NOT FOR PUBLICATION (Document Nos. 15, 21, 22, 24, 25, 31, 55, 56)

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF NEW JERSEY**
**CAMDEN VICINAGE**

| | | |
|---|---|---|
| RUSS SMITH,<br><br>Plaintiff,<br><br>v.<br><br>TRUSTED UNIVERSAL STANDARDS IN ELECTRONIC TRANSACTIONS, INC., MICROSOFT, INC., CISCO SYSTEMS, INC., and COMCAST CABLE COMMUNICATIONS, LLC.,<br><br>Defendants. | : | Civil No. 09-4567 (RBK/KMW)<br><br>**OPINION** |

**KUGLER**, United States District Judge:

This matter arises out alleged improper monitoring and blocking of internet activities. Presently before the Court are several motions: 1) the Motion to Remand by Plaintiff Russ Smith (Doc. No. 15); 2) the Motion to Dismiss by Defendant True Ultimate Standards Everywhere, Inc. (TRUSTe)[1] (Doc. No. 21); 3) the Motion to Dismiss by Defendant Comcast Cable Communications, LLC (Doc. No. 22); 4) the Motion to Dismiss by Defendant Cisco Systems, Inc. (Doc. No. 24); 5) the Motion to Dismiss by Defendant Microsoft, Inc. (Doc. No. 25)[2]; 6) the

[1] Improperly named in the Complaint as Trusted Universal Standards in Electronic Transactions, Inc.

[2] In support of the Motions at Document Numbers 22, 24, and 25, Defendants Comcast, Cisco, and Microsoft submitted a joint memorandum of law.

Motion for Leave to File an Amended Complaint by Plaintiff (Doc. No. 31); 7) the Motion for Leave to File a Sur-Reply by Plaintiff (Doc. No. 55); and 8) the Motion to Strike by Plaintiff (Doc. No. 56). For the reasons discussed below, the Motion to Remand and the Motion to Strike are denied. The Motions to Dismiss, the Motion for Leave to File a Sur-Reply, and the Motion for Leave to File an Amended Complaint are granted.

## I. BACKGROUND

Exactly what is alleged to have happened in this case is somewhat unclear. Plaintiff, proceeding pro se, filed a Complaint in excess of ninety-two paragraphs and sought relief for a number of "counts" that do not amount to any cognizable cause of action. As well as the Court can determine, Plaintiff alleges as follows.

Plaintiff is a subscriber of Comcast's Broadband Internet Services. Twice Comcast blocked all of Plaintiff's outgoing email, once on March 9, 2009, and again on April 16, 2009. After the first blocking, Plaintiff called Comcast and was told it detected "spam e-mail" coming from his account. Compl. at ¶ 39. Plaintiff asked for evidence of what was wrong, but Comcast refused his request, saying it was "proprietary." Compl. at ¶ 39. Comcast also told him that he would not have to worry about any additional email blocking if he subscribed to a higher level of service. This phone call, however, was not the final word from Comcast.

In a letter dated April 6, 2009, Comcast claimed that the blocking was due to a report from a third party, IronPort, owned by Cisco, and due to an IP address "reputation." Compl. at ¶ 40. Cisco later claimed the report came from Spamhaus, an entity outside the United States. Plaintiff alleges that to provide the report, Cisco intercepted and "eavesdropped" on his communications.

After Comcast blocked Plaintiff's communications for the second time, Plaintiff filed a "Watchdog Complaint" against Comcast with TRUSTe. TRUSTe operates a website that provides a complaint service, whereby internet users can verify web site privacy policies and file complaints against companies that display the TRUSTe verification seal. In these complaints, users allege that they have encountered problems with their personal information with a TRUSTe licensee, whereupon TRUSTe mediates and decides the dispute. In Plaintiff's complaint about Comcast, he alleged that it failed to adhere to its privacy policy by not sufficiently explaining why his communications were blocked. TRUSTe determined that Comcast had supplied the information they used to make their decision.

This interaction with TRUSTe was not Plaintiff's first. Indeed, sometime in September 2008, Plaintiff filed a Watchdog Complaint against Microsoft. Microsoft provides a service known as Frontbridge, which compiles information about internet mail servers by "intercepting Internet e-mail traffic and creat[ing] IP address 'blacklists/blocklists.'" Compl. at ¶ 20. Microsoft in turn distributes these lists to third parties or permits those using Microsoft services to use them for the purpose of blocking email communications of the IP addresses on the lists. On July 3, 2008, Microsoft included the IP address of Plaintiff's email server in a blacklist and distributed it to third parties, which resulted in his email being blocked. After Plaintiff complained to Microsoft, it sent him a response on July 7, 2008, explaining that they did not retain the evidence of his alleged spam. They also did not provide him any information that caused Microsoft to blacklist his IP address. Microsoft again placed Plaintiff on a blacklist on September 23, 2008, but again did not provide him any information about his blacklisting.

As a result, Plaintiff filed a Watchdog Complaint against Microsoft. TRUSTe responded

that his complaint did not fall within the scope of their program because TRUSTe did not certify the Frontbridge service, though it did certify other Microsoft services.

Plaintiff commenced suit against Comcast, Cisco, Microsoft, and TRUSTe in the Superior Court of New Jersey on July 29, 2009. Defendants timely removed the Complaint to this Court on September 4, 2009. The removed Complaint alleges a number of "counts" against each Defendant that really do not amount to separate causes of action. See, e.g., Compl. at ¶ 54 ("Count 1 [against TRUSTe]: failing to provide a reasonable resolution to complaint filed by Plaintiff against Microsoft"). As has been interpreted by Defendants, and seemingly not disputed by Plaintiff, the Complaint really alleges the following causes of action:

> 1) violation of the New Jersey Consumer Fraud Act (NJCFA), N.J. Stat. Ann. § 56:8-2 et seq. (against TRUSTe, Comcast, Cisco, and Microsoft);
>
> 2) breach of contract (against TRUSTe, Comcast, Cisco, and Microsoft);
>
> 3) violation of the Federal Wiretap Act, 18 U.S.C. § 2510 et seq. (against Comcast and Cisco);
>
> 4) violation of the Pen Register Act, 18 U.S.C. § 3121 et seq. (against Comcast and Cisco);
>
> 5) violation of the New Jersey Wiretapping and Electronic Surveillance Control Act, N.J. Stat. Ann. § 2A:156A-1 et seq. (against Comcast and Cisco);
>
> 6) defamation (against Microsoft and Cisco);
>
> 7) violation of Comcast's local franchise agreement with the City of Ocean City (against Comcast); and
>
> 8) violation of the Cable Communications Policy Act of 1984, 47 U.S.C. § 521 et seq. (against Comcast).

Plaintiff filed the Motion to Remand on September 18, seeking remand of only the state law claims. Defendants TRUSTe, Comcast, Cisco, and Microsoft each separately moved to

dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6) on September 29. On October 9, Plaintiff sought leave to file the First Amended Complaint. Plaintiff also filed two ancillary Motions that are discussed in the footnote below.[3] The Motions are now all briefed and ripe for review.

## II. STANDARD

Under Federal Rule of Civil Procedure 12(b)(6), a court may dismiss an action for failure to state a claim upon which relief can be granted. With a motion to dismiss, "'courts accept all factual allegations as true, construe the complaint in the light most favorable to the plaintiff, and determine whether, under any reasonable reading of the complaint, the plaintiff may be entitled to relief.'" Fowler v. UPMC Shadyside, 578 F.3d 203, 210 (3d Cir. 2009) (quoting Phillips v. County of Allegheny, 515 F.3d 224, 233 (3d Cir. 2008)). In other words, a complaint survives a motion to dismiss if it contains sufficient factual matter, accepted as true, to "state a claim to relief that is plausible on its face." Bell Atlantic Corp. v. Twombly, 550 U.S. 544, 570 (2007).

In making this determination, a court must engage in a two part analysis. Ashcroft v. Iqbal, 129 S. Ct. 1937, 1949-50 (2009); Fowler, 578 F.3d at 210-11. First, the court must

---

[3] On November 10, 2009, Plaintiff sought leave of the Court to file an untimely brief in opposition to the Comcast, Cisco, and Microsoft Motions. Doc. No. 39. Plaintiff attached a proposed brief. After the Court granted Plaintiff leave to file, Doc. No. 41, Plaintiff filed a brief that differed from the one previously attached. Compare Doc. No. 45, with Doc. No. 39. On December 8, 2009, counsel for TRUSTe filed a letter with the Court, objecting to Plaintiff's brief and urging its rejection. Doc. No. 47. Plaintiff filed the Motion to Strike the letter. Doc. No. 56. Because the Court otherwise accepts the pro se Plaintiff's brief and because counsel's letter does not otherwise prejudice or influence the decision of this case, Plaintiff's Motion to Strike is denied.

Plaintiff also filed a Motion for Leave to File a Sur-Rely to Defendants' Joint Reply. See Doc. No. 55. Pursuant to Local Civil Rule 7.1(d)(6), Plaintiff's Motion is granted, and the Court will accept and consider the sur-reply brief attached to the Motion.

separate factual allegations from legal conclusions. Iqbal, 129 S. Ct. at 1949. "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." Id. Second, the court must determine whether the factual allegations are sufficient to show that the plaintiff has a "plausible claim for relief." Id. at 1950. Determining plausibility is a "context-specific task" that requires the court to "draw on its judicial experience and common sense." Id. A complaint cannot survive where a court can only infer that a claim is merely possible rather than plausible. See id.

## III. DISCUSSION

### A. Motion to Remand

As an initial matter, Plaintiff has moved to remand the state law claims in this dispute. Defendants oppose, arguing that remand is improper under 28 U.S.C. § 1441(c). Def. remand br.(26) at 4.[4] The Court agrees.

Under 28 U.S.C. § 1441(c), a district court, in its discretion, may remand all matters previously removed in which State law predominates. But this discretion applies only where federal question claims are "separate and independent." Borough of W. Mifflin v. Lancaster, 45 F.3d 780, 786 (3d Cir. 1995) (quoting § 1441(c)). Federal question claims are not separate and independent where plaintiff seeks relief for a single injury, "arising from an interrelated series of events or transactions." Id. Here, Plaintiff's federal question claims arise out of the same series of events as his related state law claims. He has alleged a course of conduct where the Defendants allegedly breached agreements with him in furtherance of illegal wiretapping activities. No separate and independent claim exists under these circumstances, and thus the

[4] All Defendants joined in opposition to Plaintiff's Motion to Remand. See Doc. No. 26.

Court cannot grant remand. Plaintiff's Motion is denied.

The Court now turns to the merits of the individual Motions to Dismiss.

**B. TRUSTe Motion**

Defendant TRUSTe asserts that the two claims against it (NJCFA, breach of contract) should be dismissed because 1) Plaintiff lacks standing to pursue his claims; 2) the NJCFA is faulty because Plaintiff has not pled an ascertainable loss and/or a consumer transaction; and 3) Plaintiff has failed to allege the existence of any contact. TRUSTe br.(21) at 8-14. Plaintiff responds by essentially arguing that the deficiencies in his Complaint are remedied by his proposed First Amended Complaint. Pl. br.(45) at 4-5. The Court agrees with TRUSTe's arguments and will grant the Motion to Dismiss.

Even though TRUSTe significantly briefed the standing issue, the Court finds that Plaintiff's Complaint is more readily and clearly disposed of on its pleading deficiencies. Thus, the Court reserves analysis on the standing issue and turns to the shortcomings of the individual claims.

**1. NJCFA**

TRUSTe argues that the NJCFA claim is faulty because Plaintiff has not pled an ascertainable loss and/or a consumer transaction. TRUSTe br.(21) at 12-13. The NJCFA provides "[a]ny person who suffers any ascertainable loss of moneys or property, real or personal, as a result of the use or employment by another person of any method, act, or practice declared unlawful under this act . . . may bring an action . . . in any court of competent jurisdiction." N.J. Stat. Ann. § 56:8-19. Thus, to state a claim under the NJCFA, a plaintiff must allege (1) unlawful conduct by the defendants; (2) an ascertainable loss on the part of the

plaintiff; and (3) a causal relationship between the defendants' unlawful conduct and the plaintiff's ascertainable loss. New Jersey Citizen Action v. Schering-Plough Corp., 842 A.2d 174, 176 (N.J. Super. Ct. App. Div. 2003). As is relevant to this dispute, one type of unlawful conduct is fraud in the connection with the sale or advertisement of merchandise. See N.J. Stat. Ann. § 56:8-2. Under that provision, it is unlawful to use or employ "[1] any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, [2] in connection with the sale or advertisement of any merchandise or real estate . . . ." Id.

It is apparent on the face of the Complaint that Plaintiff has not plead any ascertainable loss of moneys or property (real or personal) resulting from TRUSTe's actions. Ascertainable loss requires that the plaintiff show "a quantifiable or otherwise measurable loss" from the unlawful practice. See Thiedemann v. Mercedes-Benz USA, LLC, 872 A.2d 783, 786 (N.J. 2005). In breach of contract or misrepresentation cases, ascertainable loss is shown by "out-of-pocket loss or a demonstration of loss in value." Id. at 792. Here, Plaintiff has not pled any loss whatsoever vis-a-vis TRUSTe, and indeed the only monetary relief he seeks is the costs of bringing suit. Compl. at ¶ 92i. At most, the Complaint alleges that TRUSTe repeatedly failed to act, see Compl. at ¶¶ 53-63, but it in no way creates a plausible inference that those failures led to some quantifiable or otherwise measurable loss of money or property. Without this showing, Plaintiff's Complaint cannot survive. See Dabush v. Mercedes-Benz USA, LLC, 874 A.2d 1110, 1116 (N.J. Super. Ct. App. Div. 2005). Therefore, the Court could grant TRUSTe's Motion to Dismiss as to the NJCFA claim on this ground alone.

But in addition to Plaintiff's failure to plead ascertainable loss, he also failed to plead fraud in connection with the sale or advertisement of any merchandise or real estate. This is a second sufficient ground for dismissal. Simply stated, the purpose of the NJCFA is "to protect consumers engaging in consumer transactions." Directv, Inc. v. Marino, No. 03-5606, 2005 WL 1367232, at *3 (D.N.J. June 8, 2005) (citing J&R Ice Cream Corp. v. California Smoothing Licensing Corp., 31 F.3d 1259, 1272 (3d Cir. 1994)). The NJCFA only creates a cause of action for "bona fide consumers of [a] product." See Grauer v. Norman Chevrolet Geo, 729 A.2d 522, 524 (N.J. Super. Ct. Law Div. 1998). The absence of a consumer transaction is fatal to a NJCFA claim. Directv, Inc., 2005 WL 1367232, at *3. Plaintiff alleges that TRUSTe's privacy seal program constitutes a sale or advertisement of merchandise because TRUSTe offers the seal to businesses and those businesses in turn offer goods and services for sale. Pl. br.(45) at 4, ¶ 9. But this argument fails to show how Plaintiff engaged in a consumer transaction. He did not buy anything from TRUSTe. Moreover, even using his own logic (and assuming arguendo that TRUSTe's placement of its seal on others' websites could produce a consumer transaction) he did not buy anything in reliance on TRUSTe's seal. Simply put, there was no transaction. Therefore, the Court must grant TRUSTe's Motion to Dismiss the NJCFA claim.

**2. Breach of Contract**

TRUSTe also moves to dismiss the breach of contract claim, arguing that the Complaint does not allege the existence of any contract between Plaintiff and TRUSTe. TRUSTe br.(21) at 14. Plaintiff responds by essentially arguing that the proposed First Amended Complaint pleads the existence of a contract. Pl. br.(45) at 4, ¶ 8. In other words, he seemingly agrees that the Complaint as presently stated fails to allege breach of contract. This is a wise concession as it

clearly does not.

To state a claim for breach of contract, a party must allege 1) the parties entered into an agreement, 2) the plaintiff satisfied the terms of the agreement, 3) the defendant failed to satisfy at least one term of the agreement, and 4) the breach caused the plaintiff to suffer a loss. Cargill Global Trading v. Applied Development Co., No. 03-5920, - - - F. Supp. 2d - - - -, 2010 WL 1568457, at *14 (D.N.J. Apr. 21, 2010). The oft-repeated elements of a basic contract are offer, acceptance, and consideration. See Smith v. SBC Commc'ns, Inc., 839 A.2d 850, 861 (N.J. 2004). Liberally construing the Complaint, it seems as if the only thing that TRUSTe "offers" is a gratuitous service whereby the public can complain about TRUSTe licensees. See Compl. at ¶¶ 8-11. Of course it is blackletter law that a gratuity without consideration does not form a contract. See Rex Distribs. v. Jensen & Mitchell, 21 A.2d 327, 328 (N.J. 1941). Plaintiff alleged no plausible inference of consideration given to TRUSTe; he merely alleges that he availed himself of its free service. Therefore, the breach of contract claim fails and TRUSTe's Motion is granted as to the breach of contract claim.

### C. Comcast, Cisco, and Microsoft Motions

Defendants Comcast, Cisco, and Microsoft move to dismiss the Complaint on various deficiencies of the individual claims, and on the basis of immunity as to all of the claims. Analysis must begin with the immunity challenge.

#### 1. Immunity

Comcast, Cisco, and Microsoft argue that they are immune from suit for all of Plaintiff's claims because they are entitled to "Good Samaritan" immunity under the Communications

Decency Act (CDA), 47 U.S.C. § 230(c). Comcast br.(22) at 5.[5] Plaintiff lodges a number of challenges to the defense, most importantly arguing that these Defendants acted in bad faith in blacklisting his IP address, blocking his email, and failing to disclose information about their decisions. Pl. br.(45) at 8, ¶ 13g. The Court is not convinced (at least on the present record) that Comcast, Cisco, or Microsoft is immune from suit.

Under the CDA's Good Samaritan immunity provision, a provider or user of "an interactive computer service" cannot be held liable for

> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

47 U.S.C. § 230(c)(2).[6] An "interactive computer service" is defined as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." § 230(f)(2). An "access software provider" is defined as "a provider of software (including client or server software), or enabling tools that do any one or more of the following: (A) filter, screen, allow, or disallow content; (B) pick, choose, analyze, or digest content; or (C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content." § 230(f)(4).

---

[5] For purposes of simplicity, the Court will refer to the Comcast, Cisco, and Microsoft joint brief as simply the "Comcast brief."

[6] The reference to paragraph "(1)" in § 230(c)(2)(B) should likely refer to paragraph "(A)."

In its basic form, a party is entitled to immunity for causes of action arising out of its efforts to restrict or block material when the party 1) is a provider or user of an interactive computer service; 2) acted in good faith; and 3) subjectively believed that the material blocked or restricted was a) obscene, b) lewd, c) lascivious, d) filthy, e) excessively violent, f) harassing, or g) otherwise objectionable. See § 230(c)(2)(A); see also e360Insight, LLC v. Comcast Corp., 546 F. Supp. 2d 605, 607-08 (N.D. Ill. 2008) (holding § 230(c)(2) involves a subjective determination). Similarly, a party is entitled to immunity when it 1) is a provider or user of an interactive computer service; 2) the party acts to enable or make available to a) information content providers, b) or others; 3) technical means to restrict access to materials that are subjectively a) obscene, b) lewd, c) lascivious, d) filthy, e) excessively violent, f) harassing, or g) otherwise objectionable. See § 230(c)(2)(B).

Whether immunity applies here requires the Court to address at least one threshold issue: Does § 230 immunity apply where the actions taken involve blocking (or providing the means to block) spam email? More succinctly, can spam email be "material" that is subjectively "otherwise objectionable"? This question was squarely addressed by the court in e360Insight, LLC v. Comcast Corporation, 546 F. Supp. 2d 605, 607-08 (N.D. Ill. 2008), and affirmatively answered yes. This Court agrees with that answer.

Congress expressly intended the CDA "to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services[.]" § 230(b)(3). Congress further intended "to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or

inappropriate online material[.]" § 230(b)(4). Both of these goals are served when an entity subjectively deems spam "otherwise objectionable" and chooses to block it. Cf. 15 U.S.C. § 7701(a)(5) (Congressional findings in the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM) noting that "[t]he convenience and efficiency of electronic mail are threatened by the extremely rapid growth in the volume of unsolicited commercial electronic mail. Unsolicited commercial electronic mail is currently estimated to account for over half of all electronic mail traffic, up from an estimated 7 percent in 2001, and the volume continues to rise. Most of these messages are fraudulent or deceptive in one or more respects."). The Court does not find merit in Plaintiff's argument that the blocked material must be "obscene, lewd, filthy, excessively violent, or harassing." See Pl. br.(45) at 6, ¶ 13a. Congress included the phrase "or otherwise objectionable" in its list of restrictable materials, and nothing about the context before or after that phrase limits it to just patently offensive items. See Langdon v. Google, Inc., 474 F. Supp. 2d 622, 631 (D. Del. 2007) (rejecting argument that § 230 immunity did not apply where defendants restricted ads that were not obscene or harassing, reasoning that "or otherwise objectionable" permitted restriction); see also Doe v. SexSearch.com, 502 F. Supp. 2d 719, 726 (N.D. Ohio 2007) (noting § 230 immunity should be interpreted broadly), aff'd on other grounds, 551 F.3d 412 (6th Cir. 2008).

But the mere finding that spam email can be subjectively "otherwise objectionable" does not conclude the immunity inquiry. Comcast, Cisco, and Microsoft must also satisfy the other elements for protection. Turning first to Comcast, the Court cannot grant immunity on the present record because it is not clear that Comcast acted in good faith. Construing the Complaint broadly, and giving the pro se Plaintiff the benefit of the doubt, Plaintiff alleges bad faith by

Comcast. After the first email block, Plaintiff alleges that he called Comcast and was told that "he would not have to worry about any e-mail blocking if [he] subscribed to a higher level of service." Compl. at ¶ 39. This explanation, assumed true, seems to suggest that Comcast was not concerned that people were receiving large quantities of emails, or concerned about the content of the emails, but rather was concerned that Plaintiff had not purchased a sufficient level of service. This is not a good faith belief that the emails were objectionable, but rather a belief that they violated a service agreement. Additionally, Plaintiff pleads that Comcast failed to produce an explanation for the second email block, which as argued somewhat inartfully in his brief, seems to suggest bad faith. One would expect that if an interactive computer service had acted in good faith, it could and would come forward with the legitimate basis for its actions when questioned (though the Court is not suggesting they must do so). Importantly, Comcast has not produced anything to show that it in fact acted in good faith to screen objectionable spam, rather than to enforce its terms of service.[7] Therefore, the Court cannot grant CDA immunity to Comcast, at least not on the present record.

Likewise, the Court cannot grant immunity as to Cisco or Microsoft. These Defendants argue that they are access software providers, and thus are entitled to immunity under § 230(c)(2)(B) because they provide the technical means to restrict access to material. Comcast reply(48) at 4. At no point do Cisco or Microsoft argue they are "users" of an interactive

[7] The Court recognizes that the present Motion is a motion to dismiss, under which the Court cannot consider matters extraneous to the Complaint (with some limited exceptions). Thus, that Comcast did not submit affidavits or other evidence in support of its immunity argument is understandable. That said, nothing about this Opinion forecloses Comcast from filing a motion for summary judgment, which can be filed "at any time," Fed. R. Civ. P. 56(c)(1)(A), attaching appropriate evidence.

computer service, thus they must be saying they are a provider.

However, assuming Cisco and Microsoft are access software providers, such status alone is not enough to secure immunity. Immunity only extends to users or providers of an "interactive computer service." § 230(c)(2). While the definition of interactive computer service includes "access software provider," it also requires that the access software provider "provides or enables computer access by multiple users to a computer server . . . ." § 230(f)(2). At no point do Cisco or Microsoft represent that they satisfy this critical access element. Cf. Comcast reply(48) at 4 (discussing Cisco's and Microsoft's status as access software providers, but not discussing whether they provide access by multiple users to a computer server). Cisco's and Microsoft's reliance on Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169 (9th Cir. 2009) and Optinrealbig.com, LLC v. Ironport Systems, Inc., 323 F Supp. 2d 1037 (N.D. Cal. 2004) to support their argument is misplaced. In Zango, where the Ninth Circuit held that an internet security software company was entitled to Good Samaritan immunity, the court specifically analyzed whether the defendant provided access to multiple users to a computer server. 568 F.3d at 1175-76. Likewise, in Optinrealbig.com, the court granted Good Samaritan immunity to a company that forwarded email recipients' spam complaints to internet service providers, but only after determining that the defendant was a user of interactive computer services. 323 F. Supp. 2d at 1047. Neither Cisco nor Microsoft has made the showing that they are providers or users of interactive computer services. Therefore, the Court cannot grant them immunity.

Notwithstanding the failing of the immunity defenses, Comcast, Cisco, and Microsoft also argue that each of the claims against them are otherwise deficient.

**2. NJCFA (against Comcast, Cisco, and Microsoft)**

Comcast, Cisco, and Microsoft first challenge the NJCFA claims in the same manner as TRUSTe, namely that Plaintiff failed to allege an ascertainable loss. Comcast br.(22) at 20. Plaintiff's response is effectively a concession that they are right, as he merely cites to his proposed First Amended Complaint as showing that he suffered an ascertainable loss. See Pl. br.(45) at 5, ¶12, 14, ¶ 37. The Court finds that Plaintiff failed to plead ascertainable loss in the Complaint.

As was true with Plaintiff's NJCFA claims against TRUSTe, the Complaint fails to allege that any of these Defendants' fraudulent actions caused him any quantifiable or otherwise measurable loss. See Thiedemann, 872 A.2d at 786. Plaintiff merely pleads a claim on the basis that these Defendants breached contracts with him. See Compl. at ¶¶ 67, 76, 82. At no point does he plead or even raise the inference of loss flowing from these alleged wrongs. Thus, Comcast's, Cisco's, and Microsoft's Motion must be granted as to the NJCFA claims.

**3. Breach of Contract (against Comcast, Cisco, and Microsoft)**

Comcast, Cisco, and Microsoft also move to dismiss the Complaint for failure to allege breach of contract. Comcast br.(22) at 18. Comcast argues that nothing in the Complaint alleges a breach of the Subscriber Agreement, an agreement which in fact permits Comcast to do exactly what it did–filter and block email. Comcast br.(22) at 18. Cisco and Microsoft assert that the claims against them are simply based on their online privacy policies, and those policies are insufficient to form a contract because they are not definite and no consideration was given. Comcast br.(22) at 18-19. Plaintiff's response once again is that the shortcomings of the Complaint are cured by the proposed First Amended Complaint. Pl. br.(45) at 5, ¶ 12. The Court agrees that Plaintiff's breach of contract claims must be dismissed.

**a. Comcast**

To support the breach of contract claim against Comcast, Plaintiff alleges the following specific breaches: 1) it failed to provide him access to the personally identifiable information (PII)[8] that it compiled about him; 2) it failed to allow him access to correct the PII that Comcast compiled about him; 3) it provided a false and/or misleading explanation of why his email communications were blocked; 4) it monitored and blocked specific "protocols and services, such as e-mail," while representing that monitoring and blocking is "protocol agnostic"; and 5) it posted policies on its website that inconsistently state how internet communications are monitored and/or blocked. Compl. at ¶¶ 68-73. Plaintiff's claimed breaches are seemingly based on three provisions that he believes form part of the agreement with Comcast. First, he alleges that the 2009 Comcast Customer Privacy Notice states:

> "How can I see my personally identifiable information [PII] or CPNI and correct it if necessary? You may examine and correct, if necessary, the personally identifiable information regarding you that is collected and maintained by Comcast in our regular business records."

Compl. at ¶ 17. Second, he alleges that Comcast's Network Management FAQ states:

> Will the technique target P2P or other applications, or make decisions about the content of my traffic?
>
> No. The new technique is "protocol-agnostic," which means that the system does not manage congestion based on the applications being used by customers. It is content neutral, so it does not depend on the type of content that is generating traffic or congestion. Said another way, customer traffic is congestion-managed not based on their applications, but based on current network conditions and recent bytes transferred by users.

Compl. at ¶ 18. Third, he alleges that the Privacy Policy further states:

---

[8] Personally identifiable information is discussed below in section III.C.9.

> We will not read your outgoing or incoming e-mail . . . We also monitor the performance of our Service and your Service connection in order to manage, maintain, and improve the Service and your connection to it. We (or our third party providers) use tools to help prevent and block "spam" e-mails, viruses, spyware, and other harmful or unwanted communications and programs on the Service. These tools may automatically scan your e-mails . . . and other files and communications in order to help us protect you and the Service against these harmful or unwanted communications and programs. However, these tools do not collect or disclose personally identifiable information about you . . .

Compl. at ¶ 37b.

Comcast asserts that under the Subscriber Agreement, attached to the Friedman Certification,[9] it was permitted to block and filter email, which is all that happened here. Comcast br.(22) at 18. Comcast also asserts (though in the context of defending against the NJCFA claim) that Plaintiff has failed to show any loss from any of Comcast's alleged breaches. Comcast br.(22) at 20. Comcast seemingly agrees that provisions of the Privacy Policy do form part of the agreement with Plaintiff, but is it not clear whether they also agree that the Network FAQ also forms apart of the agreement. See Comcast br.(22) at 10 ("The Subscriber Agreement also reflects Plaintiff's express consent to the terms of Comcast's Privacy Policy."). However, at this stage of the litigation, the Court finds that all of the above language formed part of the agreement, but the Court also finds that Plaintiff has failed to allege the requisite loss from the alleged breaches.

Some courts have held that general statements like "privacy policies" do not suffice to

[9] The Court can consider the Subscriber Agreement because it is a document expressly relied on in the Complaint and is seemingly an undisputedly authentic document on which Plaintiff's claims are based. See In re Burlington Coat Factory Sec. Litig., 114 F.3d 1410, 1426 (3d Cir. 1997) (holding "a 'document *integral to or explicitly relied* upon in the complaint' may be considered 'without converting the motion [to dismiss] into one for summary judgment'"); Pension Ben. Guar. Corp. v. White Consol. Indus., Inc., 998 F.2d 1192, 1196 (3d Cir. 1993) (holding "a court may consider an undisputedly authentic document that a defendant attaches as an exhibit to a motion to dismiss if the plaintiff's claims are based on the document").

form a contract because they are they are not sufficiently definite. See Dyer v. Nw. Airlines Corps., 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004); In re Nw. Airlines Privacy Litig., No. 04-126, 2004 WL 1278459, at *6 (D. Minn. June 6, 2004). However, at least one court has held that on a motion to dismiss, a court's inquiry should be whether it is plausible that the policy or statement constituted a contract. See Meyer v. Christie, No. 07-2230, 2007 WL 3120695, at *4 (D. Kan. Oct. 24, 2007); see also In re Jetblue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 325 (E.D.N.Y. 2005) (holding privacy policy can form a contract). In making this inquiry, a court must determine whether the plaintiff has alleged that he relied on the policy. See Meyer, 2007 WL 3120695, at *5. This Court finds this line of logic persuasive. Applied here, giving Plaintiff the benefit of the doubt, he seems to have alleged that all of the above provisions were part of his agreement with Comcast and that he relied on them. See, e.g., Compl. at ¶¶ 13-18. Moreover, he seems to have alleged that Comcast refused his request to see and correct his PII, alleged that it used non-neutral monitoring and blocking techniques, and alleged that they failed to adequately explain how his email was identified as being spam (i.e., he alleged they blocked his email for an impermissible reason). See Compl. at ¶¶ 39-41, 46.

Nevertheless, even assuming that a contract did exist between Comcast and Plaintiff that incorporated the above terms, and even assuming that Comcast violated those terms, Plaintiff must still plead loss flowing from the breach to sustain a claim. Cargill Global Trading, 2010 WL 1568457, at *14; see also In re Jetblue, 379 F. Supp. 2d at 327 (holding even if plaintiffs demonstrated a contract based on privacy policy, plaintiffs' breach claim failed because they could not allege loss). He has not done so. As discussed at length above, Plaintiff has not pled any loss whatsoever in the Complaint. Therefore, he has not stated a claim for breach of contract

and Comcast's Motion must be granted.

**b. Cisco and Microsoft**

The same result must also be reached as to the alleged breach claims against Cisco and Microsoft. But as to these Defendants, not only has Plaintiff failed to allege damages (which the Court will not rehash), he has also failed to allege a contract. Plaintiff once again seems to concede a failure to state a claim, and directs the Court's attention to the proposed First Amended Complaint. See Pl. br.(45) at 5, ¶12.

The Complaint squarely alleges breach claims against Cisco and Microsoft based on their privacy policies. See Compl. at ¶¶ 22, 26. But Plaintiff has failed to allege how these statements form a contract. He has failed to allege what offer was made that he accepted and what consideration was given. See Smith, 839 A.2d at 861 (basic elements of a contract); see also See Meyer, 2007 WL 3120695, at *4 (holding a court's inquiry on motion to dismiss should be whether it is plausible that a policy or statement constituted a contract). Nothing in the Complaint even remotely suggests that Cisco or Microsoft owed any contractual obligation to Plaintiff. It is of course elementary that absent a contract, there can be no breach. Therefore, the Court grants Cisco's and Microsoft's Motion to Dismiss as to the breach of contract claims.

**4. Federal Wiretap Act (against Comcast and Cisco)**

Comcast and Cisco move to dismiss the Federal Wiretap Act claims against them, arguing the claims should be dismissed because 1) Plaintiff consented to the interception of his communications, 2) any interception was lawful under the service provider exception, and 3) Plaintiff failed to allege the essential elements of a claim. Comcast br.(22) at 7. Plaintiff responds that dismissal is inappropriate because 1) Cisco's acts are not protected by whatever

consent Plaintiff gave to Comcast, 2) Comcast is not entitled to the service provider exception, 3) Comcast's policies indicate that they "may use" a technique that "may violate" federal law, and 4) Plaintiff is entitled to discovery to determine what if any eavesdropping took place, what if any interception took place, and what if any devices were used. Pl. br.(45) at 10-11, ¶¶ 20-24. On the basis of the Complaint, the Court is compelled to grant dismissal.

The Wiretap Act provides that "[e]xcept as otherwise specifically provided in this chapter any person who-(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication; . . . shall be subject to suit as provided in subsection (5)." 18 U.S.C § 2511(1)(a). The Act further provides for civil liability as follows: "[A]ny 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(a). Setting aside for the moment the consent and service provider exception defenses, it seems clear that under Iqbal, Plaintiff has failed to state a claim. The Complaint merely states in a conclusory fashion that Comcast violated the Wiretap Law "by monitoring Plaintiff's Internet communications and/or allowing third parties to do so." Compl. at ¶ 65. It contains the same conclusory allegation as to Cisco. Compl. at ¶ 89. Plaintiff has not made any factual averments that any of his communications were in fact intercepted. If any doubt remains on that point, Plaintiff puts it to rest with his brief wherein he admits that the Complaint is a mere fishing expedition for liability:

> Plaintiff does not know the exact reason for being blocked. It may be due to eavesdropping or some other reason. It is also possible that all reports, blocking and blacklisting are erroneous and *no eavesdropping took place*. Discovery is necessary to

determine the exact circumstances of what happened and what devices were used, if any. Compl. at 11, ¶ 23 (emphasis added). What Plaintiff has alleged in effect is the mere possibility of liability, but not plausible liability. See Iqbal, 129 S. Ct. at 1949. Absent facts to support his speculation, he is not entitled to discovery to see what he may find. See id. at 1950 ("Rule 8 marks a notable and generous departure from the hyper-technical, code-pleading regime of a prior era, but it does not unlock the doors of discovery for a plaintiff armed with nothing more than conclusions."). On the basis of the Complaint as it now exists, Plaintiff is not entitled to relief and Comcast's and Cisco's Motions must be granted as to the Federal Wiretap Act claims.

**5. New Jersey Wiretapping and Electronic Surveillance Control Act (against Comcast and Cisco)**

Comcast and Cisco also move to dismiss the New Jersey Wiretapping claims since it largely tracks the Federal Wiretap Act and Plaintiff has otherwise failed to state a claim under the Federal analogue. Comcast br.(22) at 17. The Court agrees, see Pascale v. Carolina Freight Carriers Corp., 898 F. Supp. 276, 281 (D.N.J. 1995); PBA Local No. 38 v. Woodbridge Police Dept., 832 F. Supp. 808, 824 (D.N.J. 1993), and therefore grants Comcast's and Cisco's Motions to Dismiss the New Jersey Wiretapping and Electronic Surveillance Control Act claims.

**6. Pen Register Act (against Comcast and Cisco)**

Comcast and Cisco also move to dismiss the Pen Register Act claims against them. The Court can grant that request in short order. Under the Pen Register Act, "no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978." 18 U.S.C § 3121. The Pen Register Act itself does not contain a civil liability provision, but liability for violation

of the Act is available under the Stored Communications Act, 18 U.S.C. § 2707(g). See Bansal v. Russ, 513 F. Supp. 2d 264, 279 (E.D. Pa. 2007). However, civil liability under § 2707(g) only applies where there has been "willful disclosure of a 'record'" by an "investigative or law enforcement officer, or a governmental entity." § 2707(g). There are no such government actors in this case, thus no civil liability arises. Plaintiff cites to Diaz v. Allstate Insurance Group, 185 F.R.D. 581, 594 (C.D. Cal. 1998) for the proposition that "Pen Register Acts may be actionable under state law." Pl. br.(45) at 11, ¶ 26. Even if that statement were true, no New Jersey law has been invoked here that would supply such liability. Therefore, the Court grants Comcast's and Cisco's Motion as to the Pen Register Act claims.

**7. Defamation (against Cisco and Microsoft)**

Cisco and Microsoft move to dismiss the defamation claims against them, arguing that Plaintiff has failed to plead the requisite level of fault. Comcast br.(22) at 21. Plaintiff responds by relying on the proposed First Amended Complaint to cure any deficiencies, arguing (under an understandable misapprehension the meaning of fault in a defamation context) that it shows that all Defendants are at fault for various injuries. Pl. br.(45) at 15, ¶ 41. The Court agrees that Plaintiff has failed to plead the requisite elements of a defamation claim and grants dismissal.

The elements of a defamation are "'(1) the assertion of a false and defamatory statement concerning another; (2) the unprivileged publication of that statement to a third party; and (3) fault amounting at least to negligence by the publisher.'" Leang v. Jersey City Bd. of Educ., 969 A.2d 1097, 1114 (N.J. 2009) (quoting DeAngelis v. Hill, 847 A.2d 1261, 1267-68 (N.J. 2004)). Where the person defamed is a private party and the statement involves a private matter, the fault element is satisfied by showing that the person communicated the false statement "while acting

negligently in failing to ascertain the truth or falsity of the statement before communicating it." Feggans v. Billington, 677 A.2d 771, 775 (N.J. Super. Ct. App. Div. 1996). In other words, the person failed to take sufficient care to determine the truth of the statement before uttering it.

In this case, Plaintiff has made mere conclusory allegations that he was defamed by Cisco and Microsoft. See Compl. at ¶ 81 ("Microsoft defamed Plaintiff by placing his IP address on blacklists/blocklists for e-mail communications without allowing Plaintiff to review and correct, if necessary, the information that led to these blacklist/blocklist listings."), ¶ 91 ("Cisco defamed Plaintiff by giving a reputation score for e-mail communications to plaintiff's IP address without allowing Plaintiff to review and correct, if necessary, the information that led to the reputation score."). Notably, at no point does he allege that the information communicated about him was actually false, instead he merely claims that he was not permitted to review and change the information. Further, he has not alleged that Cisco or Microsoft acted negligently in communicating their reports. At most he has alleged that they subsequently did not let him review and change what they said, but not that they failed to reasonably determine the truth or falsity of the statements when they were made. Therefore, his defamation claims fail and Cisco's and Microsoft's Motion must be granted.

**8. Comcast's local franchise agreement with the City of Ocean City (against Comcast)**

Comcast moves to dismiss the claim based on its purported failure to comply with the local franchise agreement with the City of Ocean City, alleging that the claim is "wholly conclusory." Comcast br.(22) at 22. Plaintiff responds that the proposed First Amended Complaint cures the deficiencies. Pl. br.(45) at 15, ¶ 43. The Court agrees that the Complaint

fails to state a claim under this count. At no point does Plaintiff identify the agreement, what its terms are, and how Comcast violated them. His claim is an unadorned, barebones claim of liability, which is insufficient. See Iqbal, 129 S. Ct. at 1949-50. Therefore, Comcast's Motion is granted as to the local franchise agreement claim.

**9. Cable Communications Policy Act of 1984 (against Comcast)**

Comcast finally moves to dismiss the claim based on the Cable Communications Policy Act of 1984 (Cable Act), arguing that it is stated in "wholly conclusory terms." Comcast br.(22) at 22. In what by now should be a familiar refrain, Plaintiff claims that the shortcomings of the Complaint are cured by the proposed First Amended Complaint. Pl. br.(45) at 15, ¶ 43. The Court agrees with Comcast and will grant the Motion to Dismiss.

Under the Cable Act, a cable operator has a host of responsibilities, the violation of which are actionable in a civil suit. 47 U.S.C. § 551. As is relevant here, among those responsibilities is a duty to provide cable subscribers access to all "personally identifiable information" about the subscriber that the cable operate collects and maintains. § 551(d). The Cable Act does not define what such information is, but does state what it is not: "the term 'personally identifiable information' does not include any record of aggregate data which does not identify particular persons." § 551(a)(2)(A). One court has noted that the legislative history to the Act states that personally identifiable information "'would include specific information about the subscriber, or a list of names and addresses on which the subscriber is included . . . .'" Scofield v. Telecable of Overland Park, Inc., 973 F.2d 874, 876 n.2 (10 Cir. 1992). Another court has held that a person's name, address, and telephone is quintessential personally identifiable information. Warner v. Am. Cablevision of Kansas City, Inc., 699 F. Supp. 851, 855 (D. Kan. 1988); see also Pruitt v.

Comcast Cable Holdings, LLC, 100 Fed. Appx. 713, 716 (10th Cir. 2004) (finding cable box did not contain personally identifiable information where, inter alia, it did not contain the name address or "any other information regarding the customer").

Liberally construing the Complaint, it seems as if Plaintiff *tried* to allege that Comcast failed to provide him access to his personally identifiable information. See, e.g., Compl. at ¶¶ 39, 45, 75. However, what he *did* allege was that Comcast failed to let him access the information that led to his blocking. Compl. at ¶ 39. Plaintiff has not alleged or created an inference that the information that led to his blocking was somehow personally identifiable information. In fact, on the basis of the Complaint as a whole, it does not seem plausibly alleged that Comcast failed to disclose information that identified him, e.g., his name, address, or telephone number. Therefore, the Court must grant Comcast's Motion to Dismiss as to the Cable Act claim.

**D. Motion to Amend**

Notwithstanding the above, Plaintiff has filed a Motion for Leave to Amend to clarify his claims and to add claims. See Doc. No. 31. In support he attached a voluminous proposed First Amended Complaint (404 total pages with exhibits). See Doc. No. 31. All Defendants jointly opposed the Motion, arguing that leave to amend should be denied because the proposed claims are futile. Comcast br.(37) at 3. Because the Court is mindful of Plaintiff's pro se status (and mindful that he did not have the benefit of the above analysis at the time of his Motion), the Court will grant the Motion and permit Plaintiff to file a Second Amended Complaint.

In brief, a pro se pleading is held to less stringent standards than more formal pleadings drafted by attorney. See Erickson v. Pardus, 551 U.S. 89, 94 (2007). Further, leave to amend is

normally liberally granted under Federal Rule of Civil Procedure 15. See Fed. R. Civ. P. 15(a)(2). Nonetheless, Rule 15 is not permissive of whatever amended pleadings a party wishes to file (pro se or otherwise): leave to amend is not warranted where the proposed amendment would not withstand a motion to dismiss. Massarsky v. Gen. Motors Corp., 706 F.2d 111, 125 (3d Cir. 1983).

Here, without a doubt most of the claims in the proposed First Amended Complaint are futile. However, the Court recognizes that Plaintiff did not have the benefit of the above analysis at the time of his Motion. While the Court is convinced that the attached proposed First Amended Complaint would likely succumb to a motion to dismiss for the same pleading failures as outlined above, the Court is not convinced that there are no facts under which Plaintiff could show he has plausible claims for relief. In other words, an amendment is not per se futile. Thus, the Court is compelled to grant the Motion for Leave to Amend, and to grant Plaintiff leave to file an amended complaint (the Second Amended Complaint) within thirty (30) days of the accompanying Order. But such leave is granted with one added caveat.

Plaintiff must familiarize himself with the directives of Federal Rule of Civil Procedure 8. That Rule requires that a pleading must contain "*a short and plain* statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2) (emphasis added). Certainly 404 total pages does not a short and plain statement make. Whatever amended complaint Plaintiff files must comport with the spirit of the rule.

## IV. CONCLUSION

For the foregoing reasons, the Motion to Remand by Plaintiff Russ Smith is **DENIED**. The Motion to Dismiss by Defendant TRUSTe is **GRANTED**. The Motion to Dismiss by

Defendant Comcast, the Motion to Dismiss by Defendant Cisco, and the Motion to Dismiss by Defendant Microsoft are **GRANTED**. The Motion for Leave to File an Amended Complaint by Plaintiff is **GRANTED** and Plaintiff shall file the Second Amended Complaint within **THIRTY (30) DAYS** of the accompanying Order. The Motion for Leave to File a Sur-Reply by Plaintiff is **GRANTED**. The Motion to Strike by Plaintiff is **DENIED**. An appropriate Order shall follow.

Date: 5-4-10

/s/ Robert B. Kugler
ROBERT B. KUGLER
United States District Judge