately alleged, there can be no Wiretap Act violation—as the Court has already recognized. *See* Order at 5-8.[13]

[13] *See also United States. v. Eady*, 648 Fed. Appx. 188, 191 (3d Cir. 2016) ("[A] 'party' is a participant whose presence is known to the other parties contemporaneously with the communication."); *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001) ("Amazon merely received the information transferred to it . . . , an act without which there would be no transfer. Amazon acted as no more than the second party to a communication. This is not an interception as defined by the Wiretap Act.").

Plaintiff's speculation that the App could have been designed differently to exclude Bose as a party to the communication is of no moment. *See* SAC ¶ 28. In *In re Google Inc. Cookie Placement*, plaintiffs alleged that defendant internet advertisers placed cookies on their computers in the process of injecting advertisements, which would "intercept" plaintiffs' communications and transmit their web browsing history back to defendants. 806 F.3d 125, 131 (3d Cir. 2015). As alleged here, the cookies were not necessary to serve the ads, and defendants could have designed their ad injection mechanism differently to not track or profile users. *Id.* The Third Circuit nonetheless affirmed dismissal of the Wiretap Act claim, finding that "[a]s the intended recipient of a communication is necessarily one of its parties, and the defendants were the intended recipients of the GET requests they acquired here, the defendants were parties to the transmissions at issue." *Id.* at 140-141, 143 (rejecting plaintiffs' allegations as implausible and at odds with a "common sense reading" of the complaint's factual allegations). So here too—Bose, as the intended recipient of the Media Information from Bose Connect, is a party to that communication.

Plaintiff's alleged lack of knowledge that Bose collected track information transmitted to the Bose Connect App from his headphones is equally irrelevant. As an initial matter, the App's Privacy Policy clearly disclosed that Bose (and its service providers) collected and transmitted information from the App when it was in use. Landis Decl., Ex. 1 at 1. By definition then, Bose was a party to all communications sent to or through the App. The Complaint also admits that audio track information is displayed prominently on the App as part of its functionality, the name of the App is "Bose Connect," and the App routinely connects to Bose for purposes such as downloading and installing firmware updates. *See* SAC ¶ 15. But even if that were not the case, Plaintiff's claim goes to the adequacy of disclosure—it does not transform it into a Wiretap Act violation, as it does not change the fact that Bose is a party to the communication. Order at 5 ("A

defendant is a 'party' to the communication within the meaning of the Wiretap Act when the defendant is a participant, even if the defendant was not an *intended* participant . . . .").

Plaintiff's allegations are like those of a website visitor claiming she did not know about her web browser's communications with an embedded third-party tracking server. That lack of awareness does not give rise to a Wiretap Act claim. *See In re Google Cookie Placement*, 806 F.3d at 143 ("[B]y design[,] there is no statutory language by which the defendants' various alleged deceits would vitiate their claims to be parties to the relevant communications."); *Allen v. Quicken Loans Inc.*, No. 17-12352, 2018 WL 5874088, at *4 (D.N.J. Nov. 9, 2018) (fact that "extreme supermajority" of users were unaware of alleged interception was "irrelevant" to evaluating whether defendant was party to communication). Similarly, where Media Information was being sent to Bose as part of Plaintiff's deliberate use of Bose Connect to view that information, Bose was a party to that communication. "Interception connotes a situation in which by surreptitious means a third party overhears a telephone conversation between two parties." *United States v. Pasha*, 332 F.2d 193, 198 (7th Cir. 1964). That is not what Plaintiff's allegations describe.[14]

Plaintiff attempts to save his Wiretap Act claim by repackaging his prior argument that Bose Connect is equivalent to Microsoft Outlook or the iPhone dialer app. *Compare* SAC ¶ 28 *with* FAC ¶ 29. But these statements are mere legal arguments supporting his view that Bose is not a party to any communication—and as such, should be disregarded by the Court. *McCauley*, 671 F.3d at 617-18 ("[A]lleged 'facts' [that] are actually legal conclusions . . . may be disregarded on a motion to dismiss . . . [as they] contribute nothing to the plausibility analysis.") Further, the Court

[14] If Bose is not a party to the communication that the SAC actually describes being intercepted, there is no second party—Plaintiff is simply communicating with himself, much as he may use a remote control to communicate with a TV in the same room, or an app to fly a drone. No court has found a Wiretap Act violation under such circumstances. *See, e.g.*, *Ropp*, 347 F. Supp. 2d at 835 (dismissing Wiretap Act indictment where government's theory was that "when [the user] enters data through her keyboard, she is communicating with her own computer").

already considered these arguments and found them insufficient.[15] That is because unlike Outlook and the iPhone dialer—which both serve as communication channels between the user and a third party—Bose Connect is not a communication channel between Plaintiff and any party except Bose. The Complaint asserts that streaming music providers are the other party to any communication (*see* SAC ¶¶ 32, 56), but that statement is a conclusory misidentification of the communication allegedly being intercepted. *See* Order at 6. That assertion is also rendered implausible by the basic facts of how iPhones work. (*See infra* I.B.1.) While streaming music providers may communicate with Plaintiff's device, Bose Connect has no access to ***that*** communication, as opposed to the subsequent local communication between his Bose headphones and the App. The SAC admits as much, explaining that only after "the user's mobile device receives the requested audio materials" does it "route[] the information to the headphones." SAC ¶ 27.

B. The SAC Still Does Not Allege an Acquisition Over a System that Affects Interstate Commerce

Plaintiff's Wiretap Act claim independently fails because he does not allege an interception of a communication in interstate commerce. The only plausible reading of the ***facts*** in the SAC is that the relevant "communications"—*i.e.*, the transmission of song information to the App—was over Bluetooth between the App and Plaintiff's headphones. Such short-distance, local transmissions cannot form the basis of a Wiretap Act claim.[16] The Act defines "intercept" as the acquisition of contents of any "electronic communication" through the use of certain devices. 18

[15] Similarly, Plaintiff's allegations that the App added "hidden [collection] functionality in the app's code" (SAC ¶ 29) are not only irrelevant for the same reasons, but they are also not new—they are imported from his prior opposition brief already considered and rejected by the Court. *See* ECF No. 34 at 6.

[16] *See, e.g., Using a Bluetooth Mouse, Keyboard, or Trackpad*, Apple Support, https://support.apple.com/en-us/HT201171 (last visited May 28, 2019) ("Bluetooth is a wireless technology that makes short-range connections . . . at distances up to 10 meters."). Courts may take judicial notice of well-established scientific facts that are generally accepted as irrefutable. *See Golaris v. Jewel Tea Co.*, 22 F.R.D. 16, 20 (N.D. Ill. 1958).

U.S.C. § 2510(4). Electronic communication is defined as "any transfer of signs, signals, [etc.] . . . transmitted in whole or in part by a . . . ***system that affects interstate or foreign commerce***." *Id.* § 2510(12) (emphasis added). Thus, "an electronic communication within the purview of the statute must be transmitted by a system that affects interstate or foreign commerce." *Rene v. G.F. Fishers, Inc.*, 817 F. Supp. 2d 1090, 1093 (S.D. Ind. 2011).

1. The SAC Alleges the Bose Connect App Collected Information Over a Local Bluetooth Connection

The SAC does not allege facts suggesting any interception of an electronic communication being transmitted by a system that affects interstate commerce. Plaintiff ***argues*** that Bose captured communications between his iPhone and streaming music services over the Internet. *See* SAC ¶¶ 25, 56. If that were true, the factual allegation would state that Bose captured the music and lyrics sent from the streaming service. But that is neither what happened nor what is alleged. The SAC's ***factual allegations*** show that any collection occurred during a purely local Bluetooth communication between Plaintiff's headphones and the App. Specifically, the SAC describes "three general steps" when Bose Connect is used with a streaming audio provider:

- "First, a user presses the track forward button in the Bose Connect app when listening to streaming audio, ***which causes the user's mobile device to send a request to a remote audio provider***, like Spotify, for specific audio content (e.g., 'Please send me the next song in my playlist.')."
- "Second, upon receipt of that communication, ***the remote audio provider communicates the requested audio content***—including information about the requested audio content, such as the specific song name, artist, and album—***back to the user's mobile device***."
- "Third, the user's mobile device receives the requested audio materials, ***and then routes the information to the headphones and the Bose Connect app***, where the information about the audio file is then displayed to the user."

SAC ¶ 27 (emphasis added). Plaintiff's own allegations describe communications with streaming audio providers as coming from, and going to, ***the user's device,*** with the Bose Connect App only receiving information ***afterward*** through its direct local connection to paired Bose headphones.

This description accords with how iPhones work with third-party apps and Bluetooth devices, as set forth in the formal documentation describing how those technologies operate. Music apps can send information about currently playing audio tracks to the iPhone's operating system, which sends it to connected Bluetooth accessories via the AVRCP profile. Bluetooth accessories use the same channel to send music control commands back to the iPhone (using, for instance, hardware buttons like those found on Plaintiff's Bose headphones). *See* SAC ¶ 20. iOS does not allow third-party apps like Bose Connect to directly access any of this information. Such an app can only interact with a compatible Bluetooth device (and access information from it) using a separate transmission protocol provided by Apple. The only plausible reading of the Complaint's factual allegations is that the App receives Media Information exclusively through its direct local connection to paired Bose headphones. The SAC, though perhaps unintentionally, admits as much.

And while the headphones received Media Information in the first instance from the iPhone's operating system (via the AVRCP profile), the Bluetooth communication between the headphones and the App is a distinct one—entirely separate from any internet communication between a streaming music provider and the music app. *See In re Facebook Internet Tracking Litig.*, 263 F. Supp. 3d 836, 844 (N.D. Cal. 2017) (fact that computer application sends the same information to two separate parties "does not establish that one party intercepted the user's communication with the other").[17] The fact that pushing the "next track" button in some cases may initiate a separate command in the Spotify app does not transform the local Bluetooth

[17]Another cosmetic change in the SAC was to swap the word "redirect" (or "redirection") for "transmit" or "intercept" in various places. *E.g.*, *compare* SAC ¶¶ 25, 26, 28 *with* FAC ¶¶ 25, 26, 32. But the SAC does not identify or explain what "redirection" occurred. The Court is no more required to accept as true the "redirection" label as it was to accept the "interception" label. *See Adams*, 742 F.3d at 733. To the extent it is meant to characterize the App's operation described in SAC ¶ 27, that process is not a "redirection" but a sequence of separate communications. *See Ropp*, 347 F. Supp. 2d at 837-38 (analyzing keyboard-to-computer and computer-to-internet communications separately for Wiretap Act purposes).

communication into an interstate one. *See United States v. Ropp*, 347 F. Supp. 2d 831, 837-38 (C.D. Cal. 2004) (fact that device is internet-connected is "irrelevant" if the alleged interception occurred on a local connection, such as the one between a keyboard and computer).

The only plausible interpretation of the alleged facts—stripping out Plaintiff's conclusory allegations and argument—is that the App receives Media Information from the Bose headphones it is paired with over a local Bluetooth connection, which is not a communication in interstate commerce. Plaintiff's Wiretap Act claim should be dismissed independently for that reason. *See In re Google Cookie Placement*, 806 F.3d at 142 (dismissing Wiretap Act claim based on implausible technical characterization of underlying communications); *see also In re Facebook Internet Tracking Litig.*, 263 F. Supp. 3d at 844 (dismissing Wiretap Act claim where plaintiff "misstate[d] the [technical] means by which Facebook receives [] data").

2. Bluetooth Communications Cannot Support a Wiretap Act Violation

Bluetooth is not "a system that affects interstate or foreign commerce." *See* 18 U.S.C. § 2510(12). Rather, it facilitates a ***local*** transmission between two physically proximate devices.

The transmission between a smartphone app and a wireless device via Bluetooth is like that between a keyboard and a computer, which courts have found repeatedly to be outside the scope of the Wiretap Act. In *United States v. Barrington*, students installed keylogger software on registrar computers. 648 F.3d 1178, 1183–84 (11th Cir. 2011). The software "covertly recorded the keystrokes made by registrar employees . . . , capturing their usernames and passwords," and automatically transmitted them to the students' email accounts. *Id*. The Eleventh Circuit held that "use of a keylogger [does] not violate the Wiretap Act if the signal or information captured from the keystrokes is not at that time being transmitted beyond the computer on which the keylogger is installed." *Id.* at 1202. The court in *Rene v. G.F. Fishers, Inc.*, considering a keylogger alleged to intercept passwords typed into a computer, reached the same conclusion. 817 F. Supp. 2d at

1093. The court (adopting *Barrington*) agreed with defendants that there was no "interception" because the keyboard-computer communication was not being transmitted by a system affecting interstate or foreign commerce. *Id.* at 1093-94. It further explained:

> The relevant 'interception' acted on a system that operated solely between the keyboard and the local computer, and captured a transmission that required no connection with interstate or foreign commerce to reach its destination.

Id. at 1094.[18] Similarly, the App and Plaintiff's Bose headphones are communicating not over a system affecting interstate commerce, but over Bluetooth—a local connection between devices within close range. The only difference here is that the "keyboard" is connected to the computer via Bluetooth rather than a physical wire. If that rendered the App's data collection an "interception," nearly every app using Bluetooth could violate the Wiretap Act if it collects usage information (as most do). The ability of Plaintiff's iPhone to communicate over the Internet does not turn the App-to-headphones communications over Bluetooth into a transmission by a system affecting interstate commerce. *See Ropp*, 347 F. Supp. 2d at 837-38 ("[T]he network connection is irrelevant to the transmissions [captured by the keylogger], which could have been made on a stand-alone computer that had no link at all to the internet or any other external network").

C. Plaintiff Does Not Allege that Bose Acquired Communication Contents

Plaintiff's Wiretap Act claim also fails because the allegedly intercepted track information is not "content." The Act requires an interception of "contents," defined as "any information concerning the substance, purport, or meaning of [the] communication." 18 U.S.C. § 2510(8).

[18] Courts within this circuit and elsewhere have reached similar conclusions. *See Halperin v. Int'l Web Servs., LLC*, 70 F. Supp. 3d 893, 902 (N.D. Ill. 2014) (noting defendants' "text enhance" software "capture[s] a transmission that require[s] no connection to the outside world"); *Ropp*, 347 F. Supp. 2d at 834 (whether intercepted signals were electronic communications "turns on whether [they] were transmitted by a system that affects interstate or foreign commerce"); *United States v. Scarfo*, 180 F. Supp. 2d 572, 581 (D.N.J. 2001) (dismissing Wiretap Act indictment where software program did not "search for and record data entering or exiting the computer from the transmission pathway through the [attached] modem").

"Congress intended the word 'content' to mean a person's intended message to another (i.e., the 'essential part' of the communication, the 'meaning conveyed' and the 'thing one intends to convey.')" *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014).

Audio track information does not meet this description—it is simply record information allegedly collected each time Plaintiff plays an audio track while the App is open. It does not convey Plaintiff's intended message to another (if there is "another"). Plaintiff does not allege that the Bose listens to—or can even access—the songs or podcasts themselves, but only that it logs record information about those songs and podcasts, like the name of the track. *See* SAC ¶ 43. Indeed, he does not even allege that users select or search for specific songs using the App. Rather, users simply provide directions like track forward, track back, play, stop. *See* SAC ¶ 27.

Courts have found that similar information is not "content" under the Wiretap Act. The Ninth Circuit held that referrer headers—the portion of a website request that provides the address of the webpage from which the request originated—did not meet the definition of "content." *In re Zynga*, 750 F.3d at 1106-7. The court explained that "'contents' refers to the intended message conveyed by a communication and does not include record information regarding the characteristics of that message [] generated in the course of the communication." *Id.* That referrer header simply identified the "location of [the] website a user [was] viewing," and thus functions like an address. *Id.* at 1107. Similarly, *In re Facebook Internet Tracking Litigation* held that the identity of webpages that users visited and those users' unique identification information did not qualify as content under the Wiretap Act—despite the fact that Facebook could glean information about such users from their browser history. 140 F. Supp. 3d 922, 935 (N.D. Cal. 2015).[19]

[19] *See also In re iPhone Application Litig.*, 844 F.Supp.2d 1040, 1061 (N.D. Cal 2012) (geolocation data was not content, as it was "generated automatically, rather than through the intent of the user" and not "information the user intended to communicate, such as the words spoken in a phone call"); *Gilday v. Dubois*, 124 F.3d 277, 296 n. 27 (1st Cir. 1997) (device that "captures electronic signals relating to the

Plaintiff does not allege that Bose collected the songs or podcasts sent by a streaming service, or any substantive communication Plaintiff entered into his smartphone. Absent such allegations, the SAC fails to allege the acquisition of "contents" required for a Wiretap Act claim.

D. There Was No Disclosure of an Intercepted Electronic Communication

Plaintiff's claim that Bose violated the Wiretap Act by ***disclosing*** audio track information must also be dismissed. It is well settled that "if the interception itself [is] not unlawful, then the subsequent use or disclosure of intercepted information is not unlawful." *Vazquez-Santos v. El Mundo Broadcasting Corp*., 219 F. Supp. 2d 221, 229 (D.P.R. 2002); *see also Forsyth v. Barr*, 19 F.3d 1527, 1538 (5th Cir. 1994) (liability for disclosure or use under Wiretap Act requires that the information was obtained from an intercepted communication). That is the case here.[20]

II. Plaintiff's Illinois Eavesdropping Act Claim Fails as Matter of Law

Plaintiff's Eavesdropping Act claim should also be dismissed. As the Court recognized, it "is based on the same alleged conduct as the federal Wiretap Act claim, namely that Bose was not a party to the private electronic communications between users and Spotify, and that Bose intercepted these communications and transmitted them to a third party without users' consent." Order at 11. The Court thus dismissed Plaintiff's eavesdropping claim from the FAC for the same reason it dismissed his Wiretap Act claim. *Id.* For the same reasons that the SAC fails to cure the deficiencies in Plaintiff's Wiretap Act claim, it fails with respect to his eavesdropping claim.[21]

[personal identification number] of the caller, the number called, and the date, time and length of the call" does not capture communications contents and therefore "is not within the ambit of the Wiretap Act").

[20] Plaintiff's improper disclosure claim is also based on a mischaracterization of Segment's services. His depiction of Segment as a third-party "data miner" is based on disingenuous omission of language from its website, which makes clear it only collects and processes information within Bose's own data sets for Bose's own benefit. Similarly, while Plaintiff wildly speculates about Bose's ability to sell data "to the highest bidder," he offers no facts suggesting that ever happened (it did not). SAC ¶ 4.

[21] *See, e.g.*, *Bender v. Board of Fire and Police Comm'rs*, 539 N.E.2d 234, 237 (Ill. App. Ct. 1989) (holding that "no eavesdropping occurs where an individual to whom statements are made or directed records them, even without the knowledge or consent of the [other] person").

Plaintiff's Eavesdropping Act claim also fails for two additional reasons. First, there was no interception of "[a]udio recordings of truly private conversations." *People v. Clark,* 6 N.E.3d 154, 161 ¶ 22 (Ill. 2014). Rather, the App merely collected publicly available audio track information from commercial songs or podcasts, which cannot form the basis of an eavesdropping claim.[22] Second, any alleged interception was not "surreptitious." 720 ILCS 5/14-1(g) (surreptitious means "obtained or made by stealth or deception, or executed through secrecy or concealment"). Given that 'receiving and displaying Media Information is a primary function of the App" (Order at 6) and the privacy policy discloses Bose's collection of usage information when the App in use, the "secrecy or concealment" requirement is not met. *Id.*[23]

CONCLUSION

After three tries, this is not a Wiretap Act or Eavesdropping Act case. Besides self-serving conclusory allegations, the SAC does not plausibly state any claims or cure the deficiencies identified in the Order. The Court should grant Bose's motion to dismiss, this time with prejudice.

[22] *See Thomas v. Pearl*, 793 F. Supp. 838, 845 (C.D. Ill. 1992) (disclosure of a non-private conversation is not unlawful), *aff'd*, 998 F.2d 447 (7th Cir. 1993).

[23] Bose also reasserts—mainly to preserve for appeal—its arguments that Plaintiff's remaining claims should be dismissed. His Illinois Consumer Fraud Act claim fails because the SAC does not adequately allege an actionable omission or cognizable damages, or that any purported omissions about the App were material to Plaintiff's headphone purchase. His unjust enrichment claim fails because it is premised on the same conduct as his other claims and the SAC does not adequately allege any benefit Bose unjustly retained in violation of fundamental principles of justice where he downloaded a free app.

Dated: May 30, 2019

By: /s/ *Bart Huff*

Bart Huff (6225211)
bart@zwillgen.com
ZWILLGEN PLLC
300 N LaSalle St, Suite 4925
Chicago, IL 60654
(312) 685-2278 (telephone)

Marc Zwillinger (6226447)
marc@zwillgen.com
Jeffrey Landis (admitted *pro hac vice*)
jeff@zwillgen.com
Nicholas Jackson (admitted *pro hac vice*)
nick@zwillgen.com
ZWILLGEN PLLC
1900 M. Street NW, Suite 250
Washington, DC 20036
(202) 706-5205 (telephone)
(202) 706-5298 (facsimile)

Counsel for Defendant

CERTIFICATE OF SERVICE

I, the undersigned attorney, hereby certify that on May 30, 2019, I caused the foregoing to be electronically filed with the Clerk of Court using the CM/ECF system, which will send notification of such filing to the following attorneys of record:

Jay Edelson
Benjamin Thomassen
J. Eli Wade Scott
EDELSON PC
350 North LaSalle, 14th Floor
Chicago, IL 60654
jedelson@edelson.com
bthomassen@edelson.com
ewadescott@edelson.com

Rafey S. Balabanian
EDELSON PC
123 Townsend Street, Suite 100
San Francisco, CA 94107
rbalabanian@edelson.com

/s/ Jeffrey Landis
Jeffrey Landis