Not for Publication

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

MICHAEL ALLEN, individually and on behalf of all others similarly situated, **Plaintiff,** **v.** **QUICKEN LOANS INC. AND NAVISTONE, INC.,** **Defendants.**	**Civil Action No. 17-12352 (ES) (MAH)** **OPINION**

SALAS, DISTRICT JUDGE

Before the Court are Defendant Quicken Loans Inc.'s ("Quicken") and Defendant NaviStone, Inc.'s ("NaviStone") (collectively, "Defendants") motions to dismiss (D.E. Nos. 19 & 20), Plaintiff Michael Allen's ("Allen" or "Plaintiff") Amended Complaint. The Court has subject-matter jurisdiction pursuant to 28 U.S.C. § 1331. The Court has considered the parties' submissions (D.E. Nos. 18-20, 25, 27-28, & 33-35) and decides the motions without oral argument under Federal Rule of Civil Procedure 78(b). For the reasons set forth below, the Court GRANTS Defendants' motions to dismiss.

I. BACKGROUND[1]

Allen filed the instant lawsuit on February 9, 2018. (*See* D.E. No. 18, Amended Complaint ("Am. Compl.")). At the heart of this controversy is Quicken's and NaviStone's implementation

[1] The Court must accept Plaintiff's factual allegations as true for purposes of resolving Defendants' motions to dismiss. *See Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009); *Bistrian v. Levi*, 696 F.3d 352, 358 n.1 (3d Cir. 2012) ("As such, we set out facts as they appear in the Complaint and its exhibits.").

and execution of a JavaScript code (the "Code") on a web server whose domain points to "www.quickenloans.com" ("Quicken's Website"). (*Id.* ¶¶ 1, 4 & 11). Allen alleges that on June 20, 2017, gizmodo.com, a technology news website, published an article describing how NaviStone's Code works to unmask anonymous website visitors. (*Id.* ¶ 18). Allen states that he visited and interacted with Quicken's Website "[o]n several occasions within the 6 months prior to filing of this lawsuit," but did not purchase any of Quicken's services or products. (*Id.* ¶¶ 2, 4 & 44). Quicken's Website provides visitors with information about its products and services related to mortgages, and offers prospective customers the ability to apply for a mortgage, or to calculate refinancing terms. (*See id.* ¶¶ 13, 23, 26, 29, 33-35 & 39). Quicken's Website provides this functionality through an on-line form. (*See id.* ¶¶ 13, 23, 34 & 44).

NaviStone is a marketing company and data broker that offers the Code to e-commerce companies such as Quicken to help them identify who visits their websites. (*Id.* ¶ 11). NaviStone does this by maintaining a database containing the names and mailing addresses of various U.S. consumers. (*Id.* ¶ 14). NaviStone attempts to identify live-time website visitors by matching their internet protocol ("IP") addresses, and other personally identifiable information ("PII") they provide, to information on NaviStone's databases. (*Id.* ¶¶ 13-14). The task of identifying visitors is handled by NaviStone's Code, which runs in the background of websites and can intercept the electronic communications of visitors, such as their "keystroke[s] and mouse click[s]." (*Id.* ¶ 13).

NaviStone provides this functionality to web services through voluntary partnerships, whereby the web service agrees to insert the Code onto its websites. (*Id.* ¶ 11). The Code sits on individual webpages and acts as a "back door" to retrieve and execute more complex code stored on other "remotely hosted [] servers" managed by NaviStone. (*Id.* ¶ 15). In the process, the Code collects a "visitor's IP address and other PII," which is then "sent to NaviStone in real-time." (*Id.*

¶ 13). NaviStone's Code is also capable of scanning a visitor's computer for "tracking files" employed by other websites capable of de-anonymizing the visitor. (*Id.* ¶ 32; *see also id.* ¶¶ 1-2, 13, 16 & 22).

Allen alleges that because NaviStone has partnered with hundreds of e-commerce websites, it can identify and track consumers across those partner websites. (*Id*. ¶ 15). He alleges that Quicken, one of NaviStone's voluntary partners, embeds the NaviStone Code onto its website to scan visitors' computers for files that can be used to identify who they are, intercept their electronic communications, and obtain their de-anonymized PII. (*Id.* ¶ 16). The Amended Complaint further alleges that NaviStone's Code is concealed "through dummy domains" in an attempt to "obfuscate the wiretap codes," and that the Code loads simultaneously with Quicken's Website. (*Id.* ¶ 17). Thus, NaviStone—and the partnering website—can "intercept[] the communication[] in real time . . . even if [a user doesn't] hit submit." (*Id.* ¶ 21). In addition, Allen alleges that the NaviStone Code intercepts information that a visitor types into a webform, such as when a visitor enters "the balance of his or her mortgage, the total value of his or her home" in an attempt to model hypothetical financing options. (*Id.* ¶ 23). Because "NaviStone's wiretaps are deployed on hundreds of e-commerce websites," and because "NaviStone maintains and correlates its back-end database of User Data and PII across these hundreds of websites," NaviStone can identify website visitors. (*Id*. ¶ 24).

Allen alleges that the security and privacy policy maintained on Quicken's Website ("Quicken's Privacy Policy") is "false and/or misleading," because Quicken "does in fact share visitor's information with NaviStone for NaviStone's marketing purposes and promotional use." (*Id.* ¶ 41). Further, Allen alleges that Quicken's Privacy Policy misleadingly and fraudulently states that: (1) "[Quicken] does not share your personal information with outside companies for

their promotional use without your consent"; (2) "[Quicken] will not ask you for personally identifiable information to use these features, and [does] not attribute the information that you provide to you as an individual"; and (3) "[Quicken does] not track URLs that you type into your browser [or] track you across the Internet once you leave [the] site." (*Id.* ¶¶ 37-41).

Allen alleges that when Defendants "implemented the wiretaps" they "intended to commit tortious acts including disclosures of the intercepted information which violated Quicken's Privacy Policy, violated the [Stored Communications Act], violated the confidentiality provisions of the Gramm-Leach-Bliley Act ["GLBA"], and several New Jersey privacy torts." (*Id.* ¶ 45).

He seeks to represent a nationwide class of persons affected by Defendants' alleged practices, and also seeks to represent a New Jersey subclass. (*Id.* ¶ 48). The Amended Complaint alleges that Defendants' practices violated: (Count I) 18 U.S.C.§ 2511(1)(a) of the Electronic Communications Privacy Act ("ECPA") by intentionally intercepting, endeavoring to intercept, and procuring another to intercept electronic communications; (Count II) 18 U.S.C. § 2511(1)(c) by intentionally disclosing electronic communications intercepted in violation of § 2511(1)(a); (Count III) 18 U.S.C. § 2511(1)(d) by intentionally using or endeavoring to use the contents of electronic communications intercepted in violation of § 2511(1)(a); (Count IV) 18 U.S.C. § 2511(1)(a) by intentionally procuring another to intercept or endeavor to intercept electronic communications; (Count V) 18 U.S.C. § 2512 by creating wiretap codes, possessing wiretaps, by advertising them, and by distributing them; (Count VI) the Stored Communications Act ("SCA"), 18 U.S.C. § 2701 *et seq*., by intentionally accessing stored files without authorization or by exceeding authorization; and (Count VII) the New Jersey common-law tort of intrusion upon seclusion by intentionally intruding on Plaintiff's solitude or seclusion in a highly offensive manner. (*Id.* ¶¶ 55-74).

II. LEGAL STANDARD

To withstand a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6), "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)). A successful claim presents "factual allegations sufficient to raise a right to relief above the speculative level" *Twombly*, 550 U.S. at 545, and does not hide behind "labels and conclusions," or "formulaic recitation[s] of the elements of a cause of action" *Iqbal*, 556 U.S. at 678 (*Twombly*, 550 U.S. at 555). Thus, "[w]hen reviewing a motion to dismiss all allegations in the complaint must be accepted as true, and the plaintiff must be given the benefit of every favorable inference to be drawn therefrom," but a court is not required to accept as true "mere conclusory statements." *Malleus v. George*, 641 F.3d 560, 563 (3d Cir. 2011) (internal quotations omitted); *Iqbal*, 556 U.S. at 678.

III. DISCUSSION

All parties make a number of arguments in favor of their respective positions. The Court addresses only arguments relevant to the disposition of Defendants' motions.

A. ECPA Claims

Allen's Amended Complaint alleges five violations of the ECPA, 18 U.S.C. § 2510 *et seq.*; four under section 2511 and one under section 2512. The Court discusses each in turn.

1. Section 2511 Claims: Counts I-IV

Plaintiff brings claims under subsections (a), (c), and (d) of section 2511(1) of the ECPA. Since claims under subsection (c) and (d) are predicated on a violation of subsection (a), the Court considers all section 2511 claims together. *See* 18 U.S.C. 2511(1)(a), (c) & (d); *see also Walsh v. Krantz*, 386 F. App'x 334, 340 (3d Cir. 2010) ("Inasmuch as Dr. Krantz did not 'intercept' the

telephone call, logically he could not have 'disclosed' the content of the call to a third person, or 'used' any information disclosed during the call for any purpose, 18 U.S.C. § 2511(1)(c), (d).").

The federal Wiretap Act makes it unlawful for "any person" to, among other things, intentionally intercept an electronic communication, or procure any other person to intercept an electronic communication. 18 U.S.C. § 2511(1)(a). Liability premised under § 2511(1)(a) relies on the definitions of "electronic communication" and "intercept" set forth in 18 U.S.C. § 2510. An "electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photoopical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12). The Third Circuit has understood "electronic communication" to include a diverse set of digital communications, such as web cookies, URLs, and emails. *See In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 274-75 (3d Cir. 2016); *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 137 (3d Cir. 2015).

As noted above, another prerequisite to liability under section 2511(1)(a) is demonstrating that the electronic communication in question was "intercepted." Section 2510(4) defines "intercept[ion]" as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Under the statute, one cannot intercept electronic communications if the electronic communication does not contain content. *Id.* Thus, to fulfill § 2511(1)(a)'s "intercept[ion]" requirement, a plaintiff must sufficiently allege that the electronic communications in question contained content. *See* 18 U.S.C. § 2510(4). The statute defines "content" as "any information concerning the substance, purport, or meaning of that communication." *Id.* § 2510(8).

Thus, "[a] plaintiff pleads a prima facie case under the [section 2511] by showing that the

defendant (1) intentionally (2) intercepted . . . (3) the contents of (4) an electronic communication, (5) using a device." *In re Google*, 806 F.3d at 135 (internal quotation marks omitted). However, section 2511(2)(d) makes the interception lawful when the person intercepting "is a party to the communication or where one of the parties to the communication has given prior consent to such interception." As explained below, Allen's section 2511 claims fail because Allen cannot show that Defendants unlawfully intercepted the communications.

a. Defendants' Interception Was Lawful

Defendants argue that Allen's claims fail because the liability exception under section 2511(2)(d) permitted the alleged interception. Particularly, Quicken argues that Allen "admits that any allegedly intercepted communications were made on QuickenLoans.com website" making Quicken a party to the communication. (D.E. No. 20, Memorandum of Points and Authorities in Support of Defendant Quicken Loan's Motion to Dismiss Plaintiff's First Amended Complaint ("Def. Quicken's Mov. Br.") at 11). Both Defendants also argue that Allen admits in his Amended Complaint that "Quicken Loans and NaviStone intercepted these communications '[p]ursuant to an agreement,'" and as a result Allen concedes that Quicken consented to NaviStone's interception of his communications. (*Id.* at 12 (citing Am. Compl. ¶ 16)); *see also* D.E. No. 19, Memorandum of Defendant NaviStone, Inc. in Support of Its Motion to Dismiss the Amended Complaint ("Def. NaviStone's Mov. Br.") at 14).

In opposition, Allen only counters that NaviStone was not a party to the communication because Allen and "an extreme supermajority of website visitors" do not know of NaviStone's involvement with Quicken. (D.E. No. 25, Plaintiff's Memorandum of Law in Opposition to Defendants Quicken Loans Inc. and NaviStone, Inc.'s Motions to Dismiss the Amended Complaint ("Pl. Opp. Br.") at 9-10).

Section 2511(2)(d) makes interception under § 2511(1)(a) lawful if the person carrying out the interception "is a party to the communication or where one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(d). As the Amended Complaint plainly admits, all relevant communications occurred on Quicken's Website, making Quicken the intended recipient (and a party) to the communications. (*See* Am. Compl. ¶¶ 1-4, 13, 23, 26, 33-34 & 45);[2] *see also In re Google*, 806 F.3d at 142-43 ("Because the defendants were the intended recipients of the transmissions at issue . . . we agree that § 2511(2)(d) means the defendants have done nothing unlawful under the Wiretap Act."). Indeed, Allen waived any argument to the contrary by failing to respond to Defendants' arguments in his brief. (*See* Pl. Opp. Br. (not disputing Defendants arguments that Quicken was a party to the communication)); *see also Leisure Pass N. Am., LLC v. Leisure Pass Grp., Ltd.*, No. 12-03375, 2013 WL 4517841, at *4 (D.N.J. Aug. 26, 2013) ("Plaintiff has waived its opposition to this argument by failing to respond to it.").

Similarly, Allen's argument that NaviStone was not a party to the communication because "an extreme supermajority of website visitors" do not know of NaviStone's involvement with Quicken is irrelevant. (*See* Pl. Opp. Br. at 9-10). Whether website visitors were aware of NaviStone is immaterial; the ECPA is a one-party consent statute, and so long as "one of the parties

[2] In a single paragraph, Plaintiff also alleges that "at least some of the communications" were "communications with [Plaintiff's] Internet service provider [("ISP")]" rather than with Defendants. (Am. Compl. ¶ 44). However, Plaintiff's opposition brief appears to abandon this allegation. In any event, this allegation fails to hold any water, 1) because it is contradicted by the rest of Plaintiff's Amended Complaint which states that all the communications occurred when he and similarly situated putative class members visited Quickens' Website, and 2) because ISPs are intermediaries who facilitate electronic communications, not recipients of such communications. *See United States v. Ackerman*, 831 F.3d 1292, 1294 (10th Cir. 2016) (explaining that an email never reached its "intended recipient" because AOL, the ISP, had a filter which thwarted its transmission); *United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010) ("An ISP is the intermediary that makes email communication possible. Emails must pass through an ISP's servers to reach their intended recipient. Thus, the ISP is the functional equivalent of a post office or a telephone company."); *Ctr. for Democracy & Tech. v. Pappert*, 337 F. Supp. 2d 606, 613 (E.D. Pa. 2004) ("A hypothetical [electronic] communication . . . might originate on the user's computer, travel through . . . a regional ISP's network . . . and finally to the computer of the intended recipient of the communication."). As NaviStone aptly puts it, Plaintiff's "claim of an intention to communicate solely with his ISP is nonsensical. It is akin to a person claim[ing] that, in calling a retailer's telephone number, it was his intention to speak with the phone company." (NaviStone Mov. Br. at 11).

to the communication has given prior consent to such interception," no liability exists under section 2511. *See* 18 U.S.C. § 2511(2)(d); *In re Nickelodeon Consumer Privacy Litig.*, No.12-7829, 2014 WL 3012873, at *13 (D.N.J. July 2, 2014). Here, Allen admits that Quicken, one of the parties to the communication, gave prior consent to NaviStone's interception "[p]ursuant to an agreement." (*See* Am. Compl. ¶ 16). Therefore, NaviStone's interception is not unlawful under the ECPA.

Further, Allen's reliance on *United States v. Eady*, 648 F. App'x 188 (3d Cir. 2016), is misplaced. *Eady* involved an individual who surreptitiously recorded conversations between two other individuals without the knowledge or consent of *any* party to that communication. 648 F. App'x at 189-90. Eady argued that he was a party to the communication because he could have spoken during the phone calls he intercepted. *Id.* at 191. Thus, the court in *Eady* interpreted the meaning of the first part of 2511(2)(d)—"where such as person is a party to the communication"—which "will always consist of at least two parties: the speaker and/or sender, and at least one intended recipient." *In re Google*, 806 F.3d at 143. However, *Eady* says nothing about the second part of the exception, which only requires that "*one of the parties* to the communication" give consent to the outsider. For this part of the exception, the non-consenting party's knowledge of the interception by the outsider is irrelevant. Consequently, Defendants' are entitled to the liability exception under section 2511(2)(d).

b. The Exception To The Exception

Allen attempts to circumvent the liability exception by invoking the "exception to the exception." (*See* Pl. Opp. Br. at 7). Particularly, section 2511(2)(d) reinstates liability if "such communication is intercepted *for the purpose* of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." (emphasis added).

Allen advances three arguments for why Defendants should not be entitled to the liability

exception. He contends that 1) Defendants committed the New Jersey tort of intrusion upon seclusion, 2) that Defendants violated Quicken's Privacy Policy, and 3) that Defendants violated the confidentiality provisions of the GLBA by intercepting his communications and searching his computer for files. (Pl. Opp. Br. at 7-8). Allen argues that as a result, Defendants should not be entitled to the liability exception under section 2511(2)(d) because that section "provides an 'exception to the exception' where the underlying act is criminal or tortious." (Pl. Opp. Br. at 7). But this assertion misapprehends the language of the statute and the controlling case law in this Circuit.

For liability to be reinstated under section 2511(2)(d), this Circuit requires that the "plaintiff . . . plead sufficient facts to support an inference that the offender intercepted the communication for the *purpose* of a tortious or criminal act that is *independent* of the intentional act of [intercepting]." *In re Google*, 806 F.3d at 145 (quoting *Caro v. Weintraub*, 618 F.3d 94, 100 (2d Cir. 2010) ("Congress chose the word 'purpose' for a reason. Therefore, the offender must have as her objective a tortious or criminal result.") (emphasis added); *see also Sussman v. Am. Broad. Companies, Inc.*, 186 F.3d 1200, 1202–03 (9th Cir. 1999) ("Under section 2511, the focus is not upon whether the interception itself violated another law; it is upon whether the *purpose* for the interception—its intended use—was criminal or tortious . . . . Where the purpose is not illegal or tortious, but the means are, the victims must seek redress elsewhere."). Thus, the plaintiff must plead that the defendant intercepted the communications "for the *purpose* of facilitating some further impropriety, such as blackmail," not merely that the interception itself (or the means of interception) is tortious or criminal. *Sussman*, 186 F.3d at 1203 (emphasis added).

Under this statutory scheme, Allen's arguments plainly fail because the alleged tortious or criminal activities are not independent from the intentional act of intercepting; they are the

interception itself. *See In re Google*, 806 F.3d at 145 ("[T]he plaintiffs point to no legal authority providing that the exception to § 2511(2)(d) is triggered when, as here, the tortious conduct is the alleged wiretapping itself."). First, Allen's argument that Defendants' alleged violation of the New Jersey tort of intrusion upon seclusion permits liability under 2511 is unpersuasive. (*See* Pl. Opp. Br. at 8 & 20; Am. Compl. ¶¶ 1, 4, 41 & 71-74). Allen admits that the *purpose* of Defendants' interception was for "marketing purposes and promotional use," and not to commit a tort or crime. (Am. Compl. ¶ 41). Thus, Allen's intrusion upon seclusion claim is about the means (the use of the NaviStone Code to "de-anonymize" Allen), not the purpose of the interception. *See In re Nickelodeon Consumer Privacy Litig.*, 2014 WL 3012873, at *13 (refusing to use intrusion upon seclusion tort allegation to reinstate liability under 2511(2)(d) because "courts have almost uniformly found that the 'criminal or tortious act' exception applies only where defendant has 'the intent to use the illicit recording to commit a tort or crime beyond the act of recording itself.'") (quoting *Caro*, 618 F.3d at 101 ("Invasion of privacy through intrusion upon seclusion presents a problem for Caro—it is a tort that occurs through the act of interception itself.").

The same holds true for Allen's reliance on Defendants' alleged violation of Quicken's Privacy Policy. Put in the best light, Allen's argument merely restates his section 2511 interception claims. (*Compare* Pl. Opp. Br. at 8, *with id.* at 2-3). Further, even if this was not the case, Allen cites no law that would support his assertion that a mere violation of a website's privacy policy by itself constitutes a "criminal or tortious act" under section 2511(2)(d). And to the extent this violation is the basis for his intrusion upon seclusion claim, that does not change the analysis outlined above.

Finally, Allen's reliance on the GLBA—contained in two conclusory statements in the Amended Complaint—is also misplaced. The GLBA was enacted to "provid[e] consumers with

new protections with respect to the transfer and use of their nonpublic personal information by financial institutions." H.R. Conf. Rep. 106–434 (1999), 106th Cong., 1st Sess. 1999, 1999 U.S.C.C.A.N. 245, 265. Accordingly, the GLBA sets forth both "affirmative and continuing obligation[s]" on the part of financial institutions to "respect the privacy of [their] customers and to protect the security and confidentiality of . . . nonpublic personal information," 15 U.S.C. § 6801(a), as well as criminal penalties to prevent private individuals, from "obtain[ing] . . . customer information of a financial institution" through fraudulent means, 15 U.S.C. §§ 6821(a)(3); 6823(a).

Allen argues that he "alleges that Defendants' conduct 'violated the confidentiality provisions of the [GLBA].'" (Pl. Opp. Br. at 8 (quoting Am. Compl. ¶ 45); *see also* D.E. No. 34 at 2 (arguing that section 2511(d)(2) reinstates liability "where the underlying act is criminal or tortious")). In effect, Allen argues that a mere alleged violation of the GLBA gives rise to liability under Section 2511(2)(d). But this ignores the plain language of the statute and this Circuit's precedent; the question is not whether Defendants' interception violated the GLBA, but "whether the *purpose* for the interception—its intended use—was" to facilitate an independent criminal activity. *Sussman*, 186 F.3d at 1203 (emphasis added); *In re Google*, 806 F.3d at 145 ("[P]laintiff must plead sufficient facts to support an inference that the offender intercepted the communication for the purpose of a tortious or criminal act that is independent of the intentional act of recording."). As explained above, Allen fails to do that here and instead only alleges that Quicken used NaviStone's Code to intercept the communications and de-anonymize Allen for the purpose of facilitating marketing. (*See* Pl. Opp. Br. at 5). Indeed, there are "no facts pleaded to indicate that the interceptions in this case were motivated by anything other than Defendants' desire to monetize Plaintiffs' [use of the Quicken Website], and thus the 'criminal or tortious act' exception embodied in § 2511(2)(d) is inapplicable." *See In re Nickelodeon Consumer Privacy Litig.*, 2014 WL

3012873, at *13; *see also Cohen v. Casper Sleep Inc.*, No. 17-9325, 2018 WL 3392877, at *3 (S.D.N.Y. July 12, 2018) ("[C]ollecting data to de-anonymize consumers was not Defendants' primary motivation for installing the Code. Rather, it was the means Defendants used to achieve their real purpose—marketing.").

Allen cites two cases from sister district courts to support his argument that a violation of a criminal statute is sufficient to reinstate liability. (*See* D.E. 34 at 2 (citing *United States v. Lam*, 271 F. Supp. 2d 1182 (N.D. Cal. 2003), *Hawaii Reg'l Council of Carpenters v. Yoshimura*, No. 16-00198, 2016 WL 4745169 (D. Haw. Sept. 12, 2016)). But both of these cases support the contrary position. In *Lam*, the alleged interception was done for the purpose of "keeping business records for [the party's] unlawful gambling activities." *Lam*, 271 F. Supp. 2d at 1184. Similarly, in *Yoshimura* the interception was done for the purpose of "covering up [the party's] breaches of fiduciary duties and extorti[on]. . . ." *Yoshimura*, 2016 WL 4745169, at *8. Thus, in both cases the alleged tortious or criminal purpose was independent from the intentional act of intercepting; the interception was done for the purpose of facilitating unlawful gambling and extortion. By contrast, Allen here offers nothing to show that Defendants intended facilitate some further impropriety, or even intended to violate the GLBA.

Finally, Allen's reliance on the GLBA to reinstate liability is also misplaced for two additional reasons. First, the GLBA does not apply to NaviStone because Allen has not alleged that NaviStone is a financial institution as defined by the statute, or is otherwise subject to it. *See* 15 U.S.C. § 6809(3). As to Quicken, Allen concedes that he was not a consumer for purposes of the GLBA, and thus, he has not alleged that either Defendant obtained his nonpublic personal information in violation of the statute. The relevant portion of the GLBA prohibits financial institutions from disclosing "nonpublic personal information." 15 U.S.C. § 6802. Although

section 6802(4)(A) defines nonpublic personal information as information "provided by a consumer to a financial institution," section 6809(9) defines a consumer as "an individual who *obtains*, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes . . . ." (emphasis added). Because Allen's Amended Complaint concedes that he "never procured financial services from Quicken" (Am. Compl. ¶¶ 2 & 4), he is not a consumer and the information that he alleges Defendants misused is not protected by the GLBA. The GLBA simply does not apply here, and any argument that rests on an assumption that it does must fail.

Because Allen's section 2511 claims fail as a matter of law, Counts I through IV are dismissed *with prejudice*. *See In re Nickelodeon*, 827 F.3d at 275 (affirming district court's dismissal of ECPA claims with prejudice when plaintiff's allegations gave rise to the conclusion that the defendants lawfully intercepted the communications under section 2511(2)(d)).

2. Section 2512 Claim: Count V

Allen also charges Defendants with violating 18 U.S.C. 2512. (Am. Compl. ¶¶ 64-67). Allen's claim is implicitly based on his supposition that 18 U.S.C. § 2520(a), which authorizes the recovery of civil damages under some sections of the ECPA, provides for a private right of action for violations of section 2512. Defendants maintain that no such private right of action exists under a plain interpretation of the statute. (Def. Quicken's Mov. Br. at 25-26). The Court agrees with Defendants.

Section 2512 imposes criminal liability for any person who manufactures, distributes, possesses, or advertises a device the design of which renders it primarily useful for surreptitiously intercepting electronic communications. 18 U.S.C. § 2512(1). Such conduct is classified as a felony and is punishable, under the statute, by imprisonment of up to five years, or a fine, or both.

Id. Strikingly absent from this provision is any mention of a civil remedy.

In turn, section 2520(a) establishes a private right of action for violations of certain provisions of the ECPA. The plain text of § 2520(a) makes clear that "any person whose wire, oral, or electronic communication is *intercepted*, *disclosed*, or intentionally *used* in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged *in that violation* such relief as may be appropriate." 18 U.S.C. § 2520 (emphasis added). As the Third Circuit found, this language closely tracks section 2511, which makes it unlawful to intentionally *intercept*, *disclose*, or *use* the contents of an electronic communication. 18 U.S.C. § 2511(1)(a),(c)-(d); *DIRECTV, Inc. v. Pepe*, 431 F.3d 162, 167 (3d Cir. 2005) ("The linguistic interlock between the two provisions could not be tighter, nor more obviously deliberate: § 2511(1)(a) renders unlawful the unauthorized interception of electronic communications, including encrypted satellite television broadcasts, while § 2520(a) authorizes private suit against those who have engaged in such activities."). But when drafting section 2520(a) Congress chose to omit any mention of an avenue to seek civil redress for manufacturing, possessing, distributing, or advertising a wiretap device. *See* 18 U.S.C. § 2520.

Still, Allen argues that section 2520 gives rise to civil liability under section 2512 when the defendant who possesses the wiretap device engaged in "more than mere possession." (*See* Pl. Opp. Br. at 17 ("Plaintiff alleges 'more than mere possession' of a wiretapping device.")).

Courts that have previously addressed arguments that section 2520 opens the door for civil liability under section 2512 have come to inconsistent conclusions, giving rise to three separate interpretations: 1) a broad view, 2) a plain language view, and 3) a hybrid view. The first line of cases involves a number of district courts that have adopted a broad reading of section 2520 by concluding that the section gives rise to a private cause of action against anyone who violates the

ECPA, regardless of whether that violation was specifically an interception, disclosure, or use of a communication. *See, e.g.*, *DIRECTV, Inc. v. Dougherty*, No. 02-5576, 2003 WL 24046760, at *2-3 (D.N.J. Oct. 8, 2003) (noting, at the time, that "the majority position, and the better view, is that the ECPA allows for recovery of civil damages against one who possesses an intercepting device in violation of § 2512"); *DIRECTV, Inc. v. Kitzmiller*, No. 03-3296, 2004 WL 692230, at *4 (E.D. Pa. Mar. 31, 2004) (agreeing with *Dougherty* that "anyone who violates a provision of the ECPA is a potential defendant" and stating that "this newly-developed majority view is the better approach").

Since 2004, however, an overwhelming majority of courts around the country, including district courts in this Circuit, have adopted a plain language interpretation. These courts hold that section 2520 provides a private cause of action only against those defendants who violate the plain language of section 2520(a), i.e. those who unlawfully intercept, disclose, or use a communication, all of which are within the ambit of section 2511. Consequently, no private cause of action exists for possessing, manufacturing, distributing, or advertising a wiretapping device. *See e.g.*, *DirecTV, Inc. v. Treworgy*, 373 F.3d 1124, 1127 (11th Cir. 2004) ("The phrase 'which engaged *in that violation*' makes apparent the intent of Congress to limit liability to a certain class of defendants. Congress chose to confine private civil actions to defendants who had 'intercepted, disclosed, or intentionally used a communication in violation of . . . [the ECPA.]'") (emphasis in original) (citations and some alterations omitted)); *DIRECTV Inc. v. Robson*, 420 F.3d 532, 539 & n.31 (5th Cir. 2005) (reaching the same conclusion and collecting cases that have found "no merit in [the] assertion that § 2520 expressly provides a private cause of action for [all] violations of the criminal proscriptions of § 2512") (cleaned up); *see also Byrd v. Aaron's, Inc.*, No. 11-101, 2012 WL 12887775, at *11 (W.D. Pa. Feb. 17, 2012) (collecting Third Circuit district court cases and

noting that "this Court will join the growing number of district courts within the Third Circuit in concluding that 18 U.S.C. § 2520(a) does not provide a private cause of action for violations of 18 U.S.C. § 2512"); *DIRECTV Inc. v. Cignarella*, No. 03-2384, 2005 WL 1252261, at *4-5 (D.N.J. May 24, 2005) (examining the legislative history of the ECPA and concluding that "not only does the plain language of the statute demonstrate that no civil liability exists for a violation of § 2512, but the legislative history also supports this conclusion").

More recently, the Sixth Circuit applied a sort of hybrid interpretation, indicating that "a defendant . . . —which allegedly violates § 2512(1)(b) by manufacturing, marketing, and selling a violative device—is subject to a private suit under § 2520 only when that defendant also plays an active role in the use of the relevant device to intercept, disclose, or intentionally use a plaintiff's electronic communications." *Luis v. Zang*, 833 F.3d 619, 637 (6th Cir. 2016). In reaching this conclusion, the Sixth Circuit agreed with the majority view concluding "that those other courts that have adopted a narrow reading of § 2520 have the better end of this debate. This is because the phrase 'engaged in that violation' plainly refers back to the earlier clause defining the 'violation' as an 'intercept[ ], disclos[ure], or intentional[ ] use[ ].'" *Id.* at 636 (citing 18 U.S.C. § 2520) (alterations in original). However, the Sixth Circuit then primarily relied on a factual analysis to distinguish its case from *Treworgy* to conclude that violations of section 2512 could still give rise to civil liability. *Id.* at 637. Particularly, the Sixth Circuit emphasized that unlike *Treworgy*, the defendant in its case "manufactured, marketed, and sold [the wiretap device] with knowledge that it would be primarily used to illegally intercept electronic communications" and then "remained actively involved" by operating the server where the intercepted communications were stored. *Id.* Thus, because the defendant "actively manufactured, marketed, sold, and operated the device" that it knew was used to intercept, disclose, or intentionally use

communications, the Sixth Circuit concluded that the defendant had "'engaged in' a violation of the Wiretap Act. . . ." *Id.*

Having considered these different interpretations, the Court joins the majority of courts which have applied a plain language interpretation. As a starting point, the plain language of section 2520(a) permits plaintiffs to seek civil relief only when the "electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter. . . ." 18 U.S.C. 2520(a). The statute, as drafted by Congress, does not include language that would permit a plaintiff to seek civil redress from a defendant who manufactures, possesses, distributes, or advertises the wiretap device. Indeed, the plain language of the section limits liability only to defendants who "engaged *in that violation*," meaning defendants who intercepted, disclosed, or intentionally used the communications in "violation of this chapter." *See id.*; *Treworgy*, 373 F.3d at 1127 ("[A]s a matter of grammar and sentence structure, the phrase 'that violation' refers to the interception, disclosure, or intentional use of communications mentioned earlier in the sentence, and not to the possession[, manufacturing, or distribution] of prohibited devices.") (citations omitted).

In this respect, the Court finds Allen's arguments and the Sixth Circuit hybrid interpretation unpersuasive. In finding that section 2520 extends civil liability to section 2512, the Sixth Circuit held that because the plaintiff had alleged that the defendant had "actively manufactured, marketed, sold, and *operated* the device" that was used to intercept, disclose, or intentionally use communications, then defendant had "'engaged in' *a violation* of the Wiretap Act. . . ." *Luis*, 833 F.3d at 637 (noting that civil liability under 2512 exists when the "defendant also plays an active role in *the use of the relevant device* to intercept, disclose, or intentionally use a plaintiff's electronic communications") (emphasis added).

Respectfully, this Court submits that this analysis "confuses . . . alleged violations of §

2512 with violations of § 2511." *Luis*, 833 F.3d at 644 (Batchelder, J. dissenting). First, section 2512(1) only makes it illegal for a person to (a) send through the mail or carry in interstate commerce, (b) manufacture, assemble, possesses, or sell, or (c) disseminate or advertise a wiretap device when it is known that the device is primarily useful for surreptitious interception of electronic communications. Section 2512 says nothing about a person "operating" or using such a device. *See* 18 U.S.C. § 2512. Section 2511(b), however, does make it plain that it is illegal for a person to "intentionally use" a wiretap device in the manner prescribed by subsections (i) through (v). 18 U.S.C. § 2511(1)(b); *see also* § 2511(1)(d) (making it unlawful to intentionally use the contents of an electronic communication). Clearly then, only section 2511, not 2512, applies when a person "operates" or "plays an active role in the use" of a wiretap device.

Second, the Sixth Circuit's choice of words is also telling. It found that the plaintiff had established that the defendant had "'engaged in' *a violation* of the Wiretap Act. . . ." But as the Sixth Circuit's opinion had noted just three paragraphs earlier, section 2520(a) does not permit civil liability for "*a* violation" of the ECPA; it only permits civil liability when a defendant "engaged in *that violation*," namely the interception, disclosure, or intentionally use of communications in violation of the statute. *See Luis*, 833 F.3d at 636 ("This is because the phrase 'engaged in that violation' plainly refers back to the earlier clause defining the 'violation' as an 'intercept[ ], disclos[ure], or intentional[ ] use[ ].'") (citing 18 U.S.C. § 2520) (alterations in original). And as noted earlier, section 2511, not 2512, defines when an interception, disclosure, or intentional use of an electronic communication occurs "in violation of this chapter."

To be sure, if a defendant both possesses a wiretap device and then uses the device to intercept or disclose an electronic communication (or intentionally uses the contents of said communication which were acquired by an interception using said device), then logically the

defendant would be in violation of both section 2511 and section 2512. However, he would still be liable for civil penalties only as to the section 2511 violations. The mere fact that he committed both violations does not suddenly transform the plain statutory language of section 2520 to provide an avenue for civil relief under section 2512, when none exists otherwise. After all, Congress "does not, one might say, hide elephants in mouseholes." *See Whitman v. Am. Trucking Ass'ns*, 531 U.S. 457, 468 (2001).[3]

In short, until the Third Circuit holds otherwise, or until Congress explicitly establishes a private right of action for violations of § 2512, Allen does not have a viable legal pathway for pursing a claim for an alleged violation of § 2512. Count V of Allen's Amended Complaint is dismissed *with prejudice*.

B. Stored Communications Act Claim: Count VI

The Amended Complaint alleges that Defendants "intentionally accessed stored files on Allen's and Class members' computers and devices without authorization or by exceeding authorization." (Am. Compl. ¶ 70). Defendants argue that under this Circuit's precedent, "an individual's computer is not a 'facility through which an electronic communication service is provided' and, thus, a plaintiff does not plead a claim under the SCA by alleging access to a person's computer (or other personal device)." (Def. Quicken's Mov. Br. at 27 (citing *In re Google*, 806 F.3d at 146)).

Allen does not respond to this argument, and in fact, his brief appears to abandon the claim entirely by not mentioning it at all. (*See generally* Pl. Opp. Br.). In any event, the Court finds that

[3] Even if this Court were to apply the interpretation espoused by the Sixth Circuit, Plaintiff would still have no claim under section 2512. In *Luis*, the Sixth Circuit found that the plaintiff had established that the defendant had violated section 2511. *See Luis*, 833 F.3d at 626. Here, as outlined above, Plaintiff fails to do so because the interceptions were lawful under the statute. Thus, at best, Plaintiff has only alleged that Defendants unlawfully possessed and advertised a wiretap device, which under *Luis*, is not enough to give rise to civil liability.

this claim fails as a matter of law because Allen cannot allege that Defendants accessed a "facility."

To establish a *prima facie* claim for the violation of 18 U.S.C. § 2701, a plaintiff must show that the defendant: "(1) intentionally access[ed] without authorization a *facility* through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that *facility*; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system." *In re Google*, 806 F.3d at 145-46 (emphasis added). Crucial here is whether Allen has sufficiently alleged that Defendants unlawfully accessed a "facility through which an electronic communication service is provided." *Id*. He has not.

The Third Circuit has held that "an individual's personal computing device is not a facility through which an electronic communications service is provided." *Id.* at 146 (internal quotations omitted). Allen alleges that "Defendants intentionally accessed stored files on Plaintiff's and Class members' computers and devices . . . ." (Am. Compl. ¶ 70). Because under the SCA an individual's personal computer or device is not a facility through which an electronic communications service is provided, Allen's SCA claim fails. And because amendment would be futile, Count IV of Allen's Amended Complaint is dismissed *with prejudice*. *See Grayson v. Mayview State Hosp.*, 293 F.3d 103, 108 (3d Cir. 2002).

C. Intrusion Upon Seclusion: Count VII

1. Jurisdiction

Defendant NaviStone requests that the Court exercise its discretion to decline supplemental jurisdiction over the intrusion upon seclusion claim pursuant to 28 U.S.C. § 1367(c)(3). (Def. NaviStone's Mov. Br. at 23). Allen's Amended Complaint alleges that the basis of this Court's jurisdiction is federal question under 28 U.S.C. § 1331, for the alleged violations of the ECPA and

SCA. (Am. Compl. ¶¶ 7-8). NaviStone points that Allen has not alleged any other basis for this Court to exercise jurisdiction over the New Jersey intrusion upon seclusion claim. (Def. NaviStone's Mov. Br. at 24). Allen responds that the Court has diversity jurisdiction over Plaintiff's state-law claim pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d). (Pl. Opp. Br. at 23). He argues that the Amended Complaint has sufficiently alleged that diversity exists, and that he meets the amount in controversy requirement. (*Id.* (citing Am. Compl. ¶¶ 4-6 & 74)). In reply, NaviStone counters that the Amended Complaint lacks allegations establishing that the damages arising from Count VII for the New Jersey class exceed $5,000,000, because Allen has not alleged any harm for the intrusion and Allen offers nothing concerning the size of the New Jersey class that would permit a rough computation of potential damages. (D.E. No. 27 at 13-14).

Section 1332(d)(2) provides federal district courts with "original jurisdiction" over a case when three requirements are met: (1) an amount in controversy that exceeds $5,000,000; (2) minimally diverse parties; and (3) a class consisting of at least 100 or more members. *Standard Fire Ins. Co. v. Knowles*, 68 U.S. 588, 133 (2013). "In order to determine whether the CAFA jurisdictional requirements are satisfied, a court evaluates allegations in the complaint." *Judon v. Travelers Prop. Cas. Co. of Am.*, 773 F.3d 495, 500 (3d Cir. 2014). "The burden of establishing federal jurisdiction rests with the party asserting its existence." *Lincoln Benefit Life Co. v. AEI Life, LLC*, 800 F.3d 99, 105 (3d Cir. 2015) (citing *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 342 n.3 (2006)). Indeed, "CAFA does not change the proposition that the plaintiff is the master of her own claim." *Morgan v. Gay*, 471 F.3d 469, 474 (3d Cir. 2006). Thus, the plaintiff must allege the jurisdictional facts upon which subject matter jurisdiction is based. *See McNutt v. Gen. Motors Acceptance Corp.*, 298 U.S. 178, 182 (1936).

Here, Allen sufficiently alleges diversity. (*See* Am. Compl. ¶¶ 4-6) (alleging that Allen is a New Jersey citizen, Quicken is a Michigan citizen, and NaviStone is a Delaware citizen); 28 U.S.C. § 1332(d)(2)(A) (stating that diversity is satisfied if "any member of a class of plaintiffs is a citizen of a state different from any defendant"). Similarly, Allen alleges that the entire national class "number[s] in the millions" (Am. Compl. ¶ 49), thus it could be reasonably inferred that at least 100 of those class members are part of the New Jersey subclass. However, the Amended Complaint fails to sufficiently allege that the amount in controversy for the New Jersey subclass exceeds the $5,000,000 requirement. Allen points Defendants, and the Court, to the section of his Amended Complaint labeled "relief sought." (Pl. Opp. Br. at 23). However, that does not help him because the only damages quantified are statutory damages arising from the ECPA and SCA claims, which have been dismissed. Omitting these statutory damages, the section simply reads:

> WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks a judgment against Defendants as follows:
> A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;
> . . . .
> C. For an order finding in favor of Plaintiff and the Class on [the intrusion upon seclusion claim] asserted herein;
> . . . .
> F. For all remedies specified under New Jersey's privacy torts;
> G. For prejudgment interest on all amounts awarded;
> H. For an order of restitution and all other forms of equitable monetary relief;
> I. For injunctive relief as pleaded or as the Court may deem proper;
> J. For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and costs of suit; and
> K. Grant any and all such relief as the Court deems appropriate.

(Am. Compl. at 26).

These allegations fail to sufficiently state the amount Allen reasonably seeks for the intrusion upon seclusion claim—or the loss any putative New Jersey class member—in a way that

would permit the Court to estimate the total amount of the controversy. Consequently, the Amended Complaint does not properly plead the amount in controversy requirement under CAFA. *See Golden v. Golden*, 382 F.3d 348, 354 (3d Cir. 2004) ("Where a federal cause of action is based on diversity jurisdiction , the complaint must allege an amount in controversy between the parties in excess of the statutory minimum."); *Sunshine v. Reassure Am. Life Ins. Co.*, No. 10-1030, 2011 WL 666054, at *2 (E.D. Pa. Feb. 22, 2011), *aff'd*, 515 F. App'x 140 (3d Cir. 2013) ("Neither compensatory nor punitive damages are quantified in the complaint. The complaint does not state the amount of Mr. Sunshine's actual loss, nor the actual loss of any putative class members . . . . The complaint does not satisfy [CAFA's] amount in controversy requirement."); *Hyman v. WM Fin. Servs., Inc.*, No. 06-4038, 2007 WL 1657392, at *5 n.4 (D.N.J. June 7, 2007) ("Plaintiffs, though, have not alleged damages of any particular amount in their complaint. Therefore, they have failed to meet the pleading standards under the CAFA.").

The Court, however, is not ready to completely dismiss this case because it appears that Allen might be able to allege sufficient facts for this Court to exercise original jurisdiction over his intrusion upon seclusion claim. Therefore, the Court denies NaviStone's request and dismisses Count VII *without prejudice*.[4]

[4] Even assuming jurisdiction was properly pleaded, the Court finds that Count VII must be dismissed for failure to state a claim. New Jersey "explicitly recognizes a right to informational privacy." *In re Nickelodeon Consumer Privacy Litig.*, 2014 WL 3012873, at *18 (internal quotations omitted). An "intrusion upon seclusion occurs whenever a plaintiff can show (i) an intentional intrusion (ii) upon the seclusion of another that is (iii) highly offensive to a reasonable person." *In re Nickelodeon*, 827 F.3d at 293.

Here, Plaintiff has failed to properly plead that Defendants' conduct is highly offensive to a reasonable person. Particularly, Allen's Amended Complaint alleges that "Defendants' intentional intrusion on Plaintiff's solitude or seclusion is highly offensive to a reasonable person in that Defendants' conduct violated federal and state civil and criminal statutes designed to protect individual privacy." (Am. Compl. ¶ 73). However, as outlined above, Allen failed to establish that Defendants violated the ECPA, the SCA, or even the GLBA. Eliminating those bases, the Amended Complaint simply concludes that "Defendants' intentional intrusion on Plaintiff's solitude or seclusion is highly offensive to a reasonable person . . . ." (*Id.*). Because this allegation is "entirely conclusory," it is "properly disregarded on a motion to dismiss for failure to state a claim." *In re Nickelodeon Consumer Privacy Litig.*, 2014 WL 3012873, at *19.

D. Leave to Amend

Defendants also request that the Court dismiss Allen's Amended Complaint without leave to amend. Defendants argue that Allen amended his original Complaint after previewing NaviStone's arguments in its first motion to dismiss, yet Allen only chose to add "bogus" claims and allegations that he readily abandoned during briefing. (*See* D.E. No. 27 at 14; D.E. No. 28 at 15). Thus, Defendants argue that this has caused them great expense and that further amendments will prejudice them. (*Id.*).

The Court is cognizant that the allegations here indicate that Allen began visiting Quicken's Website almost immediately after the gizmodo.com article was published on June 20, 2017, and that Allen visited Quicken's Website "[o]n several occasions within the 6 months prior to filing of this lawsuit," but never actually acquired any Quicken service or product. (Am. Compl. ¶¶ 2, 4 & 18). The inference could be drawn that Allen visited Quicken's Website, not as an unsuspecting potential customer seeking services, but simply to start the instant lawsuit. However, at a motion to dismiss stage the Court must draw all reasonable inferences in favor of the plaintiff, and thus, Allen must be given the benefit of the doubt.

Whether to grant leave to amend is at the discretion of the Court. *See Foman v. Davis*, 371 U.S. 178, 182 (1962); Fed. R. Civ. P. 15(a). But "[i]n the absence of substantial or undue prejudice, denial instead must be based on bad faith or dilatory motives, truly undue or unexplained delay, repeated failures to cure the deficiency by amendments previously allowed, or futility of amendment." *Lorenz v. CSX Corp.*, 1 F.3d 1406, 1414 (3d Cir. 1993). And at this juncture, the Court is not yet ready to rule that amending the complaint, particularly as to the intrusion upon seclusion claim, would be futile. Therefore, the Court will permit Allen to amend his complaint, but he is forewarned that this will be his last bite of the proverbial apple.

IV. CONCLUSION

For the foregoing reasons, the Court GRANTS Defendants' motions to dismiss. Counts I through VI of Allen's Amended Complaint are dismissed *with prejudice*. Count VII is dismissed *without prejudice*. Allen may file a final amended complaint within 20 days, but failure to do so shall constitute dismissal of the entire action *with prejudice*.[5] An appropriate Order accompanies this Opinion.

s/Esther Salas
Esther Salas, U.S.D.J.

[5] If Plaintiff "does not desire to amend, he may file an appropriate notice . . . asserting his intent to stand on the complaint, at which time an order to dismiss the action would be appropriate." *Shane v. Fauver*, 213 F.3d 113, 116 (3d Cir. 2000).