IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

MICHAEL PETERSON, et al., Plaintiffs, v. AARON'S, INC., et al., Defendants.	CIVIL ACTION FILE NO. 1:14-CV-1919-TWT

OPINION AND ORDER

This is a tort action in which the Plaintiffs Michael Peterson and Matthew Lyons allege that the Defendant Aspen Way Enterprises, Inc., a franchisee of the Defendant Aaron's, Inc., unlawfully accessed their computers from a remote location and collected private information stored therein. It is before the Court on the Defendant Aaron's, Inc.'s Motion for Summary Judgment [Doc. 144] and the Defendant Aspen Way Enterprises, Inc.'s Motion for Summary Judgment [Doc. 152]. For the reasons set forth below, Aaron's Motion for Summary Judgment [Doc. 144] is GRANTED and Aspen Way's Motion for Summary Judgment [Doc. 152] is GRANTED in part and DENIED in part.

I. Background

The Defendant Aaron's franchises independently-owned stores that are in the business of, *inter alia*, selling and leasing consumer electronics.[1] The Plaintiff Matthew Lyons – an Oklahoma resident – entered into a lease agreement to rent laptop computers from Aspen Way – a Montana-based franchisee of Aaron's.[2] The Plaintiffs contend that Mr. Lyons entered into the lease agreement on behalf of his law firm, Peterson & Lyons, LLC. The Plaintiff Michael Peterson – a Colorado resident – was the other named partner at the law firm, which is now defunct.[3]

The Plaintiffs allege that Aspen Way remotely accessed their computers and captured private information. They contend that Aspen Way was able to obtain their private information through a spyware software program named PC Rental Agent ("PCRA"), which was installed on their computers without their consent.[4] Aspen Way directly licensed PCRA from a third-party developer, and its primary function was to locate and shut down a computer in the event of theft or missed payment.[5]

---

[1] Def.'s Stat. of Undisputed Mat. Facts ¶ 3 (hereinafter "Aaron's SOF").

[2] Pls.' Stat. of Undisputed Mat. Facts ¶ 7 (hereinafter "Plaintiffs' SOF"); Aaron's SOF ¶ 39.

[3] Plaintiffs' SOF ¶ 7; Aaron's SOF ¶ 40.

[4] Aaron's SOF ¶ 5.

[5] Id. at ¶ 10; Plaintiffs' SOF ¶ 2.

The software also had an optional function called "Detective Mode." When activated, Detective Mode could collect screen shots, keystrokes, and webcam images from the computer.[6] On October 21, 2010, Aspen Way installed and activated Detective Mode on Lyons' rented computer, and continued to use Detective Mode until February 7, 2011.[7] Aaron's, meanwhile, contends that it was unaware of Aspen Way's use of Detective Mode whatsoever until May 2011.[8]

The Plaintiffs originally filed their Complaint as a class action against both Aaron's and Aspen Way, alleging common law invasion of privacy, aiding and abetting, unjust enrichment, and violations of the Georgia Computer Systems Protection Act ("GCSPA"). Eventually the Court dismissed the unjust enrichment and GCSPA claims,[9] and denied the Plaintiffs' Motion to Certify.[10] Aaron's now moves for summary judgment on the Plaintiffs' single claim against it for aiding and abetting Aspen Way's alleged intrusion upon seclusion.

---

6 Aaron's SOF ¶ 17.

7 Aaron's SOF ¶ 38.

8 Id. at ¶ 30.

9 See Order Granting in Part and Denying in Part Defs.' Motions to Dismiss [Doc. 42] and Order Granting Defs.' Motions to Dismiss [Doc. 61].

10 Order Denying Class Cert. [Doc. 138].

II. Legal Standard

Summary judgment is appropriate only when the pleadings, depositions, and affidavits submitted by the parties show no genuine issue of material fact exists and that the movant is entitled to judgment as a matter of law.[11] The court should view the evidence and any inferences that may be drawn in the light most favorable to the nonmovant.[12] The party seeking summary judgment must first identify grounds to show the absence of a genuine issue of material fact.[13] The burden then shifts to the nonmovant, who must go beyond the pleadings and present affirmative evidence to show that a genuine issue of material fact does exist.[14] "A mere 'scintilla' of evidence supporting the opposing party's position will not suffice; there must be a sufficient showing that the jury could reasonably find for that party."[15]

---

11 FED. R. CIV. P. 56(a).

12 Adickes v. S.H. Kress & Co., 398 U.S. 144, 158-59 (1970).

13 Celotex Corp. v. Catrett, 477 U.S. 317, 323-24 (1986).

14 Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 257 (1986).

15 Walker v. Darby, 911 F.2d 1573, 1577 (11th Cir. 1990).

III. Discussion

A. Standing

Prerequisite to any action, a plaintiff must show that he has standing to bring a claim. There are three elements to standing: "First, [the plaintiff] must show that he has suffered an 'injury-in-fact.' Second, the plaintiff must demonstrate a causal connection between the asserted injury-in-fact and the challenged action of the defendant. Third, the plaintiff must show that 'the injury will be redressed by a favorable decision.'"[16]

Aspen Way challenges the Plaintiffs' standing with regard to the first required element: injury. The Supreme Court has said that a plaintiff must show "he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'"[17] For reasons similar to those contained in the Court's previous Order,[18] it is clear that at least one plaintiff, Michael Peterson, has not met this standard. Peterson was not on

---

[16] Shotz v. Cates, 256 F.3d 1077, 1081 (11th Cir. 2001) (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992)).

[17] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1543 (2016) (quoting Lujan, 504 U.S. at 560).

[18] Order Denying Mot. to Cert. Class at 6-8 [Doc. 138].

the lease, Lyons was.[19] The Plaintiffs have failed to demonstrate any "legally protected interest" Peterson had in the laptop at all.

Regarding Lyons, Aspen Way argues that simply because his rights were violated does not necessarily mean he suffered an injury. In support of its argument, Aspen Way cites three cases: Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1543 (2016), Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011), and Storm v. Paytime, Inc., 90 F. Supp. 3d 359 (M.D. Pa. 2015). All three cases, however, are different from this case in at least one significant respect: the nature of the right violated.

In Spokeo, the defendant was a technology company that operated a search engine which allowed users to find out publicly available personal information about individuals.[20] The plaintiff eventually discovered that his personal search results contained inaccurate information, which he argued violated the Fair Credit Reporting Act of 1970 ("FCRA").[21] The Supreme Court found that the plaintiff did not show enough of a concrete injury to have standing for two reasons. First, the Court said that bare procedural violations of the FCRA – like a failure to provide notice – do not

---

[19] See Def.'s Stat. of Undisputed Mat. Facts ¶ 1. The parties disagree about whether this is the particular lease agreement signed by both parties. However, they both agree that Lyons was the one who signed an agreement, not Peterson.

[20] Spokeo, 136 S. Ct. at 1543.

[21] Id.

necessarily result in harm.[22] "For example, even if a consumer reporting agency fails to provide the required notice to a user of the agency's consumer information, that information regardless may be entirely accurate."[23] Second, using the example of an incorrect zip code listing, the Court said that "not all inaccuracies cause harm or present any material risk of harm."[24] In other words, the Court merely reiterated the truism that violations of rights do not necessarily entail actual harm.

The other two cases, Reilly and Storm, were data breach cases in which the plaintiffs feared that their identities were stolen after their personal information had been exposed in a data breach. The courts in those cases found that the fear of future harm did not necessarily give them standing. In the words of the Reilly court, "[u]nless and until [identity theft occurs], Appellants have not suffered any injury; there has been no misuse of the information, and thus, no harm."[25]

By contrast, the rights violated in those cases are substantially different than that violated in this case. In Spokeo, it was the plaintiff's right to have certain procedures followed under the FCRA. In the data breach cases, it was the plaintiffs'

---

22 Id. at 1550.

23 Id.

24 Id.

25 Reilly, 664 F.3d at 42.

right to due care on the part of the defendants. In this case, however, it was Lyons' right to privacy that was violated. A violation of the right to privacy necessarily entails an injury. If a voyeur installs a camera in a person's home, or opens their mail, the victim suffers a harm as soon as their privacy is violated. That remains true whether or not the tortfeasor does anything with the information collected; indeed, it remains true whether the victim knows about it or not.[26]

In this case, as soon as Aspen Way activated Detective Mode and screenshots were taken and keystrokes logged, Lyons suffered a harm. And unlike plaintiffs in other data collection cases,[27] Lyons did not consent to the collection of his data, nor did he give it willingly to Aspen Way.[28] Lyons has sufficiently demonstrated that he suffered an injury-in-fact and therefore has standing to pursue his claims against the Defendants.

---

[26] Of course, the victim could not bring a claim unless they knew about it, but the violation and the harm would still have occurred.

[27] See Vigil v. Take-Two Interactive Software, Inc., 235 F. Supp. 3d 499, 516-18 (S.D.N.Y. 2017) (finding that plaintiffs did not suffer injury-in-fact when video game scanned and retained their faces because they had consented to have their faces scanned).

[28] Pls.' Stat. of Add'l Material Facts ¶ 11 [Doc. 159-1].

B. Choice of Law

This case is before the Court based on diversity jurisdiction. The Court therefore looks to Georgia's choice of law requirements to determine the appropriate rules of decision.[29] Georgia follows the traditional approach of *lex loci delecti* in tort cases, which generally applies the substantive law of the state where the last event occurred necessary to make an actor liable for the alleged tort.[30] Usually, this means that the "law of the place of the injury governs rather than the law of the place of the tortious acts allegedly causing the injury."[31]

Lyons accuses Aspen Way of intruding upon his seclusion, and Aaron's of aiding and abetting that intrusion. The injury is to his privacy, and the nature of the right to privacy being what it is, it follows that any injury that occurred to Lyons occurred wherever he was located at the time of the injury.[32] At the time Aspen Way

---

[29] Frank Briscoe Co., Inc. v. Ga. Sprinkler Co., Inc., 713 F.2d 1500, 1503 (11th Cir.1983) ("A federal court faced with the choice of law issue must look for its resolution to the choice of law rules of the forum state.").

[30] Dowis v. Mud Slingers, Inc., 279 Ga. 808, 816 (2005); Int'l Bus. Machines Corp. v. Kemp, 244 Ga. App. 638, 640 (2000).

[31] Mullins v. M.G.D. Graphics Sys. Grp., 867 F. Supp. 1578, 1581 (N.D. Ga. 1994).

[32] See Restatement (Second) of Conflict of Laws § 153 (1971). Though the Restatement (Second) of Conflict of Laws operates a different choice of law analysis than Georgia does, it is illustrative of the fact that the injury to a right to privacy claim

accessed his computer, Lyons was residing in Oklahoma. As such, the Court will apply Oklahoma law.[33]

C. Intrusion Upon Seclusion Claim Against Aspen Way

Aspen Way moves for summary judgment on Lyons' intrusion upon seclusion claim. Oklahoma has adopted the Restatement (Second) of Torts for claims of intrusion upon seclusion.[34] Section 652B of the Restatement (Second) of Torts defines intrusion upon seclusion as "intentionally intrud[ing], physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns...if the intrusion would be highly offensive to a reasonable person." To sustain the tort claim, the Plaintiff must therefore prove two elements: (1) an intrusion upon his privacy, and (2) that a reasonable person would find it highly offensive.

---

occurs wherever the plaintiff is located. See also Bullard v. MRA Holding, LLC, 890 F. Supp. 2d 1323, 1327 (N.D. Ga. 2012) (applying the law of the plaintiff's residence where her likeness was captured and disseminated in other states).

[33] The evidence in this case suggests Lyons was in Oklahoma during the entirety of the active use of Detective Mode on the computer. See Def.'s Mot. for Summ. J., Ex. C at 15 [Doc. 153-2]. The Court declines to address what law would apply in a similar situation if the Plaintiff had resided in multiple states.

[34] See McCormack v. Okla. Publ'g Co., 613 P.2d 737, 739 (Okla. 1980).

1. Reasonable Expectation of Privacy

Aspen Way first argues that it did not intrude upon Lyons' privacy because Lyons did not have a reasonable expectation of privacy in the computer. In particular, Aspen Way points to the fact that the computer was leased, that it was used for business and not personal reasons, and that Lyons was in default on his payments. None of these reasons, however, means that Lyons did not have a reasonable expectation of privacy in his use of the computer.

Though the property rights of lessees and owners differ in many respects, they do not differ in their right to privacy. A lessee in possession of property expects reasonably similar levels of privacy as an owner.[35] So the fact that Lyons was a lessee, and not the owner of the property, does not on its own mean he lacked a reasonable expectation of privacy.

Nor is that expectation undermined by the fact that he used the computer for business purposes. It is true that, generally speaking, employees have less privacy expectations in their work computers than in their personal computers.[36] But the cases

---

[35] See Sundheim v. Bd. of Cty. Comm'rs of Douglas Cty., 904 P.2d 1337, 1350 (Colo. App. 1995), aff'd, 926 P.2d 545 (Colo. 1996) (stating that searches of leased property implicates the lessee's right to privacy, not the owner's).

[36] See New York v. Burger, 482 U.S. 691, 700 (1987) ("An expectation of privacy in commercial premises, however, is different from, and indeed less than, a

which state that rule are generally dealing with either employer-employee relationships or searches by the government.[37] This case, by contrast, is not between Lyons and his firm. Indeed, it is not the firm's computer at all; Lyons was the lessee. The fact that he allowed others to use his leased computer may reduce his expectation of privacy with regard to those users, but it does not diminish his privacy rights vis-a-vis a third party. To adopt the Defendant's approach would mean that granting access to some people necessarily means granting access to all people. Such an outcome would be absurd.

Aspen Way's final argument suggests that Lyons lost any expectation of privacy in the computer because he defaulted in his payments on the lease, but even this does not necessarily excuse all of Aspen Way's alleged actions. First, there seems

---

similar expectation in an individual's home.").

[37] See, e.g., id. (government search); Thygeson v. U.S. Bancorp, No. CV-03-467-ST, 2004 WL 2066746, at *18 (D. Or. Sept. 15, 2004) (employer search). There are limits, however, to how much an employer can search. See Fischer v. Mt. Olive Lutheran Church, 207 F. Supp. 2d 914 (W.D. Wis. 2002) (finding dispute of material issue of fact regarding whether pastor had reasonable expectation of privacy in his personal email account accessed on his work computer); Stengart v. Loving Care Agency, Inc., 990 A.2d 650 (N. J. S. 2010) (finding that employee had a reasonable expectation of privacy in her emails sent from her personal email account to an attorney on a work computer).

to be a dispute about if and when Lyons was actually in default.[38] That dispute alone demonstrates that there is a genuine issue about a material fact, for if Lyons was never in default (or was only in default for a portion of the time Detective Mode was activated), then Lyons certainly had a reasonable expectation of privacy regarding his use of the computer. But even assuming *arguendo* that Lyons was in default for the entirety of the time Detective Mode was activated, that is still not necessarily enough to show that he abandoned any expectation of privacy. Aspen Way argues that because Colorado law allowed it to take immediate possession of the computer once Lyons defaulted, Lyons no longer had a reasonable expectation of privacy in the contents of the computer. In support, Aspen Way cites a dissent in People v. Sotelo, 336 P.3d 188 (Colo. 2014)[39] which surveyed cases in other jurisdictions that found there was no reasonable expectation of privacy in personal effects contained in items

---

[38] See Pls.' Resp. to Def.'s Stat. of Undisputed Mat. Facts ¶ 26 [Doc. 159-1].

[39] Aspen Way actually refers to this dissent as the majority opinion. See Def.'s Mot. for Summ. J. at 18-19 [Doc. 152]. The Court will assume that this was merely a mistake rather than a deliberate obfuscation.

such as a stolen car or a fraudulently obtained computer.[40] But Sotelo actually undermines Aspen Way's argument for two reasons.

First, all three of those cases surveyed by the Sotelo dissent are substantively different than this case because of the defendants' states of mind. The defendants in those cases were thieves. By contrast, Lyons was a lessee in default. Thieves and defaulting lessees have qualitatively different states of mind with regard to the property, and therefore different expectations of privacy. A thief knows that he has no claim to the property in question. A lessee, on the other hand, may not even be aware that he is in default. Checks may have gotten lost in the mail or notices may never have been sent.[41]

Second, the majority opinion in Sotelo actually supports Lyons' position. The defendant in Sotelo had been pulled over in a rental car she was not authorized to

---

[40] See United States v. White, 504 Fed. Appx. 168, 172 (3d Cir. 2012) (plaintiff lacked standing to challenge search of his backpack and his locked box that were found inside stolen car he was driving); United States v. Hargrove, 647 F.2d 411, 412 (4th Cir. 1981) (plaintiff lacked reasonable expectation of privacy in stolen vehicle); United States v. Caymen, 404 F.3d 1196, 1200 (9th Cir. 2005) (plaintiff had no legitimate expectation of privacy in the contents of a computer he fraudulently obtained using a stolen credit card).

[41] That is not to say that there is not some point at which a delinquent lessee effectively has the same culpability as a thief. The Court merely finds that that is not the case here.

drive.[42] While searching the car, the officer found gift-wrapped boxes in the car and asked to search them.[43] After the defendant refused, the officer eventually obtained a warrant to search the boxes, but not until hours after the original stop.[44] The search discovered that the gift boxes were actually disguising vacuum sealed bags filled with marijuana.[45] The Sotelo court eventually said that while the defendant had no reasonable expectation of privacy in the car itself, given that she was unauthorized to drive it, she did have a legitimate expectation of privacy in the gift-wrapped packages because "society would recognize Sotelo's expectation of privacy in the gift-wrapped packages as reasonable...[i]ndeed, the reason packages are gift-wrapped is to conceal their contents."[46] Likewise, people protect their computers and digital files with passwords because they want to protect them from the view of others. If anything, therefore, Sotelo suggests that Lyons too had a legitimate expectation of privacy in his files, keystrokes, and use of the internet despite the fact that he was in default on the computer he was using to accomplish those tasks.

---

42 Sotelo, 336 P.3d at 190.

43 Id.

44 Id. at 190-91.

45 Id. at 191.

46 Id.

Aspen Way's authority to repossess the computer makes no difference. Being the true owner did not entitle Aspen Way to spy on the person it was trying to repossess the computer from. Lyons' default certainly would have allowed Aspen Way to shut down the computer, or maybe even to use location tracking software in an effort to repossess it. But the other aspects of Detective Mode, the capturing of keystrokes and screenshots, serve no legitimate purpose in repossessing the computer. Defaulting on a rental payment may allow a landlord to repossess a home from a tenant, but it does not allow him to set up cameras to spy on the activities of the tenants. Likewise, if a company defaults on its commercial lease, the landlord may also repossess the property, but the landlord may not break in without the company's knowledge and start going through its files. In other words, wrongdoing vitiates privacy expectations only to the extent of the wrongdoing. It does not eliminate privacy expectations altogether.[47]

The methods used for repossession must be reasonably related to their end. In this way, the line between reasonable and unreasonable expectations of privacy in the default context is largely influenced by whether the means of repossession are

---

[47] See Sotelo, 336 P.3d at 201 (Boatright, J. dissenting) ("As these cases illustrate, the amount of privacy a person can reasonably expect in items within a car depends, in part, on how she acquired possession of the vehicle.").

themselves reasonable or not. The Court finds that shutting down the computer or using GPS tracking would have been reasonably related to Aspen Way's goal of repossessing the computer, and if Lyons was in default, he should have expected Aspen Way would take such action. Capturing keystrokes and screenshots, however, served no legitimate purpose in repossessing the computer. Therefore, it would be possible for a jury to find that Lyons still had a reasonable expectation of privacy which Aspen Way violated.

2. Offensive Nature of the Intrusion

Aspen Way then argues that even if Lyons had a reasonable expectation of privacy in the computer, it still did not intrude upon that privacy in a way that constituted tortious conduct. Under Oklahoma law, an intrusion upon a person's privacy is tortious only "if the intrusion would be highly offensive to a reasonable person."[48] As alluded to above, the offensiveness of the intrusion is often directly tied to how reasonable the expectation of privacy is. However, the degree of offensiveness of the conduct is generally a question for the jury.[49] In this case, the Court finds that

---

[48] Restatement (Second) of Torts § 652B.

[49] See, e.g., Hall v. Harleysville Ins. Co., 896 F. Supp. 478 (E.D. Pa. 1995); Miller v. Nat'l Broad. Co., 187 Cal. App. 3d 1463, 1483 (Ct. App. 1986).

there is sufficient evidence such that a jury could find Aspen Way's use of Detective Mode to be highly offensive to a reasonable person.

D. Aiding and Abetting Claim Against Aaron's

Oklahoma courts have not directly stated what constitutes aiding and abetting in the context of an intrusion upon seclusion tort. However, in other aiding and abetting contexts, Oklahoma follows the Second Restatement approach. Section 876 of the Restatement (Second) of Torts states that one can be liable for aiding and abetting if he "*knows* that the other's conduct constitutes a breach of duty *and* gives substantial assistance or encouragement to the other so to conduct himself..."[50] Both knowledge and substantial assistance are required elements for an aiding and abetting action. Because there is no evidence to suggest Aaron's knew about Aspen Way's tortious conduct, Aaron's is entitled to summary judgment.

1. Knowledge

Though knowledge is a required element of any aiding and abetting action in Oklahoma, Oklahoma courts have not squarely addressed the issue of what level of knowledge is required. The majority of other jurisdictions relying on the Second Restatement, however, have held that a defendant must have actual knowledge that

---

[50] Restatement (Second) of Torts § 876(b) (emphasis added). There are other potential avenues to liability under § 876, but they are not relevant to this case.

the tortfeasor's conduct was tortious.[51] This means that a defendant must at least "have a general awareness of its role in the other's tortious conduct."[52] Actual knowledge can be proven by circumstantial evidence.[53] But "reckless or negligent conduct" is not sufficient, nor is mere suspicion or "red flags."[54] That means that any circumstantial evidence used "must demonstrate that the aider and abettor actually knew of the underlying wrongs committed."[55] Of course, having a general awareness of one's role in wrongful conduct necessarily presupposes that one had any knowledge of the tortfeasor's conduct in the first place.

---

[51] See Robinson v. Spittler, 191 Okla. 278, 129 P.2d 181, 184 (1942) (finding defendant liable for aiding and abetting tortfeasor's trespass when he had "full knowledge" that he did not own the property). See also Sender v. Mann, 423 F. Supp. 2d 1155, 1176 (D. Colo. 2006) (citing Colorado tort law, which also adopts the Second Restatement).

[52] Aetna Cas. & Sur. Co. v. Leahey Const. Co., 219 F.3d 519, 534 (6th Cir. 2000).

[53] Id. at 535.

[54] See Sender, 423 F. Supp. 2d at 1176 ("...aiding and abetting requires actual knowledge and is not satisfied by reckless or negligent conduct."); Maruho Co. v. Miles, Inc., 13 F.3d 6, 10 (1st Cir. 1993) (mere suspicion insufficient to show that it is aware of "its substantial, supporting role in an unlawful enterprise." Actual knowledge required for liability); El Camino Res. Ltd. v. Huntington Nat. Bank, 712 F.3d 917, 922 (6th Cir. 2013) (interpreting Michigan law and determining that actual knowledge is required).

[55] Perlman v. Wells Fargo Bank, N.A., 559 F. App'x 988, 993 (11th Cir. 2014).

The Plaintiffs argue the Court can infer that Aaron's knew of Aspen Way's use of Detective Mode because it knew Detective Mode was intrusive, it knew at least some of its franchisees were using Detective Mode as early as September 2, 2010 (prior to it being installed and activated on Lyons' computer),[56] and it could have quickly told all of its franchisees to stop using Detective Mode and avoided any harm to the Plaintiffs.[57] These arguments fail to prove the type of knowledge required for aiding and abetting for two reasons.

First, the fact that Aaron's knew that *some* of its franchisees were using Detective Mode does not mean that Aaron's knew that *Aspen Way* was using Detective Mode. In order to be found liable for aiding and abetting Aspen Way, Aaron's must have known (or at least been generally aware of) its role in *Aspen Way's* tortious conduct, not the potential conduct of another. The Plaintiffs respond by arguing that knowledge of one franchisee's conduct should be extended to include knowledge of all franchisees' conduct because Aaron's treated its "franchisee community" the same.[58] But such an approach would be nonsensical. The fact that

---

[56] The Plaintiffs also argue that Aaron's could have specifically discovered Aspen Way's use of Detective Mode earlier had it simply reviewed its own email system.

[57] See Pls.' Resp. to Def.'s Mot. for Summ. J. at 5-6, 19.

[58] Id. at 20 n.2.

Phillip knows Carlton came home late at 11:00 p.m. does not mean he knows Will came home at 1:00 a.m., despite his uniform policy that both boys be home by 10:00 p.m. Knowledge of one franchisee's wrongdoing can lead to the inference that Aaron's knew that some of its franchisees were using Detective Mode, but it cannot reasonably lead to the inference that Aaron's knew of Aspen Way's specific use.

Likewise, it is not possible to infer that because Aaron's knew Aspen Way was using PCRA, and because it knew PCRA had the ability to have Detective Mode enabled, that it necessarily knew Aspen Way was using Detective Mode. As the Court has previously held, PCRA and Detective Mode are separate pieces of software.[59] PCRA on its own is not tortious. Only when Detective Mode is activated, which requires a separate, independent step, does the software potentially cross the line. Thus, even if Aaron's was aware that PCRA had the *potential* to be tortious – in the event of a user activating Detective Mode – it cannot necessarily be said to have actual knowledge that Aspen Way did so.

Second, the Plaintiffs essentially argue that Aaron's could have or should have done more to investigate. It may very well be the case that Aaron's could have or even should have immediately told all of its franchisees to stop using Detective Mode once

---

[59] Order Denying Mot. to Cert. Class at 24 [Doc. 138].

Aaron's learned of its capabilities. It may also be the case that Aaron's could have discovered Aspen Way's use of Detective Mode had it reviewed its email servers. But while these arguments might sustain a theory of negligence or recklessness, they are insufficient for finding actual knowledge.

Ultimately, the Plaintiffs have failed to bring forward any evidence to suggest that Aaron's knew anything more than that some of its franchisees were using Detective Mode. This is not enough for a jury to infer that Aaron's had actual knowledge of Aspen Way's use of Detective Mode. For these reasons, Aaron's is entitled to summary judgment regarding the Plaintiffs' sole remaining claim of aiding and abetting.

E. The Plaintiffs' Rule 56(d) Declaration

In their Brief in Response, the Plaintiffs argue pursuant to Rule 56(d) that they do not have sufficient information essential to its opposition. Under Rule 56(d), the non-moving party may show by affidavit or declaration that it "cannot present facts essential to justify its opposition," after which the court may "(1) defer considering the motion or deny it; (2) allow time to obtain affidavits or declarations or to take discovery; or (3) issue any other appropriate order."[60]

---

[60] Fed. R. Civ. P. 56(d).

In particular, the Plaintiffs seek access to redacted email communications between Aaron's top executives and its legal department for the purpose of "verify[ing] that Aaron's had no knowledge that its franchisee' [sic] use of Detective Mode could be considered tortious."[61] The Eleventh Circuit has held that parties may impliedly waive attorney-client privilege if the party asserting the privilege "injects into the case an issue that in fairness requires an examination of otherwise protected communications."[62]

The Plaintiffs argue that Aaron's injected the issue of its knowledge of Detective Mode's abilities into the case, and thus the emails should be made available. The problem with the Plaintiffs' argument is that they misunderstand what the issue is. The issue here is not whether Aaron's knew Detective Mode was invasive. The record is clear that it did. Rather, the question is whether Aaron's knew that Aspen Way was using Detective Mode. The Plaintiffs have failed to show how the communications in question would be enlightening as to that issue. For that reason, the Court declines to pierce attorney-client privilege.

IV. Conclusion

---

[61] Pls.' Resp. to Aaron's Mot. for Summ. J. at 22 [Doc. 160].

[62] Cox v. Adm'r U.S. Steel & Carnegie, 17 F.3d 1386, 1419 (11th Cir.), *opinion modified on reh'g*, 30 F.3d 1347 (11th Cir. 1994).

For the reasons stated above, the Defendant Aaron's Motion for Summary Judgment [Doc. 144] is GRANTED. Meanwhile, the Defendant Aspen Way's Motion for Summary Judgment [Doc. 152] is GRANTED in part as it relates to the Plaintiff Peterson's claims, but DENIED in part as it relates to the Plaintiff Lyons' claims for intrusion upon seclusion.

SO ORDERED, this 3 day of October, 2017.

/s/Thomas W. Thrash
THOMAS W. THRASH, JR.
United States District Judge