UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

JASON COOPER and MEGHNA PARIKH,

Plaintiffs,

-v-

SLICE TECHNOLOGIES, INC. and UNROLLME INC.,

Defendants.

17-CV-7102 (JPO)

OPINION AND ORDER

J. PAUL OETKEN, District Judge:

This case concerns data mining and internet privacy. UnrollMe, a website operated by the Defendants, helps consumers unsubscribe from unwanted emails. But Plaintiffs claim that UnrollMe also sold user data to third parties, in violation of state and federal law. Defendants move to dismiss, arguing that UnrollMe users consented to the sale of their anonymized data. For the reasons that follow, the motion is granted.

I. Background

Defendant Slice Technologies, Inc. is the parent company of Defendant UnrollMe Inc., which operates the UnrollMe website. For simplicity, "UnrollMe" refers both to the Defendants and to the website.

UnrollMe is a free online service that allows people to opt out of mailing lists, newsletters, and other unwanted emails. (Dkt. No. 29 ("Compl.") ¶ 2.) To do so, it asks people for their email usernames and passwords. (Compl. ¶ 3.) But according to the Complaint, UnrollMe sold its customers' email data to third parties. For example, the Complaint alleges that UnrollMe compiled a list of thousands of customers who used the Lyft ridesharing app and sold the list to Lyft's competitor, Uber. (Compl. ¶ 3.)

Plaintiffs seek to represent a class of UnrollMe customers, claiming that UnrollMe did not adequately disclose to consumers the extent of its data mining practices. Plaintiffs assert claims under the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2510 *et seq.*, the Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.*, and California's Invasion of Privacy Act, Cal. Penal Code §§ 630 *et seq.* Plaintiffs also assert common-law unjust enrichment and intrusion-on-privacy claims.

UnrollMe moves to dismiss under Federal Rules of Civil Procedure 12(b)(1) and (b)(6), arguing that Plaintiffs lack standing and that the Complaint fails to state a claim.

II. Legal Standard

In resolving a motion to dismiss for lack of standing, the court "must take all uncontroverted facts in the complaint . . . as true, and draw all reasonable inferences in favor of the party asserting jurisdiction." *Tandon v. Captain's Cove Marina of Bridgeport, Inc.*, 752 F.3d 239, 243 (2d Cir. 2014). However, "the party who invokes the Court's jurisdiction bears the burden of proof to demonstrate that subject matter jurisdiction exists . . . ." *Germain v. M & T Bank Corp.*, 111 F. Supp. 3d 506, 518 (S.D.N.Y. 2015) (quoting *Gonzalez v. Option One Mortg. Corp.*, No. 12 Civ. 1470, 2014 WL 2475893, at *2 (D. Conn. June 3, 2014)).

To survive a motion to dismiss for failure to state a claim, plaintiffs must plead "only enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A claim is facially plausible when plaintiffs plead facts that would allow "the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). "Court[s] must accept as true all well-pleaded factual allegations in the complaint, and 'draw all inferences in the plaintiff's favor.'" *Goonan v. Fed. Reserve Bank of N.Y.*, 916 F. Supp. 2d 470, 478 (S.D.N.Y. 2013) (alteration omitted) (quoting *Allaire Corp. v. Okumus*, 433 F.3d 248, 249–50 (2d Cir. 2006)).

III. Discussion

This motion presents two questions: whether Plaintiffs have standing, and whether the Complaint adequately states a claim. Each is discussed in turn.

A. Standing

The first question is whether Plaintiffs have standing. Standing requires (1) that the plaintiff suffered an injury in fact, (2) that the injury is fairly traceable to the defendant's challenged conduct, and (3) that the injury is likely to be redressed by a favorable decision. *See Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992). An injury must be both "concrete *and* particularized." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1545 (2016) (quoting *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180–181 (2000)).

The parties dispute only one prong of the standing analysis: injury in fact. Here, it is worth delineating the three types of harm that the Complaint hints at: (1) that UnrollMe sold raw email account information, including Plaintiffs' personally identifiable data; (2) that UnrollMe sold redacted—or "anonymized"—email data, stripped of personally identifying information; and (3) that UnrollMe sold anonymized emails, but in such a way that the buyers could potentially "deanonymize" the data and uncover personal information.

The first category of harm—selling non-anonymized data—is the most concrete harm, but the Complaint does not adequately allege that UnrollMe did this. The Complaint merely alleges that UnrollMe "*may have* overlooked information unique to the consumer" when sharing data with third parties. (Compl. ¶ 35 (emphasis added).) For example, the Complaint alleges that "[b]ehind every Lyft email are unique identifiers that can identify each Lyft user." (*Id.*) But that alone is not enough. Just because an original Lyft email includes the user's email address does not mean that the email address was included in the anonymized dataset that UnrollMe sold.

Without more, the Complaint does not adequately allege that UnrollMe sold emails containing personal consumer data.

The third category of harm—the risk that third-party buyers might deanonymize users' data—is the next-greatest measure of harm. But when it comes to standing, the harm is too remote. The Complaint's allegations on this front are (1) that "[r]esearchers have revealed the ease [with] which particular people can be identified from purportedly anonymized data sources," particularly for taxi trips, and (2) that Uber, one of UnrollMe's clients, has a less-than-sterling reputation for snooping on customers. (Compl. ¶¶ 33–36.) But the mere possibility that someone *might* deanonymize Plaintiffs' emails is not enough to constitute injury in fact. *See Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014) ("An allegation of future injury may suffice if the threatened injury is 'certainly impending,' or there is a 'substantial risk' that the harm will occur.") (quoting *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1141 (2013)).

That leaves us with the second category of harm: the act of selling Plaintiffs' anonymized emails. Here, the question is a purely legal one: assuming that UnrollMe's customers do not consent, is the sale of their anonymized email data a concrete injury in fact?

The answer is yes. The Second Circuit recently held—albeit in a summary order—that a plaintiff could sue a company that used "cookies" to monitor and sell internet-browsing data even though the data was anonymized. *Mount v. PulsePoint, Inc.*, 684 F. App'x 32, 34–35 (2d Cir. 2017). The court noted that "unauthorized accessing and monitoring of plaintiffs' web-browsing activity implicates harms similar to those associated with the common law tort of intrusion upon seclusion so as to satisfy the requirement of concreteness." *Id.* at 34. Even though there was no allegation that the data contained personally identifying data, the court

concluded that the relevant authorities "do not signal that individual identification is required for standing purposes." *Id.* at 34−35.

UnrollMe argues that Plaintiffs suffered no injury from the sale of anonymized emails because they consented to UnrollMe using their anonymized data. But that puts the cart before the horse. Whether there was valid consent is a merits issue, not a standing issue. For standing, the question is whether the harm alleged—nonconsensual selling of anonymized emails—is concrete enough. Given that it can be, the question becomes whether the Complaint adequately alleges that the sale was indeed nonconsensual. That issue is examined below.

Accordingly, Plaintiffs have standing to lodge a claim based on the unauthorized sale of anonymized email data.

B. Failure to State a Claim

Having concluded that Plaintiffs have standing, the Court turns to the substance of their allegations. Still, it is important to keep in mind that the only live claim is that UnrollMe sold *anonymized* data; as discussed above, the Complaint does not adequately allege that UnrollMe sold personally identifiable data or that there was a concrete risk of deanonymization, and Plaintiffs lack standing for such claims.

Accordingly, the key issue is consent. UnrollMe argues that its customers consented to UnrollMe's data mining, which negates all of Plaintiffs' claims.[1]

---

[1] Plaintiffs do not argue that consent is an affirmative defense inapplicable at the motion-to-dismiss stage. But even if consent is considered an affirmative defense instead of an element, a court may dismiss a claim based on an affirmative defense that appears on the face of the complaint. *See Pani v. Empire Blue Cross Blue Shield*, 152 F.3d 67, 74–75 (2d Cir. 1998); *see also Orton v. Pirro, Collier, Cohen, Crystal & Block*, No. 95 Civ. 3056, 1996 WL 18831, at *2 (S.D.N.Y. Jan. 18, 1996) (dismissing ECPA claim because consent was evident in the complaint). Since the Complaint includes the language purportedly giving consent, the Court will consider it at the motion-to-dismiss stage. *See In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 508 (S.D.N.Y. 2001).

UnrollMe's privacy policy states:

> We . . . collect non-personal information − data in a form that does not permit direct association with any specific individual. We may collect, use, transfer, sell, and disclose non-personal information for any purpose. . . . We collect such commercial transactional messages so that we can better understand the behavior of the senders of such messages, and better understand our customer behavior and improve our products, services, and advertising. We may disclose, distribute, transfer, and sell such messages and the data that we collect from or in connection with such messages; provided, however, if we do disclose such messages or data, all personal information contained in such messages will be removed prior to any such disclosure.
>
> We may collect and use your commercial transactional messages and associated data to build anonymous market research products and services with trusted business partners. If we combine non-personal information with personal information, the combined information will be treated as personal information for as long as it remains combined.

(Compl. ¶ 31.)

Plaintiffs concede that they agreed to UnrollMe's privacy policy (Compl. ¶ 22), but they argue that UnrollMe's alleged activity was not covered by the privacy policy.

First, Plaintiffs argue that that they allowed UnrollMe to access their emails only for the limited purpose of cleaning up their inboxes, and that they did not allow UnrollMe to sell their data for market research purposes. But while it is true that consent is not an all-or-nothing proposition, the fact remains that the privacy policy reserves the right to do exactly what UnrollMe did: "collect and use your commercial transactional messages and associated data to build anonymous market research products and services with trusted business partners." (Compl. ¶ 31.) Plaintiffs are probably right that most users thought UnrollMe would reduce the noise of internet marketing rather than increase it. But while UnrollMe's conduct may be unseemly, it still falls within the ambit of the privacy policy.

Second, Plaintiffs argue that the privacy policy is misleading because it says only that UnrollMe *may* sell consumer data, not that it *would* do so. But this distinction is without difference. If I ask you if I may enter your house, and you say yes, you have given me permission to enter your house.

Plaintiffs point to *In re Google Inc.*, No. 13-MD-02430, 2013 WL 5423918 (N.D. Cal. Sept. 26, 2013), to support the distinction between "may" and "will." *Id.* at *13. That case was about Google's terms of service, which said that "advertisements may be targeted" to Gmail users. *Id.* The court held this disclaimer insufficient to demonstrate consent because "it demonstrates only that Google has the *capacity* to intercept communications, not that it will." *Id.*

This Court respectfully disagrees with that conclusion for two reasons. First, there is no legal support for this distinction. And second, the word "may" can have different meanings in different contexts. There is a difference between "X may happen" and "we may do X." While the former might just denote a possibility, the latter certainly denotes permission.

Third, Plaintiffs argue that even if they consented, UnrollMe still violated the ECPA. The ECPA prohibits interception of electronic communications, even with consent, if the interception is "for the purpose of committing any criminal or tortious act." 18 U.S.C. § 2511(2)(d). Plaintiffs argue that UnrollMe accessed their emails for a tortious purpose: "the exploitation of Plaintiffs' private and personal information for Defendants' own unjust enrichment and in breach of duties owed by them to Plaintiffs." (Dkt. No. 61 at 16.) But this argument is circular. If there was consent, then there was no tort. *See In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 515 (S.D.N.Y. 2001) ("[T]he 'criminal' or 'tortious' purpose requirement is to be construed narrowly, covering only acts accompanied by a specific contemporary intention to commit a crime or tort.").

Fourth, Plaintiffs argue that the privacy policy is unconscionable. Under New York law,[2] a contract is unconscionable when it "is so grossly unreasonable or unconscionable in the light of the mores and business practices of the time and place as to be [unenforceable] according to its literal terms." *Gillman v. Chase Manhattan Bank, N.A.*, 73 N.Y.2d 1, 10 (1988) (quoting *Mandel v. Liebman*, 303 N.Y. 88, 94 (1951)). There must be a showing that the contract is both procedurally and substantially unconscionable. *See id.* "The procedural element of unconscionability concerns the contract formation process and the alleged lack of meaningful choice; the substantive element looks to the content of the contract . . . ." *State v. Wolowitz*, 468 N.Y.S.2d 131, 145 (App. Div. 2d Dep't 1983).

In arguing that the consent provision is unconscionable, Plaintiffs argue (1) that UnrollMe's advertising belied its true purpose, (2) that UnrollMe's users signed up because they wanted to *declutter* their digital lives, and (3) that the privacy policy is a contract of adhesion. But while UnrollMe's conduct may seem unconscionable in the colloquial sense, Plaintiffs have not shown that it is unconscionable in the legal sense. On the procedural front, the mere fact that the privacy policy is a dense take-it-or-leave-it contract does not render it procedurally unconscionable. *See, e.g.*, *G&R Moojestic Treats, Inc. v. Maggiemoo's Int'l, LLC*, No. 03 Civ. 10027, 2004 WL 1110423, at *4 (S.D.N.Y. May 19, 2004). Nor was there a lack of meaningful choice: one could simply close the browser window and not use UnrollMe. And on the substantive front, the cases cited by Plaintiffs deal with contracts that are far more lopsided than the privacy policy here. This is especially so given that UnrollMe is a free internet service for which Plaintiffs paid nothing. (Compl. ¶ 18.)

[2] Defendants contend that UnrollMe's terms of use provided that New York law would apply. (Dkt. No. 54 at 4.) Since Plaintiffs appear to concede this point, (*see, e.g.*, Dkt. No. 61 at 20), the Court applies New York law to Plaintiffs' common-law claims.

It is probably true that UnrollMe's unwitting consumers simply wanted to clean up their inboxes. But it is also true that those consumers agreed to the Faustian bargain that undergirds much of the internet: you give me a free service, and I suppress the knowledge that you are probably selling my data to digital touts. We may not like it, but it is not *per se* unlawful.

Finally, Plaintiffs argue that even if they did consent, UnrollMe exceeded this consent by insufficiently anonymizing the data. But, as discussed above, the allegations on this front are meager. The Complaint does not adequately allege that UnrollMe sold unredacted data or that the data it did sell could be easily deanonymized. In other words, the Complaint does not plausibly allege that UnrollMe exceeded the terms of the privacy policy. The sole plausible allegation in the Complaint is that UnrollMe sold *anonymized* consumer data, an activity which is covered by the privacy policy.

All of the Complaint's statutory claims depend on a lack of consent. *See* 18 U.S.C. § 2511(2)(d) (exempting from the ECPA communications for which "one of the parties to the communication has given prior consent to such interception"); 18 U.S.C. § 2702(b)(3) (allowing a provider to divulge information "with the lawful consent of the originator or an addressee or intended recipient of such communication"); Cal. Penal Code § 631(a) (prohibiting wiretaps "without the consent of all parties to the communication"); *see also In re DoubleClick*, 154 F. Supp. 2d at 526 (dismissing ECPA and Wiretap Act claims because of valid consent). Consent likewise negates Plaintiffs' unjust enrichment claim because it removes the necessary element that "the circumstances [of the enrichment] were such that equity and good conscience require defendants to make restitution." *Bancorp Servs., LLC v. Am. Gen. Life Ins. Co.*, No. 14 Civ. 9687, 2016 WL 4916969, at *8 (S.D.N.Y. Feb. 11, 2016) (quoting *Labajo v. Best Buy Stores*,

L.P., 478 F. Supp. 2d 523, 531 (S.D.N.Y. 2007)). And because Plaintiffs consented to UnrollMe's sale of anonymized data, they have failed to state a claim.[3]

IV. Conclusion

For the foregoing reasons, Defendants' motion to dismiss is GRANTED. The Clerk of Court is directed to close the motion at Docket Number 51 and to close this case.

SO ORDERED.

Dated: June 6, 2018
New York, New York

J. PAUL OETKEN
United States District Judge

[3] The Complaint asserts a common law claim for intrusion of privacy, but Plaintiffs' opposition brief disclaims that cause of action in favor of a newly asserted breach-of-fiduciary-duty claim. (See Dkt. No. 61 at 22.) The Court will not consider this cause of action raised for the first time in opposition to the motion to dismiss. Moreover, consent likely negates both the breach-of-privacy and breach-of-fiduciary-duty claims. In any event, without a valid federal claim, the Court declines to exercise supplemental jurisdiction over any remaining state law claims. *See* 28 U.S.C. § 1367(c)(3).