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

JESSICA VASIL and CHRISTINE FARAG, individually and on behalf of a class of similarly situated individuals, Plaintiffs, v. KIIP, INC., Defendant.	)	No. 16-CV-09937 Judge John J. Tharp, Jr.

MEMORANDUM OPINION AND ORDER

In this putative class action, the plaintiffs allege that defendant Kiip, Inc. violated federal and state law by exploiting a popular fitness app, Runkeeper, to collect data from users even when they were not using the app or their phones. Kiip says the allegations do not plausibly establish a violation of federal or state law and moves to dismiss the complaint under Rule 12(b)(6). The Court agrees that the allegations in the current complaint fail to state a claim under federal law but concludes that it states a plausible claim under state law. The motion is therefore granted in part and denied in part. The plaintiffs will be permitted to replead.

I. BACKGROUND[1]

Runkeeper is a popular fitness application used to track how far and how fast users ran during a workout. Users grant Runkeeper permission to utilize their smartphones' geo-location capabilities, and in turn Runkeeper keeps track of the routes they run, their speed, their distance, and other information pertaining to their workouts. Runkeeper provides users with individually-

[1] As this is a motion to dismiss, the Court accepts all well-pleaded facts as true and construes all inferences in favor of the plaintiff. *Zemeckis v. Global Credit & Collection Corp.*, 679 F.3d 632, 634 (7th Cir. 2012).

tailored challenges and suggested workouts based on their recorded data. Users also input certain health and fitness information in the app.

Defendant Kiip, Inc. partnered with Fitnesskeeper, the creator of Runkeeper, to deliver advertisements in Runkeeper. Kiip's ads contained promotions for assorted products, and appeared when Runkeeper users completed challenges or beat their best run time. In essence, the advertisements were intended to make the user feel as though they were being rewarded. To implement this program, Kiip placed a "third-party tracker" in Runkeeper, allowing it to passively receive and actively extract data through the app. Compl. ¶ 21. Kiip collected information concerning Runkeeper users' preferences, behavior, and demographics, and then used that information to deliver specific ads to each user. Kiip's advertisements promoted large corporate brands, and it typically received a payment from those brands whenever a Runkeeper user purchased the advertised products.

Because the purpose of Kiip's third-party tracker was to display advertisements when Runkeeper users reached certain milestones, Kiip, like Runkeeper, had the ability to monitor in real-time certain events in the lives of Runkeeper users. Kiip, however, continued to collect information about Runkeeper users when they were not using the Runkeeper app, and even continued to mine data when Runkeeper users were not using their phones at all. The information Kiip gathered while Runkeeper users were not using their phones included their current geographic location, cell phone device identifiers, and "other personal information" that the complaint does not specifically identify. *Id.* ¶ 34. Kiip did not obtain consent from any Runkeeper user to collect information while the Runkeeper app or the smartphone were not in use.

In 2016, the Norwegian Consumer Council (a government agency) published a study that revealed that Kiip was collecting data from Runkeeper users even while they were not using their phones. Shortly thereafter, Fitnesskeeper ended its relationship with Kiip and issued a public apology. Two Runkeeper users, plaintiffs Jessica Vasil and Christine Farag, whose data Kiip collected via the Runkeeper app while they were not using the app, subsequently filed suit against Kiip alleging violations of the Wiretap Act, 18 U.S.C. § 2510, et seq., and the Illinois Eavesdropping Statute, 720 ILCS 5/14-1, et seq., as well as a claim for unjust enrichment. Plaintiffs seek to represent a nationwide class of individuals whose information was unlawfully mined by Kiip (as well as an Illinois-specific subclass). Kiip now moves to dismiss plaintiffs' complaint.

II. DISCUSSION

A. Wiretap Act

Kiip moves to dismiss plaintiffs' Wiretap Act claims, arguing that it did not receive the "content" of any communications while plaintiffs' phones were not in use, and that even if it did, it was a party to those communications and therefore is not liable under the Act. The Wiretap Act creates a cause of action against any entity who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral or electronic communication." 18 U.S.C. § 2511(1)(a). For practical purposes, the court will divide the allegedly intercepted communications into two categories: (1) current geo-locational data and device identifiers captured while plaintiffs were not using the Runkeeper app; and (2) geo-location and other personal data (including health and fitness information) plaintiffs provided to Runkeeper as part of their use of the app, which was later captured by Kiip during periods when the plaintiffs were not using the app. Plaintiffs have not stated a Wiretap Act claim for either category of data.

1. Current Geo-Locational Data and Device Identifiers

Plaintiffs contend that Kiip violated the Wiretap Act by collecting, without consent, their current GPS coordinates and cell phone device identifiers while they were not using the Runkeeper Act. Kiip responds by arguing that geo-locational data and device identifiers do not qualify as "contents" of a communication, and that even if they could, the specific locational and device identification data at issue here are not "content" because the plaintiffs never intended to communicate that information to anyone. Kiip has the better of the argument.

Under the Wiretap Act, an interception is defined as "the aural or other acquisition ***of the contents*** of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4) (emphasis added). "Contents," in turn, "include any information concerning the substance, purport, or meaning of that communication."

Although the Seventh Circuit has not yet addressed whether locational information constitutes the "content" of a communication under the Wiretap Act, other circuits have. The touchstone of each decision has been that the "content" of a communication is the substance that the speaker intended to communicate, and does not include automatically generated "record" data—for example, information about a telephone call's origination, length, and time. The Ninth Circuit, analyzing the text and history of the Wiretap Act and subsequent amendments, concluded that "Congress intended the words 'contents' 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, 1105-06 (9th Cir. 2014). The *Zynga* court considered whether the transmission of a Facebook user's Facebook identification number and the web address that the user was on when she clicked a particular link constituted contents. The court determined that because the data were automatically generated by

the user's web browser and were the functional equivalents of the user's name and address (and therefore analogous to return address information on a piece of mail, which is non-content "record" data), the data were not the contents of a communication.

The Third Circuit also adopted this framework in *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125 (3d Cir. 2015), noting:

> [T]he line between content and non-content information is inherently relative. If A sends a letter to B, asking him to deliver a package to C at a particular address, the contents of that letter are contents from A to B but mere non-content addressing information with respect to the delivery of the package to C. In the case of email, for example, a list of e-mail addresses sent as an attachment to an e-mail communication from one person to another are contents rather than addressing information. In short, whether an e-mail address is content or non-content information depends entirely on the circumstances.

Id. at 136-37 (quoting Wayne R. LaFave, et al., 2 Crim. Proc. § 4.4(d) (3d ed.)). In *Google*, the court determined that certain routing information, like URL addresses, can be "content" even when the information performs a routing function if the data reveal the substance of a communication. *Id*. at 138. For example, search engine URLs that reveal a user's search terms constitute content because they reveal the intended substance of the communication between the user and the search engine—*i.e.*, if a user searches for "The Few, The Proud" on Google, the resulting URL contains "the+few+the+proud," revealing the substance of the user's communication to Google.

In this case, the plaintiffs have not pled that they intended to communicate anything to anyone while they were not using their phones. In fact, the complaint repeatedly suggests the opposite, indicating that the plaintiffs never consented to the communication of their location data or device identifiers while they were not using their phones. *See, e.g.*, Compl. ¶ 35 ("Defendant designed and programmed its technology to covertly monitor app users without

their consent and without the consent of its app partners in an effort to gain further marketing information about such users."); ¶ 37 ("Defendant never obtained consent from any Runkeeper users before intercepting, monitoring, collecting, and transmitting their personal information"); ¶ 46 ("Defendant failed to obtain consent from the consumers whose information it collected. Because users were entirely unaware that their data were being extracted and transferred from their smartphone communications when the Runkeeper app was not in use—and even when their phone was not in use—there was a complete 'lack of consent regarding the collection and sharing of location data[.]").

Further, while these complaint excerpts indicate that plaintiffs never intended to communicate their geo-locational information or device identifiers to Kiip while they were not using their phones, the complaint also fails to identify to whom the plaintiffs actually intended to communicate such information. It is possible that the plaintiffs intended to communicate their location to Runkeeper whenever their phones were on by selecting settings that allowed Runkeeper to use the phone's location services even when the phone was not in use. It is also possible that the plaintiffs intended to communicate such data to their cell phone service provider by selecting phone settings that would accomplish that goal. But the complaint contains no allegations concerning who was supposed to receive, or actually did receive, plaintiffs' geo-locational data and device identifiers while plaintiffs were ***not*** using their phones or not using the Runkeeper app, or how they received such information. While the complaint repeatedly asserts that Kiip intercepted plaintiffs' communications, it does not contain facts sufficient to conclude that the allegedly intercepted data were the content of a communication.

Plaintiffs cite *Google* and *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016 (N.D. Ca. 2014), in support of their position that their geo-locational information and device identifiers constituted

the "content" of communications. But these cases are easily distinguished. The *Google* court determined that certain routing information may be the "content" of a communication if it reveals the substance of an intended communication. Here, the plaintiffs have not identified an intended communication comprising their geo-locational data and device identifiers. And in *Yahoo*, the court determined that plaintiffs properly stated that Yahoo unlawfully shared the contents of a communication when it shared with third parties package tracking numbers contained in the body of users' emails. The tracking numbers in *Yahoo* formed the substance of intentional communications between the shipping entities and Yahoo email users. No such communications have been pled here.

2. Personal Information and Prior Geo-Locational Data

Concluding that device identifiers and current geo-locational data gathered while plaintiffs were not using the Runkeeper app are not, as pled, the contents of a communication does not end the inquiry, as the parties also dispute whether the plaintiffs have pled that Kiip unlawfully captured personal data (such as health and fitness information) and geo-locational data (such as run routes) that users intentionally provided to Runkeeper. There is no dispute that such information constitutes the content of communications between plaintiffs and Runkeeper. The parties merely disagree as to whether plaintiffs pled that Kiip captured such data during periods when the plaintiffs were not using the Runkeeper app.

The court concludes that the plaintiffs have (if barely) plausibly alleged that Kiip captured, while plaintiffs' were not using the Runkeeper app, geo-locational data and personal information that they intentionally provided to Runkeeper. The complaint alleges that Kiip's "third-party tracker was intercepting their phones' electronic communications and collecting their personal information, including their geo-location and device identifiers, while they were

not using the Runkeeper app, and even when they were not using their respective cellphones." Compl. ¶ 52. It further provides that "[p]laintiffs never provided consent to [Kiip] to monitor, intercept, collect, and transmit their personal information while they were not using the Runkeeper app, and especially when they were not using their respective cellphones." *Id*. ¶ 53. Although the complaint is not a model of clarity, it repeatedly notes that plaintiffs' health and fitness information was among the vulnerable data. *See, e.g.*, *id*. ¶¶ 27, 76-78. Drawing all reasonable inferences in favor of the plaintiffs, the court concludes that plaintiffs have adequately pled that Kiip captured, while plaintiffs were not using their phones, some quantum of personal information that they had intentionally provided to Runkeeper.

Nonetheless, plaintiffs have not stated a Wiretap Act interception claim with respect to this information. Although the Seventh Circuit has twice demurred on the issue, numerous other circuits have held that under the Wiretap Act, "interceptions" of electronic communications must be contemporaneous with the communication. *See Epstein v. Epstein*, 843 F.3d 1147, 1149-50 (7th Cir. 2016) (collecting cases); *United States v. Szymuszkiewicz*, 622 F.3d 701, 705-06 (7th Cir. 2010) (same). These courts have explained that under an earlier version of the Wiretap Act, "'intercept' was defined as contemporaneous in the context of an aural communication." *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 (3d Cir. 2003) (citing *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457, 462 (5th Cir. 1994)). There is no indication that when Congress amended the Wiretap Act in 1986 to extend protection to electronic communications, it intended to change the definition of "intercept." *Id*. Indeed, while the amended Wiretap Act's definition of "wire communication" explicitly included (until further amendment in 2001) "any electronic storage of such communication," that caveat was never present in the Act's definition of "electronic communication," which "does not include . . . any

wire or oral communication." *Id.* at 113-14 (citing 18 U.S.C. §§ 2510(1), 2510(12)); *see also Steve Jackson Games*, 36 F.3d at 461-62 (holding, for the same reasons, that an "interception" of electronic communications under the Wiretap Act must be contemporaneous with the communication); *United States v. Steiger*, 318 F.3d 1039, 1048-49 (11th Cir. 2003) (same); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878-79 (9th Cir. 2002) (same). The 2001 amendment to the Wiretap Act lends further support to the conclusion that an "interception" must be contemporaneous with the communication at issue, as "[b]y eliminating storage from the definition of wire communication, Congress essentially reinstated the [original] definition of 'intercept'—acquisition contemporaneous with transmission[.]" *Konop*, 302 F.3d at 878. Consequently, the court concludes that under the Wiretap Act, "interception" of an electronic communication must be contemporaneous with the communication.

Here, to the extent that plaintiffs have adequately pled that Kiip captured, while plaintiffs were not using their phones, (1) health information and other personal information that they had intentionally provided to Runkeeper, and (2) geo-locational information they provided to Runkeeper while using the app, their interception claims are foreclosed by the Wiretap Act's contemporaneousness requirement. There are no allegations that Kiip unlawfully collected such data at the time it was communicated to Runkeeper; to the extent plaintiffs have pled that such data were unlawfully extracted, they have alleged only that the information taken without consent while it was stored in the Runkeeper app, after the communications were completed.

This is not necessarily to say that plaintiffs have no federal remedy for Kiip's extraction of data. Statutes like the Stored Communications Act, 18 U.S.C. § 2701(a), which creates a cause of action against an entity that "intentionally accesses without authorization a facility through which an electronic communication service is provided . . . and thereby obtains . . . access to a

wire or electronic communication while it is in electronic storage," and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2), which prohibits "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer," might provide recourse.[2] But as presently pled—that is, without contemporaneous interception—the Wiretap Act does not.[3]

B. Illinois Eavesdropping Statute[4]

Under the Illinois eavesdropping law, it is unlawful to "intercept[], record[], or transcribe[], in a surreptitious manner, any private electronic communication to which he or she is not a party unless he or she does so with the consent of all parties to the private electronic communication." 720 ILCS 5/14-2(a)(3). As an initial matter, with regard to present geo-locational data and device identifiers transmitted to Kiip while the plaintiffs were not using their phones, plaintiffs, as noted previously, have failed to adequately plead the existence of an

[2] The complaint does not invoke these statutes, and while it is not required to do so (complaints need not allege legal theories), the plaintiffs have not defended the viability of their claim under theories premised on these statutes. Accordingly, the Court takes no position at this juncture on the viability of a claim predicated on either the Stored Communications Act or the Computer Fraud and Abuse Act.

[3] Kiip also argues that the plaintiffs' Wiretap Act theory fails because Kiip was a party to the communication of any data from the plaintiffs. For reasons set forth below in the discussion of the plaintiffs' argument for liability under the Illinois Eavesdropping Statute, the Court concludes that Kiip was not a party within the meaning of either the Wiretap Act or the Eavesdropping Statute.

[4] Per the complaint, jurisdiction over the plaintiffs' state law theory is based on both supplemental jurisdiction (28 U.S.C. § 1367) and under the Class Action Fairness Act ("CAFA"; 28 U.S.C. § 1362(d)). Were jurisdiction premised solely on § 1367, the Court would decline supplemental jurisdiction over the state law count. *Cortezano v. Salin Bank & Tr. Co.*, 680 F.3d 936, 941 (7th Cir. 2012) ("when a court has dismissed all the federal claims in a lawsuit before trial, it should relinquish jurisdiction over supplemental state law claims rather than resolve them on the merits"). But since the requirements to establish CAFA diversity are properly alleged, the Court has independent jurisdiction over the claim and therefore addresses its merits.

electronic communication that was intercepted. Consequently, to the extent the plaintiffs rely on this data in pleading their Illinois eavesdropping claim, their claims fail.

1. Was Kiip a Party to the Communications?

Whether plaintiffs have pled an eavesdropping claim with regard to information that they intentionally provided to Runkeeper while they were using the app and which was subsequently collected by Kiip while plaintiffs were not using the app is a trickier question. The Illinois Eavesdropping Statute only prohibits interception, recording, or transcription of "private electronic communications to which [defendants are] not a party." 720 ILCS 5/14-2(a)(3). Although Illinois courts have not squarely addressed the definition of "party," the Illinois Supreme Court has suggested that a party is an entity "to whom [communications] are made or directed," *People v. Herrington*, 163 Ill.2d 507, 510-11, 645 N.E.2d 957, 958-59 (1994), which comports with the meaning of party under the Wiretap Act. *See, e.g., Google*, 806 F.3d at 143 (defining the parties to a communication as "the speaker and/or sender, and at least one intended recipient").

Kiip argues that the technical mechanism through which it acquired information constituted a direct communication between the plaintiffs and Kiip, rendering Kiip a party to the communication. Kiip bases this argument on diagrams included in the complaint and in the report of the Norwegian Consumer Counsel (which was attached to the complaint) that characterize the data flow as being a direct transmission to Kiip from the plaintiffs' phones rather than an intercepted transmission between the plaintiffs' phones and their cellular providers. But the fact that there is a direct transmission from the plaintiffs' phones to Kiip's servers does not make Kiip a "party" to a communication of the data included in that transmission. As Kiip itself acknowledges in arguing to dismiss the Wiretap Act count, there can be "communication" where

there is no "content," and there is no "content" where the speaker did not intend to communicate any information. Mem. in Support, ECF 13-2, at 5. The plaintiffs never intended, the complaint alleges, to communicate information to Kiip (or anyone else) when not using the Runkeeper app, so Kiip could not have been a party to a communication of data from the phones that Kiip engineered without the plaintiffs' knowledge.[5] Kiip cites—and the court can find—no support for the proposition that a direct, but unintended, recipient of a communication automatically becomes a party to that communication under Illinois law. Kiip's position suggests that a sophisticated eavesdropper could skirt Illinois law by developing a data collection program that results in a direct transmission from an entity to the eavesdropper, even if the entity (and its intended recipient) have no idea that a third party is collecting their data. It is doubtful, to say the least, that the Illinois legislature intended to reward technologically savvy privacy violators by insulating them from liability for unlawful eavesdropping simply because they managed to route the data directly to themselves rather than stealing it from an intended recipient.

Indeed, if the court adopted such an interpretation, it would swallow the Illinois Eavesdropping Statute's protection of electronic communications. Although it addresses the federal Wiretap Act and not Illinois law, the facts underlying the Seventh Circuit's opinion in *Szymuszkiewicz* illustrate why this is the case. The Seventh Circuit observed that virtually all

[5] This is distinct from the situation described in *United States v. Pasha*, 332 F.2d 193 (7th Cir. 1964), discussed extensively in the briefing, which concerned communications wherein a law enforcement officer impersonated a bookmaker and spoke with the bookmaker's clients over the phone. In that scenario, there is a speaker and a receiver, both of whom are parties to the conversation; the receiver simply is not who the speaker believes it is. In the present scenario, there are "speakers" (Runkeeper users) and a receiver (Runkeeper), both parties to the communication, and a surreptitious third party who has constructed an artifice to directly receive communications between the speaker and the receiver. Kiip was not a substitute for Runkeeper, à la *Pasha*; allegedly, it surreptitiously received the plaintiffs' information *in addition* to Runkeeper. This is precisely what the *Pasha* court thought was an interception of a conversation between two parties. *Id*. at 198 ("Interception connotes a situation in which by surreptitious means a third party overhears a telephone conversation between two persons.").

electronic communications between computers are now sent via "packet switching," during which the communications are disassembled into discrete packets containing bits of the communication, which are only reassembled just before the communication reaches its destination. *Szymuszkiewicz*, 622 F.3d at 705. The defendant in *Szymuszkiewicz* rigged his supervisor's email client to automatically forward to him all the messages that she received. This resulted in the emails being transmitted to the defendant in the exact same way that they were transmitted to his supervisor: the emails were disassembled into packets and routed to a server, which reassembled them and sent one copy to the defendant and one to his supervisor. *Id*. at 705. The defendant was as much a direct recipient as his supervisor—even though he had flagrantly intruded on her email account—because he received the data in the same way as, and contemporaneously with, the messages' intended recipient. Consequently, declaring direct recipients to be parties to a communication would render permissible the most common methods of intrusion, allowing the exception to swallow the rule. The court therefore rejects Kiip's argument that it was a party to plaintiffs' communications with Runkeeper because the information was sent directly to Kiip from plaintiffs' phones.[6]

2. Tracking Device

The Illinois Eavesdropping Statute also provides that "[e]lectronic communication does not include any communication from a tracking device." 720 ILCS 5/14-1(e). No court has decided whether a cell phone can be a tracking device under the statute. Predictably, then, Kiip argues that plaintiffs' phones are tracking devices because they tracked the plaintiffs, while the

[6] Although the plaintiffs do not plead or argue that Kiip unlawfully captured their data while they were using the Runkeeper app, the complaint does not affirmatively plead facts indicating with certainty that Kiip was a party to *any* communications between plaintiffs and Runkeeper. Indeed, the complaint suggests the opposite, noting that "[p]laintiffs were unaware that [Kiip's] third-party tracker was integrated with the Runkeeper app and that it was intercepting their communications and collecting their information." Compl. ¶ 51.

plaintiffs maintain that a multi-functional device does not automatically become a tracking device simply because it performs tracking functions. The plaintiffs argue that the court should read the Illinois Eavesdropping Statute *in pari materia* with federal surveillance laws, under which, they assert, cell phones are not tracking devices even when they perform tracking functions. Lower federal courts, however, are divided as to whether cell phones become tracking devices, for purposes of federal wiretapping laws, when they perform tracking functions. *Compare In re Order Authorizing Prospective and Continuous Release of Cell Site Location Records*, 31 F. Supp. 3d 889, 897 (S.D. Tex. 2014) (concluding that a cell phone is a tracking device under federal wiretapping laws when it performs tracking functions), *and In re Application of United States for an Order Relating to Target Phone 2*, 733 F. Supp. 2d 939, 943 (N.D. Ill. 2009) (same), *with In re Smartphone Geolocation Data Application*, 977 F. Supp. 2d 129, 149-150 (E.D.N.Y. 2013) (holding that a cell phone is not a tracking device), *and United States v. Ackies*, No. 2:16-cr-20-GZS, 2017 WL 3184178, at *11 (D. Me. July 26, 2017) (same).

In addressing a question of state law, the task of a federal court "is to determine how the state's highest court would rule. [Federal courts] base our predictions on the decisions of the state's highest court, and we consider decisions of intermediate appellate courts unless there is good reason to doubt the state's highest court would agree with them." *Anicich v. Home Depot U.S.A., Inc.*, 852 F.3d 643, 648–49 (7th Cir. 2017). But here there are no such decisions; no court has yet parsed the meaning of "tracking device" under the Illinois Eavesdropping Statute. Given the dearth of Illinois precedent, it is appropriate to look to the federal court decisions addressing this question. Illinois courts subscribe to the proposition that, "[a]lthough the decisions of foreign courts are not binding, the use of foreign decisions as persuasive authority is appropriate where

Illinois authority on point is lacking or absent." *In re Estate of Nina L. ex rel. Howerton*, 2015 IL App (1st) 152223, ¶ 14, 41 N.E.3d 930, 933 (internal quotation marks and citations omitted).

Turning, then, to the cases addressing the meaning of "tracking device" under the analogous federal statute, 18 U.S.C. § 3117, the court is persuaded that a cell phone is a tracking device to the extent it performs tracking functions. As an initial matter, it is nonsensical to say that a device capable of tracking an individual is not a tracking device simply because it performs other functions. As the Supreme Court has recognized, "the term 'cell phone' is itself misleading shorthand: many of these devices are in fact minicomputers that also have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." *Riley v. California*, 134 S. Ct. 2473, 2489 (2014). If a statute used the words "cell phone," courts would deprive the statute of all meaning by concluding that it only applied to devices whose sole—or even primary—use was as a telephone. Consequently, that a cell phone has dozens of functions aside from tracking does not mean a cell phone is not a tracking device. Moreover, interpreting "tracking device" to include only items that have no function other than tracking would exclude many, if not most, devices used to track individuals, essentially mooting the Statute's tracking device carve out. *See Cell Site Location Records*, 31 F. Supp. 3d at 899. Indeed, "multiple standards for tracking technologies . . . would seem to accomplish very little . . . other than to generate confusion and opportunity for manipulation." *Id*.

The case on which plaintiffs rely, *Smartphone Geolocation Data*, is unpersuasive. In that case, the court was concerned that "construing 'tracking device' to encompass a cell phone" was "illogical and unworkable" because "an individual travelling by bicycle, leaving tire tracks in a muddy field; an automobile taillight, which could permit officers to follow a car at night; or the

transmitter of a pirate radio station, the signal from which may be located via triangulation, would each constitute" a tracking device. 977 F. Supp. 2d at 150. But this concern (and its application to this case) ignores the context of the term "tracking device"—a constituent element of wiretapping statutes—in federal and Illinois law. And that context divines the simple limiting principle that a "tracking device" permits an individual to be tracked remotely, and not exclusively "through direct observation." *Cell Site Location Records*, 31 F. Supp. 3d at 899 n. 49. A cell phone and a pirate radio, then, can be tracking devices, because they permit the user to be tracked from afar. In other words, deeming a cell phone to be a tracking device does not require acquiescence in the absurdity that a bicycle, too, is a tracking device under state or federal wiretapping laws.

Nonetheless, it is equally specious to say that because a cell phone has tracking capabilities, Illinois law permits unlimited interception of any content that emanates therefrom. Admittedly, a literal reading of the Illinois Eavesdropping Statute might give the impression that *anything* sent from a tracking device is excluded from the definition of an "electronic communication": "Electronic communication does not include any communication from a tracking device." 720 ILCS 5/14-1(e). But "where a plain or literal reading of a statute produces absurd results, the literal reading should yield." *People v. Hanna*, 207 Ill.2d 486, 498, 800 N.E.2d 1201, 1207 (Ill. 2003). As the Supreme Court recognized in *Riley*, "[p]rior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception." 134 S. Ct. at 2490. To conclude that the Illinois Eavesdropping Act excludes protection for all communications from cell phones—which often concern the most

intimate and private details in users' lives—would give far too great an effect to the tracking device exclusion.

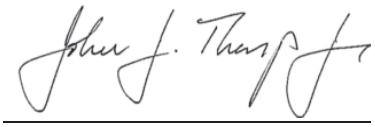
Consequently, the court concludes that under the Illinois Eavesdropping Statute, a cell phone is a tracking device to the extent it performs tracking functions. Operationalizing that framework in this case, plaintiffs' claim under the eavesdropping statute fails to the extent it concerns the collection of any geo-locational data. But to the extent it concerns information that the plaintiffs intentionally provided to Runkeeper other than geo-locational data, plaintiffs may proceed.

C. Unjust Enrichment

Finally, Kiip argues that the plaintiffs' unjust enrichment claims should be dismissed because Illinois does not recognize a standalone unjust enrichment claim, untethered from any other violation of the law. The plaintiffs respond that Illinois law permits such claims. The Seventh Circuit explained, albeit in dicta, its view of Illinois' jumbled unjust enrichment jurisprudence in *Cleary v. Philip Morris Inc.*, 656 F.3d 511, 517 (7th Cir. 2011). Surveying Illinois unjust enrichment cases, the Seventh Circuit explained that although unjust enrichment may in some circumstances be a freestanding claim, "if an unjust enrichment claim rests on the same improper conduct alleged in another claim, then the unjust enrichment claim will be tied to this related claim—and, of course, unjust enrichment will stand or fall with the related claim." *Id*. Here, the same conduct that underlies plaintiffs' unjust enrichment claims also underlies their Wiretap Act and Illinois Eavesdropping Statute claims. Plaintiffs' unjust enrichment claim, therefore, may proceed only to the extent their Illinois Eavesdropping Statute claim proceeds.

* * *

For the foregoing reasons, Kiip's motion to dismiss is granted as to plaintiffs' Wiretap Act claims, and granted in part and denied in part as to plaintiffs' state law claims. The dismissals are without prejudice.



Dated: March 5, 2018

John J. Tharp, Jr.
United States District Judge