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 Designated Magistrate Judge: M. David Weisman

DEFENDANT'S MOTION TO DISMISS FIRST AMENDED CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Defendant Bose Corporation ("Defendant"), by its undersigned counsel, respectfully moves to dismiss Plaintiff's First Amended Class Action Complaint and Demand for Jury Trial pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure. In support thereof, Defendant adopts and incorporates its accompanying Memorandum of Law in Support of its Motion to Dismiss Plaintiff's First Amended Complaint and Demand for Jury Trial and the accompanying Declaration of Jeffrey Landis.

Respectfully Submitted,

Dated: August 3, 2017

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

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 Designated Magistrate Judge: M. David Weisman

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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes and Rules

INTRODUCTION

Despite Plaintiff's amendments to the complaint, this case is still not about wiretapping or eavesdropping. Instead, it is a transparent effort to leverage the statutory damages provision of the Wiretap Act to put pressure on Bose Corp. ("Bose") for a relatively pedestrian claim that an internet app did not adequately disclose its privacy practices. Even though dismissal of the claim requires a basic understanding of how Bluetooth operates, this Court should give Plaintiff's claim careful scrutiny and dismiss it because his theory of liability is premised on implausible conclusory assertions for which he provides no factual support and which make no sense in light of the undisputed operation of the relevant technology. Indeed, this would be the first case in history to characterize information collection by an app provider as an intercept under federal or state law, and it could make the standard operation of innumerable apps and devices illegal.

Plaintiff Kyle Zak's grievance with Bose is that when he used the Bose Connect App (the "App") to view basic information about streaming music playing on his Bose wireless headphones and to control such playback, Bose collected and retained the song information being displayed in the App. The Amended Complaint ("Complaint") asserts that this collection is an interception of electronic communications between Plaintiff and streaming music providers like Spotify. But the Complaint provides no basis for this conclusory assertion—unsurprisingly so, since it is contrary to how apps work. Rather, the well-documented architecture of Apple smartphones and the Bluetooth protocol makes clear that the only "communication" in which the App is involved is a local connection between the App and compatible Bose headphones. The App cannot access communications between a user's music app or smartphone and third party streaming music providers—the App's only source of information is the Bluetooth connection it establishes with paired Bose headphones. Plaintiff alleges no facts suggesting anything else—only conclusory

statements. Nor could he, because Apple, by design, prevents one app from seeing communications sent and received by another app.

Plaintiff's Wiretap Act claim fails for two reasons. ***First***, the Act does not apply to local Bluetooth communications between a smartphone app and headphones because such communications do not affect interstate or foreign commerce. A cognizable intercept under the Wiretap Act first requires the acquisition of an "electronic communication," which is a transfer by a "system that affects interstate or foreign commerce." *See* 18 U.S.C. § 2510(12). Bluetooth is a local system that operates between devices in close physical proximity without the need for any network or internet connection, like the system that transmits information between a keyboard and computer, which numerous courts have found does not affect interstate or foreign commerce.

Second, the Wiretap Act only applies to communications between two separate parties, where the alleged interceptor is not one of them. Under the only plausible reading of the facts alleged in the Complaint, the communications at issue occurred between Plaintiff's Bose headphones and Bose's App. Either the Plaintiff was the only party to the communication, or Bose was one of the parties. In either case, neither the Wiretap Act nor the Illinois Eavesdropping Act apply. Plaintiff's Eavesdropping Act claim is also deficient because any capture of information is not surreptitious. The App's conspicuous operation, as well as the displays on Bose's website, make clear that the App receives the name of the audio track being played.

Plaintiff's Illinois Consumer Fraud Act ("ICFA") claim fares no better. Plaintiff has not pled an actionable omission—*i.e.*, one that creates an affirmatively false impression, not just an incomplete one—let alone with the particularity required for a fraud claim. He also has not adequately alleged that any omission about the App was material to his decision to purchase his headphones—which can be used without the App. Indeed, the App-related disclosures identified

in the Complaint pertain to features about which Plaintiff raises no concerns, such as personalizing headphone settings. The complained-of remote control feature—which he did not adequately allege he knew about before his purchase—is an immaterial component of the free optional App: all it does is replicate the same music controls (play, pause, fast forward, etc.) already available in the underlying music app and built in to countless headphone models. Moreover, Plaintiff's unsupported contention that he would not have purchased his Bose headphones (or paid less for them) had he known how the optional App functioned is not an actionable injury under ICFA.

Plaintiff's common law unjust enrichment claim also fails because it is based solely on the conduct underlying his deficient statutory claims, and because he does not adequately allege that Bose owed any cognizable duty to act or unjustly retained any benefit it received. Because none of Plaintiff's laundry list of claims can survive scrutiny, and because Plaintiff has already amended once, his Complaint should be dismissed in its entirety with prejudice.

BACKGROUND

A. Bose's Products and Offerings

Bose is a Delaware corporation headquartered in Framingham, Massachusetts. First Amended Complaint ("Compl."), ECF No. 24, ¶ 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 not needed to listen to music or other audio on Bose wireless headphones or speakers—customers can do so without ever downloading it. *See id.* ¶¶ 18-19. It 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," and also adjust the settings on their wireless device or download firmware updates for those products. *Id.* ¶¶ 15, 20. The App also allows users to share audio between two Bose wireless devices—for instance, two users with Bose Connect can listen to the same music while running.[2] These features (not to mention the App's name) make clear that Bose Connect "connects" a user's smartphone to his or her headphones or speakers to allow the two devices to communicate with each other.

Additionally, the App can be used as an alternate method to remotely control the playback of music being received by a compatible Bose wireless device from another media app—the App displays basic information about the currently playing track (such as artist and song name) and provides an interface to pause, resume, skip tracks, and so on. *Id.* ¶¶ 16, 26. These same controls are also available via buttons on Bose headphones and, of course, through the relevant music app itself. *See id.* ¶ 16, 19. 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 users can access Bose's privacy policy through the App. That policy disclosed that the App enables users to link their headphones "to a variety of media sources," and that Bose may use "mechanisms to track and analyze how you use the [A]pp" and "web logs or applications that recognize your device and gather information about its online activity."[3]

---

[1] *See Bose Connect on the App Store*, https://itunes.apple.com/us/app/bose-connect/id1046510029?mt=8 (last visited Aug. 1, 2017). On a motion to dismiss, a court can consider, in addition to the allegations set forth in the complaint, 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). Here, the Complaint repeatedly refers 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.*, Compl. ¶¶ 14, 15, 20, 21, 23, 27.

[2] *See QC35 Wireless Noise Cancelling Headphones*, Bose, https://www.bose.com/en_us/products/headphones/over_ear_headphones/quietcomfort-35-wireless.html (last visited Aug. 1, 2017).

[3] *See* Declaration of Jeffrey Landis, dated Aug. 3, 2017 ("Landis Decl."), Ex. 1.

B. iOS, Apps and Bluetooth Accessories

According to the Complaint, Plaintiff downloaded the App from the Apple App Store, indicating that his device is an iPhone. *See* Compl. ¶ 35-36. iPhones run the iOS operating system, the technical design and operation of which is laid out in publicly available documentation from Apple—including developer guidelines and manuals that developers rely on to create compatible iPhone apps. The Bluetooth technology standard is similarly described in formal specification documents, which define the requirements for building interoperable devices.[4] These generally accepted standards, not subject to dispute, undermine the plausibility of Plaintiff's claim.[5]

By design, iOS places third-party apps like Bose Connect into a "sandbox"—meaning that the system restricts them from "gathering or modifying information stored by other apps" or "making changes to the device," and also shields "[s]ystem files and resources . . . from the user's apps."[6] Due to these strict limitations, "[i]f a third-party app needs to access information other than its own, it [can do] so only by using services explicitly provided by iOS."[7] iOS provides a built-in mechanism (the "iOS Media Player Framework") for music player apps (such as Spotify)

---

[4] *See Specifications*, Bluetooth Technology Website, https://www.bluetooth.com/specifications (last visited Aug. 1, 2017).

[5] 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 regarding the design of its own iOS operating system, as well as formal Bluetooth specifications published by the body (Bluetooth SIG) responsible for managing that technology 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 under Fed. R. Evid. 201 of Apple's "iOS Human Interface Guidelines" and "App Store Approval Process instructions," among other materials); *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 (C.D. Cal. June 3, 2015), *aff'd*, No. 15-56021, 2017 WL 1019084 (9th Cir. Mar. 16, 2017) (taking judicial notice of product specifications readily available on manufacturer's website).

[6] *See* Apple, iOS Security White Paper, at 20 (March 2017), *available at* https://www.apple.com/business/docs/iOS_Security_Guide.pdf.

[7] *Id.*

to provide song 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 sharing it with connected accessories—though this information remains inaccessible to other third-party apps like Bose Connect (due to sandboxing).[8] Thus, neither the App nor any set of Bose headphones can access the stream of communications sent between an internet music site like Spotify and the user's iPhone. Plaintiff does not and cannot allege that Bose circumvented these protections.

To enable Bluetooth headphones to communicate with an iPhone, the manufacturer must implement the appropriate Bluetooth specifications. Bluetooth audio signals are transmitted from a smartphone to an accessory via a standardized format called the "Advanced Audio Distribution Profile" ("A2DP").[9] Bluetooth headphones can also support an additional profile—the "Audio/Video Remote Control Profile" ("AVRCP")—which provides a mechanism for receiving media information from and sending music control instructions (play, pause, fast forward, etc.) to a smartphone.[10] On iPhones, the iOS Media Player Framework transmits song information (artist, album, and song title¸ etc.) to compatible Bluetooth devices using the AVRCP profile.[11] Plaintiff does not allege that Bose Connect has any involvement in that transmission (because it does not).

iOS also enables Bluetooth devices like Bose's headphones to communicate directly with third-party apps (as opposed to the operating system itself), through a separate set of protocols.[12]

---

[8] *See* Apple, Bluetooth Accessory Guidelines for Apple Products (Release R8), § 2.2.5.7 (Jun. 16, 2017), *available at* https://developer.apple.com/hardwaredrivers/BluetoothDesignGuidelines.pdf ("Apple Bluetooth Guidelines"); *Media Player Framework*, Apple Developer Documentation, https://developer.apple.com/documentation/mediaplayer (last visited Aug. 1, 2017).

[9] *See* Bluetooth SIG, Advanced Audio Distribution Profile (A2DP) Specification v1.3.1 (Jul. 14, 2015), *available at* https://www.bluetooth.com/specifications/profiles-overview; Apple Bluetooth Guidelines § 4.

[10] *See* Bluetooth SIG, Audio/Video Remote Control Profile v1.6.1 (Dec. 12, 2015), *available at* https://www.bluetooth.com/specifications/profiles-overview.

[11] *See* Apple Bluetooth Guidelines § 2.2.5.

[12] There are a couple different mechanisms in iOS for establishing such communications channels—the iOS External Accessory Framework and the Core Bluetooth Framework—but both enable the same basic

Bluetooth device makers use these protocols to create custom iPhone apps that provide a separate, secure communications channel with their devices.[13] This is how Bose Connect works—the App "talks" to the Bose headphones—and Plaintiff does not allege any facts to the contrary.

C. Plaintiff's Use of Bose Connect

Plaintiff alleges that he purchased Bose QuietComfort 35 wireless headphones "[o]n or around February 2017" for $350. Compl. ¶ 34. While he alleges that he read on the product's packaging that he could "Enhance headphone with Bose Connect app," he does not allege that the App influenced his decision to buy the headphones. *See id.* ¶ 35. Nevertheless, he says that "immediately" after buying the headphones he downloaded the App to his smartphone. *Id.* ¶ 36. Plaintiff allegedly used the App while listening to streaming music to configure the settings on his headphones, access unnamed additional features, and skip and pause tracks. *Id.* ¶ 37. In other words, he used the App to communicate locally with his headphones, in much the same way that a remote control communicates with a TV, or a modern app controls a toy drone.

D. Bose's Alleged Improper Conduct

Plaintiff alleges that, when in use, Bose Connect's remote control feature "monitor[s] and collect[s] information resulting from listener interaction with the app." Compl. ¶ 25. Specifically, he alleges that Bose programmed the App to "intercept the contents of the electronic communications between the listener and his or her streaming music services," including "the names of music and audio tracks the listener selects to play." *Id.* ¶ 24. He offers no facts

---

functionality: allowing third-party apps 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 iOS External Accessory Framework); *Core Bluetooth Framework*, Apple Developer Documentation, https://developer.apple.com/documentation/corebluetooth (last visited Aug. 1, 2017) (describing Core Bluetooth Framework).

[13] *See id.*

explaining how this can be an interception given that Bose Connect—like any other third-party iPhone app—cannot access communications between the iPhone and streaming services. Similarly, Plaintiff asserts that Bose did so "to create detailed profiles" about its users listening habits but alleges no facts supporting the existence of such profiles. *Id.* ¶ 28.

Plaintiff further alleges that Bose Connect disclosed audio track information for tracks played through the App to a third party, Segment.io, Inc. ("Segment"). *Id.* ¶ 27. Plaintiff ominously describes Segment as a "sophisticated data mining and analysis company, " but omits language explaining that such "collection" is performed for Segment's clients within their own data sets, in order to "[s]chematize and load data into your own data warehouse."[14] *Id.* Plaintiff alleges no facts to the contrary or suggesting that Segment accesses Bose's data for any purpose other than to perform such routing services for Bose.

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). Where the alleged facts "do not permit the court to infer more than the mere possibility of misconduct," the complaint has merely alleged but has not shown that the pleader is entitled to relief. *Iqbal*, 556 U.S. at 679.

[14] *See* Landis Decl., Ex. 2.

I. Plaintiff's Wiretap Act Claim Should Be Dismissed

Plaintiff fails to state a Wiretap Act claim for multiple reasons, which stem from the fact that this is simply not a Wiretap Act case. The Electronic Communications Privacy Act, which amended the Federal Wiretap Act of 1968, 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 also prohibits disclosure or use of the contents of an unlawfully intercepted communication. *Id*. § 2511(1)(c), (d). It includes certain statutory exceptions to these limitations. *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. Bose Did Not Intercept an Electronic Communication

Plaintiff's Wiretap Act claim fails because he does not allege an interception of a communication in interstate commerce. The only plausible reading of the ***facts*** in the Complaint is that the relevant "communications"—*i.e.*, the transmission of song information to the App—took place over a Bluetooth connection between the App and Plaintiff's Bose headphones. But such short-distance local transmissions cannot form the basis of a Wiretap Act claim.[15] The Act defines "intercept" as the acquisition of "contents" of any "electronic communication" through the use of certain devices. 18 U.S.C. § 2510(4). An "electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted

[15] *See, e.g., Using a Bluetooth Mouse, Keyboard, or Trackpad*, Apple Support, https://support.apple.com/en-us/HT201171 (Apr. 12, 2017) ("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).

in whole or in part by a . . . ***system that affects interstate or foreign commerce***." *Id.* § 2510(12) (emphasis added). Together, these definitions require that "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 Only Plausible Way the Bose Connect App Could Collect Information is Over a Local Bluetooth Connection.

Plaintiff does not plausibly allege facts supporting an interception of an electronic communication transmitted by a system that affects interstate commerce. Plaintiff's theory is that Bose captured communications between Plaintiff's iPhone and streaming music services taking place over the internet. *See* Compl. ¶ 52. However, the Complaint lacks facts that would explain how such interception could actually happen. Instead, it offers only conclusory statements tracking the legal elements of a Wiretap Act claim that must be disregarded. *See Adams*, 742 F.3d at 733. To compound this pleading failure, the basic architecture and security features of iOS devices such as Plaintiff's, which are extremely well-documented and widely understood, reveal Plaintiff's theory to be utterly implausible. The far more plausible interpretation of any facts alleged is that the App's only source of audio information is the Bose headphones it is paired with over a local Bluetooth connection. "[W]hen [a] defendant's plausible alternative explanation is so convincing that plaintiff's explanation is *im*plausible," dismissal is warranted. *In re Google Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 142 (3d Cir. 2015) (dismissing Wiretap Act claim based on implausible technical characterization of underlying communications, and noting court "need not give legal effect to 'conclusory allegations' that are contradicted by the pleader's actual description of what happened"); *see also In re Facebook Internet Tracking Litig.*, No. 5:12-MD-02314-EJD, 2017 WL 2834113, at *4 (N.D. Cal. June 30, 2017) (dismissing Wiretap Act claim where plaintiff "misstate[d] the [technical] means by which Facebook receives [] data").

Bose Connect is a third-party app. As such, it is blocked from directly accessing information that belongs to other apps on Plaintiff's iPhone, including third-party music player apps like Spotify. Apple instructs developers to provide information about currently playing audio tracks to the iPhone's operating system via the iOS Media Player Framework.[16] The operating system in turn passes that information along to compatible Bluetooth accessories via the AVRCP profile, the same channel through which the accessory can issue music control commands back to the iPhone (using, for instance, hardware buttons like those found on Plaintiff's Bose headphones). *See* Compl. ¶ 19. Accessory manufacturers like Bose can also set up a separate transmission channel directly between their own app and their accessory using one of the separate protocols provided by Apple. The Connect App features described in the Complaint—the ability to download and install firmware updates to the headphones, or to adjust the headphones' noise cancellation and "Auto-Off" settings—involve such a direct connection. *See id.* ¶ 15. There is no other way those features could function and Plaintiff does not allege facts suggesting otherwise.

The legal conclusion underlying Plaintiff's claim—that the Connect App intercepts internet communications between the Spotify app on a user's iPhone and Spotify's internet server—is facially implausible given iOS's "sandbox" security design, which prevents apps from peering into the activities of other apps. Further, the App's "remote control" capabilities correspond exactly to those enabled by an AVRCP connection between an iPhone and a suitable Bluetooth device—*i.e.*, the ability to display track information and to issue playback commands. Against this backdrop, the only plausible (and in fact accurate) understanding of the Complaint's factual allegations is

[16] *Media Player Framework: Class MPNowPlayingInfoCenter*, Apple Developer Documentation, https://developer.apple.com/documentation/mediaplayer/mpnowplayinginfocenter (last visited Aug. 1, 2017) (developer instructions on how to "provide descriptive information about the content being played" by an app to iOS).

that the Connect App receives media information exclusively through its direct local connection to paired Bose headphones.

And while the headphones received that same information in the first instance from the iPhone's operating system (via the AVRCP profile), that communication is a distinct communication—and is also entirely separate from any internet communication between a streaming music provider and the music app. *See In re Facebook Internet Tracking Litig.*, 2017 WL 2834113, at *4 (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"). Plaintiff's logic appears to be that because when a user pushes the "next track" button on the App, a similar command ultimately finds its way back to Spotify, therefore the local communication of song data between a Bose headset and the App turns into an interception that affects interstate commerce. *See* Compl. ¶¶ 25-26. That logic is terribly flawed. The transmission path of any command from the App—or even from the headphones buttons without the App—is to the user's iPhone, not to Spotify. And even if it were, the music track information that is communicated locally from the headphones to the App is not a communication in interstate commerce.

When an "obvious alternative explanation" exists for a complaint's non-conclusory allegations, it fails to "state a claim to relief that is plausible on its face." *Twombly*, 550 U.S. 568-70.[17] For Plaintiff's theory to be plausible, he must allege some facts plausibly suggesting an interception could take place notwithstanding the strict limitations imposed on all third-party iOS apps. The Complaint's mere "formulaic recitation of the cause of action" is insufficient.[18]

---

[17] This explanation does not need discovery, because Plaintiff does not allege that the App has any functionality when Bose wireless headphones are not connected—this makes it clear that the App is not intercepting communications with the Spotify app, but is getting it from the headphones.

[18] *See McCauley v. City of Chicago*, 671 F.3d 611, 617 (7th Cir. 2011) (finding insufficient the allegation that defendant knowingly, intentionally and maliciously prosecuted plaintiff in retaliation for exercising his

2. Bluetooth Communications Cannot Give Rise to a Wiretap Act Violation.

Given that the facts alleged in the Complaint most plausibly suggest that the relevant communication is a local Bluetooth communication, the Complaint fails to allege an interception of a communication in interstate commerce. Bluetooth is not "a system that affects interstate or foreign commerce." *See* 18 U.S.C. § 2510(12). It facilitates a local transmission between two physically proximate devices that does not touch interstate or foreign commerce.

The transmission between a smartphone app and a wireless device via Bluetooth is like a transmission 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*, college students installed keylogger software on registrar computers in order to acquire employees' passwords and then use those passwords to change their grades. 648 F.3d 1178, 1183–84 (11th Cir. 2011). The software "covertly recorded the keystrokes made by registrar employees as they signed onto their computers, capturing their usernames and passwords," and then automatically transmitted the usernames and passwords to the students' email accounts. *Id*. The Eleventh Circuit found that the software was not a device that could be used to intercept an electronic communication in violation of the Wiretap Act. *Id* at 1202–3. Specifically, the court found that "use of a keylogger will 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 (or being otherwise transmitted by a system that affects interstate commerce)." *Id.* at 1202.

The court in *Rene v. G.F. Fishers, Inc.*, reached the same conclusion. There, plaintiff alleged that defendants' use of a keystroke logger to intercept the transmission of her keystrokes

constitutional rights); *see also United States ex rel. Ivanich v. Bhatt*, No. 13 C 4241, 2015 WL 249413, at *2 (N.D. Ill. Jan. 20, 2015) (noting that "[w]ithout supporting facts, the Court does not accept as true Ivanich's conclusion that the services provided by the physician assistants were not integral").

as she typed passwords into a computer violated the Wiretap Act. *Rene*, 817 F. Supp. 2d at 1093. Defendants argued there could be no "interception" under the Wiretap Act because the communication between the keyboard and computer was not being transmitted by a system that affects interstate or foreign commerce. *Id.* The district court, adopting *Barrington*, agreed, finding that a Wiretap Act interception "must occur while the transmission is traveling through a system that affects interstate or foreign commerce." *Id.* at 1093-94. The court explained:

> The key to the *Barrington* decision lies in the fact that the transmission of keystrokes exists internally on a computer. 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.

Courts within this circuit have recognized the Wiretap Act's interstate or foreign commerce requirement. *See Halperin v. International Web Services, LLC*, 70 F. Supp. 3d 893, 902 (N.D. Ill. 2014) (noting that defendants "text enhance" software "'capture[s] a transmission that require[s] no connection' to the outside world."). Other courts have reached similar conclusions. *See United States v. Ropp*, 347 F. Supp. 2d 831, 834 (C.D. Cal. 2004) (holding that whether intercepted signals were electronic communications within the meaning of the statute "turns on whether the signals that 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 modem attached to the computer").

The signals between the App and Plaintiff's Bose headphones are similarly not being transmitted by a system affecting interstate commerce. They are being transmitted via Bluetooth, a local connection between devices within close range. The only meaningful difference between this situation and the keylogger cases is that in this case the "keyboard" is not connected to the computer with a wire, it is connected via Bluetooth (as many keyboards now are). If that rendered

the App's collection of information a Wiretap Act "interception," nearly every App that functions via Bluetooth would potentially violate the Wiretap Act if it collects usage information (which nearly all apps do). ***No court has ever found a Wiretap Act violation in a situation such as this.***

The fact that there is no actionable Wiretap Act claim here is further demonstrated by the information allegedly intercepted. Plaintiff alleges that Bose recorded audio track information (and device serial number). If Bose was truly "intercepting" communications between Spotify and Plaintiff's iPhone, or the iPhone and his headphones, it would logically also collect the music being transmitted—the same way an interception of a telephone call captures the words being spoken. That is not Plaintiff's claim. Alleging that Bose records the title of an audio track being played using the App is not the same as alleging that Bose intercepted the actual notes or lyrics of the song. This distinction confirms that this is a case about information collection, not interception.

B. Either Bose Was a Party to Any Communication or There Was No Party Other than the User

Even if the transmission system affected interstate commerce, a communication under the Wiretap Act must involve two parties, and the alleged interceptor cannot be either of them. Here, Bose was the only other possible party to the communication sent between the Bose headphones and the App. Section 2511(2)(d) of the Wiretap Act allows a person to intercept an electronic communication "where such person is a party to the communication." Although the Complaint alleges that streaming music providers are the other party to any communication (*see* Compl. ¶¶ 29, 52), that statement is based on the Complaint's conclusory misidentification of the communication allegedly being intercepted. While streaming music providers may be communicating 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.

"Tautologically, a communication will always consist of at least two parties: the speaker

and/or sender, and at least one intended recipient." *In re Google Cookie Placement*, 806 F.3d at 143. When Bose Connect is in use, it only receives and retains audio track information transmitted to it directly from Plaintiff's headphones. In other words, the App is the intended recipient of the communication; the point of using the App is to connect it with the headphones. The name of the App alone communicates that purpose. To the extent that such connection is a communication covered by the Wiretap Act, Bose is a party to it. Under such circumstances, Bose "acted as no more than the second party to a communication. This is not an interception as defined by the Wiretap Act." *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001).

Wiretap Act cases against internet advertising providers placing cookies on computers to facilitate internet advertising provide a useful parallel. In *Google Cookie Placement*, plaintiffs alleged that defendant internet advertisers acquired the plaintiffs' internet history when, in the course of requesting webpage advertising content the plaintiffs' browsers sent information to defendants via a cookie defendants placed on their computers. 806 F.3d at 142. The theory was that once placed, the cookie would "intercept" plaintiffs' communications and transmit them back to defendants. The Third Circuit affirmed dismissal of the Wiretap Act claim on the ground that defendants were parties to the communication. *Id.*; *see also United States v. Pasha*, 332 F.2d 193, 198 (7th Cir. 1964) (noting that "officer did not 'intercept' a message while it was en route to another; there was no other on the line"); *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 274 (3d Cir. 2016) (affirming Wiretap Act dismissal where "Google was either a party to all communications with the plaintiffs' computers" or allowed to communicate with them by a party).

If there is any second party to the communications at issue, it is Bose. Plaintiff does not allege that Bose collects communications between his smartphone and headphones when the App is not running (because he cannot). Bose only receives information when headphones are

connected to the App. In other words, users intend the App to receive their information. And if Bose is not a party to the communication, there is no second party—Plaintiff would simply be communicating with himself, in much the same way 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 where the communication allegedly intercepted was between a user and himself. This makes sense. It would not violate the Wiretap Act to "intercept" a voice memo someone is recording to themselves on their smartphone. Either the Bose headphones and App are standing in for Bose as parties to the communication, or they are standing in for Plaintiff himself. Either way, there is no communication between Plaintiff and a non-Bose party. *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").

Finally, even if it were possible to "intercept" a communication between Plaintiff and himself, Plaintiff consented to the App's collection of information. The Wiretap Act authorizes interception where "one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(c). Bose's Privacy Policy disclosed that the App collected information when in use, and that Bose "may use mechanisms to track and analyze how you use the app." Landis Decl., Ex. 1 at 1. Bose Connect users agree to this Privacy Policy by downloading or using Bose Connect. *Id.* at 1. Users are also put on notice that the App has access to song information simply by using it, since the App displays such information as part of its functionality.

C. There Was No Disclosure of an Intercepted Electronic Communication

Plaintiff's claim that Bose violated the Wiretap Act by ***disclosing*** audio track and serial number information must also be dismissed. The Act prohibits disclosing the contents of an electronic communication obtained through an interception. *See* 18 U.S.C. § 2511(c). 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. Because Bose did not intercept communications under the Wiretap Act, it cannot improperly disclose such communications.[19]

II. The Court Should Decline to Exercise Jurisdiction Over Plaintiff's Other Claims

Given the deficiencies in Plaintiff's only federal claim, the Court should decline to exercise supplemental jurisdiction over his remaining claims. "[I]t is the well-established law of this circuit that the usual practice is to dismiss without prejudice state supplemental claims whenever all federal claims have been dismissed prior to trial." *Groce v. Eli Lilly & Co.*, 193 F.3d 496, 501 (7th Cir. 1999); *see also Wright v. Associated Ins. Cos. Inc.*, 29 F.3d 1244, 1251 (7th Cir. 1994) ("[T]he general rule is that, when all federal claims are dismissed before trial, the district court should relinquish jurisdiction over pendent state-law claims rather than resolving them on the merits."). As this case is still at the earliest stage, there is no need to depart from the standard practice for Plaintiff's remaining state law claims. *See, e.g., Washington v. N. Star Capital Acquisition, LLC*, No. 08 C 2823, 2008 WL 4280139, at *3 (N.D. Ill. Sept. 15, 2008) (dismissing Illinois Consumer Fraud Act and other state claims as "[p]recedent in this circuit instructs").

[19] Plaintiff's improper disclosure claim is also based on a mischaracterization of the services Segment performs for Bose. Plaintiff's depiction of Segment as a third-party "data miner" is based on the disingenuous omission of language from Segment's website which makes clear it in fact only collects and processes information within Bose's own data sets and for Bose's own benefit. Along the same lines, while Plaintiff wildly speculates about Bose's ability to sell data collected by the App "to the highest bidder," he offers no facts suggesting that ever happened (it did not). *Id.* ¶ 4; *Thomas v. Indiana Dep't of Correction*, No. 3:15-CV-18-TLS, 2015 WL 3631677, at *1 (N.D. Ind. June 10, 2015) (noting "plausible allegations must do more than speculate as to what might have happened") (citing *Twombly*, 550 U.S. at 555).

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

Plaintiff's Eavesdropping Act claim should also be dismissed for failure to adequately allege a violation. The Eavesdropping Act is meant "to protect conversational privacy." *People v. Clark*, 6 N.E.3d 154, 161 ¶ 22 (Ill. 2014). A person violates the Act "when he [] knowingly and intentionally: [i]ntercepts, records or transcribes, in a surreptitious manner, any private electronic communication to which he [] is not a party" without consent. 720 ILCS 5/14-2(a)(3).

Plaintiff's Eavesdropping Act claim fails for the same reasons his Wiretap Act claim fails, plus more. First, there was no interception of "[a]udio recordings of truly private conversations [] within the legitimate scope of the statute." *Clark*, 6 N.E.3d at 161 ¶ 22. There were no private conversations at all—the App merely collected publicly available audio track information from commercial songs or podcasts, which cannot form the basis of an Eavesdropping Act claim. *See Thomas v. Pearl*, 793 F. Supp. 838, 845 (C.D. Ill. 1992) ("[I]f a conversation is not private, then disclosing the contents of that conversation, whether verbally or by distributing a tape, cannot be unlawful."), *aff'd,* 998 F.2d 447 (7th Cir. 1993). Second, the Eavesdropping Act only applies where a person is not a party to the communication, *see* 720 ILCS 5/14-2(a)(3), and as discussed above, to the extent there was any "communication" Bose was a party to it, *see Angelo v. Moriarty*, No. 15 C 8065, 2016 WL 640525, at *4 (N.D. Ill. Feb. 18, 2016) (holding that "despite Plaintiff's argument that the conversation was private, . . . because Defendant [] was a party to this conversation, Plaintiff's cannot establish a violation of the Act"); *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 person making the statements").

Plaintiff's Eavesdropping Act claim also fails because even if there were an interception of a communication to which Bose was not a party, such interception was not "surreptitious." The

Act defines surreptitious as "obtained or made by stealth or deception, or executed through secrecy or concealment." 720 ILCS 5/14-1(g). When a person listens to an audio track while running Bose Connect, the title and track information appear on the App. This, along with the fact that Bose's Privacy Policy discloses that Bose collects usage information from Bose Connect when in use, is the opposite of "secrecy or concealment." 720 ILCS 5/14-1(g).

IV. The Complaint Fails to State a Claim Under the Illinois Consumer Fraud and Deceptive Business Practices Act

To state an ICFA claim, Plaintiff must adequately allege: "(1) a deceptive act or practice by the defendant, (2) the defendant's intent that the plaintiff rely on the deception, (3) the occurrence of the deception in the course of conduct involving trade or commerce, and (4) actual damage to the plaintiff (5) proximately caused by the deception." *Avery v. State Farm Mut. Auto. Ins. Co.*, 835 N.E.2d 801, 850 (Ill. 2005). In cases alleging "concealment, suppression or omission" of information, the allegedly concealed facts must be material, and must give rise to an impression that is "affirmatively false"—not merely "incomplete." *Spector v. Mondelēz Int'l, Inc.*, 178 F. Supp. 3d 657, 665, 672 (N.D. Ill. 2016). The Complaint cannot meet these standards.

A. The Complaint Does Not Plead with Particularity an Actionable Omission

An omission of fact is actionable under ICFA only "where it is employed as a device to mislead." *Spector*, 178 F. Supp. 3d at 672 (citing *Pappas v. Pella Corp.*, 844 N.E.2d 995, 998 (Ill. App. Ct. 2006)). "Illinois courts are always watchful that the Act not be used to transform nondeceptive and nonfraudulent omissions into actionable affirmations." *Spector*, 178 F. Supp. 3d at 672 (citation omitted); *see also Harkala v. Wildwood Realty, Inc.*, 558 N.E.2d 195, 200 (Ill. App. Ct. 1990). Further, both the Federal Rules and Illinois law impose a heightened burden for pleading deceptive practices claims under ICFA. *See Camasta v. Jos. A. Bank Clothiers, Inc.*, 761 F.3d 732, 736-37 (7th Cir. 2014); *Spector*, 178 F. Supp. 3d at 672 (in Illinois, allegations "must

show not just the mere possibility of fraud, but that fraud is a 'necessary or probable inference from the facts alleged'") (citation omitted). "The bald assertion of deception is insufficient to state a claim; the deceptive manner of the omission must be stated with specificity and particularity." *Rockford Mem'l Hosp. v. Havrilesko*, 858 N.E.2d 56, 64 (Ill. App. Ct. 2006). Moreover, "an omission is not actionable as fraud if it gives rise to an incomplete as opposed to an affirmatively false impression." *Spector*, 178 F. Supp. 3d at 672 (internal citations and quotation marks omitted).

While the putative class is composed of individuals who purchased a Bose wireless product, this case is not about misrepresentations involving those products, only the functionality of the separate free App. *See* Compl. ¶¶ 13-16. The Complaint describes two separate sets of features included in the App: the ability to manage the headphones themselves (adjusting settings, updating firmware, etc.), and the ability to "act as a remote control" for other music apps. *Id.* Plaintiff does not allege any misrepresentations relating to the App's headphone management features. And the few disclosures concerning the remote control feature reveal the very "secret" Bose is accused of concealing—that the App accessed "the names of the music and audio tracks [users] select to play." *Id.* ¶ 24. Specifically, both the Bose website and the Apple App Store site identified in the Complaint include screenshots of the App, ***in which song title and artist information are plainly visible***.[20] In other words, those disclosures make clear that Bose, through the App, receives information about a user's currently playing music. That fact is also apparent when a user starts using the App, as the Complaint itself makes clear. *See id.* ¶ 26.

Moreover, Plaintiff has not alleged any affirmatively misleading impression created by Bose's statements about the App. The mere fact that Bose did not disclose some details regarding the configuration of its App in its general marketing materials cannot give rise to ICFA liability.

[20] *See* Landis Decl. Ex. 3; *see also Bose Connect on the App Store*, https://itunes.apple.com/us/app/bose-connect/id1046510029?mt=8 (last visited Aug. 1, 2017).

See, e.g., *Phillips v. DePaul Univ.*, 19 N.E.3d 1019, 1030 (Ill. App. Ct. 2014) (while defendant "certainly could have been more specific" about the information it disclosed, ICFA claim dismissed because "plaintiffs have identified no affirmative misrepresentation"); *Spector*, 178 F. Supp. 3d at 672 (ICFA claim dismissed because "Plaintiff has not alleged facts from which the Court can plausibly infer that Defendant [made affirmative statements] . . . such that it can be said that Defendant fraudulently omitted a material fact . . . with the intent to deceive consumers.").

Plaintiff's mix of self-serving conclusions fall far short of the level of specificity and particularity required to plead deceptive omissions. They lack the "who, what, when, where, and how" of a plausible "fraud or misrepresentation." *Thrasher-Lyon v. Illinois Farmers Ins. Co.*, 861 F. Supp. 2d 898, 908–09 (N.D. Ill. 2012) (citations and quotation marks omitted); *see also Spector*, 178 F. Supp. 3d at 671-72 ("[T]he fact that Plaintiff's claims sound in fraud tips the balance decidedly against a finding of plausibility."). Nor does the Complaint establish that fraud is the "necessary or probable inference" of Bose's alleged actions. *Spector*, 178 F. Supp. 3d at 672 (citing *People ex rel. Hartigan v. E & E Hauling, Inc.*, 607 N.E.2d 165, 174 (Ill. 1992)). To the contrary, the probable inference derived from the Complaint's non-conclusory allegations is that Bose collects song information as part of the normal and visible functioning of the App.

B. Purported Omissions Relating to the App Are Not Material to Plaintiff's Purchase of Bose Wireless Products

Plaintiff's ICFA claim separately fails because the alleged omissions are not material. To be material, a fact must be "the type of information upon which a consumer would be expected to rely in making a purchasing decision." *Rockford*, 858 N.E.2d at 62. The purchasing decision in this case concerned whether or not to purchase Bose wireless headphones. *See* Compl. ¶ 34. Bose Connect is an optional app that is not necessary to use the purchased wireless devices. And the only App feature as to which Plaintiff alleges any misrepresentation—the remote control

functionality—is itself an immaterial component of the optional App. Smartphone users can already view and control their audio using the app in which their music is playing (like Spotify) or with the physical buttons on their Bose headphones. The App's remote control feature is another way to do the exact same thing, and not something a rational consumer would rely on in deciding whether to purchase premium audio equipment.

It is a corollary to the materiality requirement that a plaintiff cannot be deceived by a statement he "has neither seen nor heard." *De Bouse v. Bayer AG*, 922 N.E.2d 309, 316 (Ill. 2009). The only specific disclosure Plaintiff alleges he saw before buying his headphones was a note on the product's packaging stating, "Enhance headphone with Bose Connect app." *See* Compl. ¶ 35. But exposure to that vague statement is not a sufficient factual basis to render plausible Plaintiff's assertion that the App was material to his decision to spend $350 on premium headphones. *See Shannon v. Boise Cascade Corp.*, 805 N.E.2d 213, 217 (Ill. 2004) ("[D]eceptive advertising cannot be the proximate cause of damages under the Act unless it actually deceives the plaintiff."); *Camasta*, 761 F.3d at 738 (to state an ICFA claim, the allegedly deceptive representation "must have been made to [plaintiff] *before* the purchase of the merchandise").

C. The Complaint Does Not Allege Cognizable Damages

Plaintiff's ICFA claim also fails because he does not allege actual damages. ICFA requires that plaintiff suffer actual pecuniary loss. *Camasta*, 761 F.3d at 739; *see also Cooney v. Chi. Pub. Schs.*, 943 N.E.2d 23, 31 (Ill. App. Ct. 2010) ("To support a[n] [ICFA] claim, actual damages must arise from purely economic injuries.") (internal quotation marks omitted). The Complaint alleges that class members suffered harm "in the form of money paid for a product they would not have purchased," or "would have paid substantially less for," had they known the optional App "would monitor, collect, transmit, and disclose [their] Media Information to a third party data miner." Compl. ¶¶ 71, 75. But there is no allegation that the class did not receive the full value of the

wireless headphones they purchased, or incurred any out-of-pocket expenses as a result of the alleged concealment. The only injury alleged stems from the use of the free App.

Even if this type of damages were cognizable, Plaintiff makes no attempt to ascribe a value to the App apart from the cost of the headphones. Plaintiff makes the speculative assertion that Bose "charged a higher price for its Bose Wireless Products relative to comparable wireless headphones," but provides no supporting facts suggesting how such price difference could be attributed to the inclusion of a free optional App. Compl. ¶ 71. This failure to disentangle the value of the fully functioning headphones from the purported privacy harms warrants dismissal. *See Phillips*, 19 N.E.3d at 1034 (plaintiff's failure to "plead any reliable mechanism for calculating the 'true' value" of a law degree in light of alleged misrepresentations about employment statistics forms independent ground for dismissal); *White v. DaimlerChrysler Corp.*, 856 N.E.2d 542, 550 (Ill. App. Ct. 2006) ("Because of his failure to be specific about the diminution of value, we do not believe he has adequately pled actual damages.").

Any emotional and privacy harms Plaintiff alleges cannot satisfy ICFA's actual damages requirement. *See Morris v. Harvey Cycle & Camper, Inc.*, 911 N.E.2d 1049, 1053 (Ill. App. Ct. 2009); *Warciak v. Nikil, Inc.*, No. 16 C 5731, 2017 WL 1093162, at *5 (N.D. Ill. Mar. 23, 2017) (denying ICFA claim alleging "injuries in the form of invasions of privacy and violations of [class members'] statutory rights" as not cognizable); *Hart v. Amazon.com, Inc.*, 191 F. Supp. 3d 809, 823 (N.D. Ill. 2016) ("injury to the intangible aspects of [a] person," "mental anguish," and the like are not actual damages under ICFA, compiling cases), *aff'd*, 845 F.3d 802 (7th Cir. 2017).

V. Plaintiff's Unjust Enrichment Claim Cannot Be Maintained

Plaintiff's unjust enrichment claim also fails for multiple reasons. First, "unjust enrichment is not a separate cause of action," but rather "'a condition that may be brought about by unlawful or improper conduct as defined by law . . . and may be redressed by a cause of action based upon

that improper conduct.'" *Pirelli Armstrong Tire Corp. Retiree Med. Benefits Trust v. Walgreen Co.*, 631 F.3d 436, 447 (7th Cir. 2011). Plaintiff's unjust enrichment claim is premised solely on the alleged misconduct underlying his deficient federal and state claims and therefore must fail as well. *See Cleary v. Philip Morris Inc.*, 656 F.3d 511, 517 (7th Cir.2011); *Siegel v. Shell Oil Co.*, 656 F.Supp.2d 825, 834 (N.D. Ill. 2009) (where plaintiff fails to establish ICFA claim, "unjust enrichment cannot serve as the basis for liability"), *aff'd*, 612 F.3d 932 (7th Cir. 2010).

Second, Plaintiff has not adequately alleged the requirements for an unjust enrichment claim. He alleges no "independent basis which establishes a duty on the part of [Bose] to act," let alone that Bose "failed to abide by that duty." *Lewis v. Lead Indus. Ass'n*, 793 N.E.2d 869, 877 (Ill. App. Ct. 2003). Nor does he allege in a non-conclusory manner what benefits Bose unjustly retained in violation of fundamental principles of justice. *See HPI Health Care Servs., Inc. v. Mt. Vernon Hosp., Inc.*, 545 N.E.2d 672 (Ill. 1989). Plaintiff received the Bose wireless headphones he purchased; Bose's receipt and retention of the purchase price was not "unjust." And Plaintiff did not by downloading the free App convey a benefit to Bose that can (let alone should) be returned.

CONCLUSION

This is not a Wiretap Act or an Eavesdropping Act case. Apart from self-serving conclusory allegations, the Complaint does not plausibly state any claims for relief. At best, Plaintiff claims Bose's privacy policy should have been clearer about the information collected or retained. But that alleged deficiency does not support the specific causes of action asserted in this Complaint. The Court should therefore grant Bose's motion to dismiss this case with prejudice.

Dated: August 3, 2017

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 August 3, 2017, I caused the foregoing to be electronically filed with the Clerk of Court using the CM/ECF system, which will send notification of such filling to the following attorneys of record:

Jay Edelson
Benjamin Thomassen
Rafey S. Balabanian
EDELSON PC
350 North LaSalle, Suite 1300
Chicago, IL 60654
jedelson@edelson.com
bthomassen@edelson.com
rbalabanian@edelson.com

/s/ Jeffrey Landis
Jeffrey Landis