

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IN RE: ZETA GLOBAL DATA PRIVACY LITIGATION

25 Civ. 5780 (PAE)

OPINION & ORDER

PAUL A. ENGELMAYER, District Judge:

This case is brought on behalf of a putative class of consumers whose personally identifiable information (“PII”) was allegedly intercepted, collected, and monetized by defendants Zeta Global Corporation and Zeta Global Holdings Corporation (collectively, “Zeta”), and others, in violation of the Electronic Communications Privacy Act (“ECPA”), 18 U.S.C. § 2510, *et seq.*, and various state consumer protection laws.

Zeta and co-defendant DotDash Meredith, Inc., (“DotDash”) now each move to dismiss the First Amended Complaint (“FAC”). Under Federal Rule of Civil Procedure 12(b)(1), they argue that the FAC does not plead an injury in fact sufficient to support the named plaintiffs’ standing; under Rule 12(b)(6), they argue that the FAC fails to state a claim. For the reasons that follow, the Court grants defendants’ motions under Rule 12(b)(1).

I. Background

A. Factual Background

1. Parties

Zeta is a Delaware corporation that uses artificial intelligence to develop personalized marketing techniques aimed at helping brands acquire and retain customers. Dkt. 35 (“FAC”) ¶¶ 48–54. Zeta is headquartered, and has a principal place of business, in New York City, New York. *Id.* ¶¶ 48–49. DotDash, a client of Zeta’s, operates a portfolio of media and

print brands that publish articles on various websites. *Id.* ¶¶ 45–47. It is also a Delaware corporation headquartered in New York City, New York. *Id.* ¶ 45.

At all relevant times, plaintiff R.E.A. was a resident of Suffolk County, New York, *id.* ¶ 24; plaintiff K.G. was a resident of Los Angeles County, California, *id.* ¶¶ 31–32; and plaintiff Diane Ayerdi was a resident of San Francisco County, California, *id.* ¶¶ 38–39. Each plaintiff asserts that she visited storefronts used by Zeta’s clients; that Zeta’s technology as deployed by those clients tracked her across the Internet; and that Zeta, and its clients, profited from collecting her PII. *See id.* ¶¶ 24–44.

2. Zeta’s Business Model

Founded in 2007, Zeta is an “AI-powered omnichannel data-driven cloud platform that provides enterprises with consumer intelligence and marketing automation software.” *Id.* ¶ 60. Zeta’s clients—approximately 1,200 businesses, including some 40% of the Fortune 100—rely on Zeta for marketing services, including the Zeta Marketing Platform (“ZMP”). *Id.* ¶¶ 10, 62. The ZMP utilizes AI-techniques to “predict consumer intent, optimize messaging and drive personal messaging across all channels.” *Id.* ¶ 63.

a. Zeta’s Data Collection

To develop these insights, Zeta gathers data from third-party websites run by companies it has acquired, data aggregators, and publicly available information. *Id.* ¶¶ 63–67. A consumer who visits a third-party site is assigned a “Zeta ID,” or a “non-changeable identifier” that follows the user across other sites. *Id.* ¶¶ 77, 82–83. Zeta uses application programming interfaces (“APIs”) and pixel tracking to intercept consumer data from individual websites. *Id.* ¶ 64.

i. Zeta LiveIntent Pixel Technology

Through its subsidiary, LiveIntent, Zeta collects data using a “pixel” embedded in websites and email newsletters. *Id.* ¶¶ 101–02. When a consumer opens an email containing the embedded pixel, the pixel is activated. *Id.* ¶ 109. The pixel collects the email address, campaign identifiers, device and client information, and a unique impression ID. *Id.* It then transmits this consumer data to Zeta’s servers, while simultaneously sending the IP address and consumer data to LiveIntent’s servers. *Id.* The data collected by the pixel is used by both LiveIntent and the ZMP. *Id.* ¶¶ 109–11. Upon receipt of the information transmitted by the pixel, LiveIntent logs the occurrence as an “open event.” *Id.* ¶ 110. LiveIntent initiates real-time bid requests for the open event to its advertising partners, who can purchase this data to target consumers in subsequent marketing campaigns. *Id.* ¶¶ 110–11. Zeta states that the consumer data obtained through LiveIntent contributes the “largest share” of data in its ZMP platform. *Id.* ¶ 116.

DotDash uses Zeta’s “LiveIntent” pixel technology on its websites and in email correspondence with subscribers to them. *Id.* ¶ 101. As alleged, DotDash agreed with Zeta to deploy tracking technology on DotDash’s web properties and email communications, enabling Zeta to intercept in real-time plaintiffs’ data. *Id.* ¶¶ 46–47.

ii. Third-Party Websites

Zeta supplements this pixel-collected data with information it harvests from “deceptive websites” operated by companies it has acquired. *Id.* ¶ 65. In 2021 and 2022, for example, Zeta acquired Apptness Media Group, LLC and ArcaMax Publishing, Inc. *Id.* Both companies operate websites, promising a visitor exclusive offers, deals, and job opportunities in exchange for identifying information, such as their first and last name. *Id.* Despite promising a visitor these exclusive offers upon entry of the information, the sites do not contain “exclusive offers to

unlock,” but rather serve as “data aggregator[s].” *Id.* After a visitor enters identifying information, the sites continue to seek information from her. *Id.*

b. Zeta’s Data Set and AI Engine

Through APIs, pixel tracking, and data aggregators, Zeta has built a dataset of some 245 million individuals in the United States. *Id.* ¶¶ 66–67. It claims to generally possess, on average, 2,500 pieces of information per individual, including demographic, behavioral, psychographic, transactional, or other preference data. It uses these to build “audiences” for its clients. *Id.* ¶¶ 67, 86–87. Zeta clients can, for example, review:

- Consumers’ email addresses, postal addresses, IP addresses, and phone numbers. *Id.* ¶ 77.
- Consumers’ visitation data, capturing “real-world movement by tracking device locations through mobile application and GPS navigation systems.” *Id.* ¶ 87(b).
- Consumers’ transaction data, including whether the user has “completed a transaction within certain listed categories.” *Id.* ¶ 87(c).
- Consumers’ demographic data groups based on “age, gender, ethnicity, and income.” *Id.* ¶ 87(e).

This data also populates Zeta’s AI Engine—its “GenAI, machine learning, natural language processing, and predictive AI.” *Id.* ¶ 69. Zeta has stated that its AI Engine “collect[s] and ingest[s] structured and unstructured data into the ZMP,” clusters “related concepts and prioritize[s] actionable insights,” and “[e]nables ZMP users to create GenAI agents and workflows, which chain discrete tasks together for automations.” *Id.* ¶¶ 69(a), (d), (i). Zeta uses this AI Engine to generate “insights” which its clients can use to identify consumers who “can be targeted for specific lines of business.” *Id.* ¶ 90. Zeta has stated, for example, that it knows whether a potential consumer recently was promoted, or viewed cord-cutting guides, indicative of an intent to terminate a subscription early. *Id.* ¶ 92. Zeta also offers its clients tools, including:

- *Propensity scores*: These estimate a user’s propensity to purchase a product based on their discretionary spending, household income, net-worth, credit card usage, and education. *Id.* ¶ 90(a).
- *Multicultural audience filters*: These enable a Zeta client to “target users based on their race or origin.” *Id.* ¶ 90(b).
- *Advanced location targeting*: These enable a Zeta client to target potential customers based on “precise location information including city, state, zip code, and latitude/longitude.” *Id.* ¶ 90(c).

Zeta also advertises its “omnichannel engagement,” which enables clients to “improve how they identify and engage the modern consumer who is using multiple devices and platforms (e.g., mobile, website, applications, social media, CTV and email).” *Id.* ¶ 71. Zeta’s data sources “integrate” data in a manner that exchanges the Zeta ID assigned to a visitor with “other third parties.” *Id.* ¶ 72. Zeta claims that “this combination of identifiers enable[s] [it] to correctly identify ‘millions of events per day’” across a network of “2500+ publishers.” *Id.* ¶ 78.

c. The “Value” of Zeta’s Data

The FAC alleges that the data Zeta collects and the assumptions built into the Zeta AI Engine are “highly valuable,” as reflected in (i) the cost Zeta charges to access the ZMP and (ii) Zeta’s internal estimates as to the “average revenue per user” or ARPU. *Id.* ¶¶ 117, 120–21. A license to access the ZMP service generally costs between \$70,000 and \$100,000; additional data costs more. *Id.* ¶ 120. Zeta monitors customer-specific ARPU. *Id.* ¶ 121. Zeta’s 2023 annual report reported, for example:

During the year ended December 31, 2023, [Zeta] experienced an increase in our scaled customer [ARPU], which resulted in our revenues increasing for the year compared to the prior-year period. Our scaled customer ARPU growth resulted primarily from the initial effects of transitioning our sales team model to focus a dedicated team on new business development and a separate team on training and educating new and existing users on our platform capabilities. Our transition to this hunter/farmer sales model has included focusing more of our sales team on growth of existing scaled customers and aligning scaled customers with sellers that have specific industry expertise.

Id.

In investor reports, Zeta has stated that “the ARPU for its scaled customers reaching \$1,572,000 in 2023 per customer as compared to \$1,431,000 in 2022.” *Id.* ¶ 122.

II. Procedural History

On July 14, 2025, Ayerdi filed the complaint in *Ayerdi v. Zeta Global Holdings Corp.*, No. 25 Civ. 5780 (S.D.N.Y.). Dkt. 1. On October 14, 2025, the Court consolidated that case with related case *A.P. v. Zeta Global Corp.*, No. 25 Civ. 5823 (S.D.N.Y.). Dkt. 28.

On November 20, 2025, plaintiffs filed the FAC, the operative complaint here, seeking money damages and declaratory relief. Dkt. 35. On January 5, 2026, Zeta moved to dismiss the FAC, Dkt. 44 (“Zeta Mem.”), attaching a declaration and exhibits, Dkt. 45 (“Smith Decl.”), and DotDash also moved to dismiss (“DotDash Mem.”), Dkt. 49. On February 19, 2026, plaintiffs opposed Zeta’s motion, Dkt. 57 (“Zeta Opp’n”), attaching a request for judicial notice and exhibits, Dkt. 58, and DotDash’s motion, Dkt. 59, attaching a declaration, Dkt. 60 (“Fiorilla Decl.”). On March 20, 2026, Zeta replied, Dkt. 62 (“Zeta Reply”), attaching exhibits, Dkt. 63, as did DotDash, Dkt. 64 (“DotDash Reply”).

III. Discussion

Zeta and DotDash move to dismiss under Rule 12(b)(1) for lack of subject matter jurisdiction, arguing that plaintiffs lack Article III standing. Zeta Mem. at 7–12; DotDash Mem. at 6–11. For the reasons below, the Court grants this motion, finding that the FAC does not plausibly plead, as to any claim, that the named plaintiffs suffered a cognizable injury in fact. The Court accordingly does not reach defendants’ alternative grounds to dismiss, under Rule 12(b)(6), for failure to state a claim. *See Ross v. Bank of Am., N.A.*, 524 F.3d 217, 222 n.1 (2d Cir. 2008); *Brown v. Nat’l Football League, Inc.*, 825 F. Supp. 3d 265, 272 (S.D.N.Y. 2026) (Engelmayer, J.).

A. Applicable Legal Standards

1. Rule 12(b)(1)

A court must dismiss a claim for lack of subject matter jurisdiction under Rule 12(b)(1) when it “lacks the statutory or constitutional power to adjudicate it, such as when . . . the plaintiff lacks constitutional standing to bring the action.” *Cortlandt St. Recovery Corp. v. Hellas Telecomms., S.a.r.l.*, 790 F.3d 411, 416–17 (2d Cir. 2015) (citation omitted). “A plaintiff asserting subject matter jurisdiction has the burden of proving by a preponderance of the evidence that [jurisdiction] exists.” *Makarova v. United States*, 201 F.3d 110, 113 (2d Cir. 2000). In resolving a motion to dismiss for lack of subject matter jurisdiction, “the court must take all facts alleged in the complaint as true,” *Nat. Res. Def. Council v. Johnson*, 461 F.3d 164, 171 (2d Cir. 2006) (citation omitted), but “jurisdiction must be shown affirmatively, and that showing is not made by drawing from the pleadings inferences favorable to the party asserting it,” *Shipping Fin. Servs. Corp. v. Drakos*, 140 F.3d 129, 131 (2d Cir. 1998); *see also Amidax Trading Grp v. S.W.I.F.T. SCRL*, 671 F.3d 140, 145 (2d Cir. 2011) (per curiam); *APWU v. Potter*, 343 F.3d 619, 623 (2d Cir. 2003). On such a motion, a court may consider evidence outside the pleadings, such as affidavits and exhibits. *See Makarova*, 201 F.3d at 113.

2. Article III Standing

Article III of the Constitution limits the federal judicial power to the resolution of “cases” and “controversies.” U.S. Const. art. III., § 2. An “essential and unchanging part” of this limitation is that a plaintiff have standing to sue. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992). A plaintiff must “demonstrate standing for each claim and form of relief sought.” *Cacchillo v. Insméd, Inc.*, 638 F.3d 401, 404 (2d Cir. 2011) (quoting *Baur v. Veneman*, 352 F.3d 625, 642 n.15 (2d Cir. 2003)).

The “irreducible constitutional minimum” of standing is that a plaintiff “(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision.” *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016) (quoting *Lujan*, 504 U.S. at 560–61). That requires that a plaintiff’s injury be “concrete”—*i.e.*, “real, and not abstract.” *Id.* at 340 (cleaned up). The injury-in-fact requirement—which figures substantially in this case—is meant to “ensure that the plaintiff has a personal stake in the outcome of the controversy.” *Susan B. Anthony List v. Driehaus*, 573 U.S. 149 (2014) (citation omitted). This requirement “ensures that federal courts decide only ‘the rights of individuals’ . . . [and] exercise ‘their proper function in a limited and separated government.’” *TransUnion LLC v. Ramirez*, 594 U.S. 413, 423 (2021) (quoting *Marbury v. Madison*, 1 Cranch 137, 170 (1803), and John G. Roberts, Jr., *Article III Limits on Statutory Standing*, 42 DUKE L.J. 1219, 1224 (1993)).

Certain harms “readily qualify as concrete.” *Id.* at 425. “The most obvious” of these “are traditional tangible harms, such as physical harms and monetary harms.” *Id.* at 425. Financial loss is a “classic pocketbook injury sufficient to give [plaintiff] standing.” *Tyler v. Hennepin Cnty., Minnesota*, 598 U.S. 631, 636 (2023) (citing *TransUnion*, 594 U.S. at 425); *see also* *Moreira v. Société Générale, S.A.*, 125 F.4th 371, 385 (2d Cir. 2025) (same). As to intangible harms, the Constitution identifies the contours of such injuries, which bear a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts, that are “concrete.” *See, e.g., TransUnion*, 594 U.S. at 425. Concrete intangible harms also include those such as reputational harm, disclosure of private information, and intrusion upon seclusion. *Id.*

B. Application

In moving to dismiss, defendants contend that the FAC, which alleges that Zeta (assisted by DotDash) obtained and monetized personal information relating to plaintiffs, does not plead a cognizable injury in fact. Zeta Mem. at 7–9; DotDash Mem. at 6–9. Plaintiffs counter principally that the FAC pleads two privacy-related harms traditionally recognized as adequate to confer standing: invasion of their privacy, referred to at common law as public disclosure of “private facts,” and “intrusion upon seclusion.” See Zeta Opp’n at 3; DotDash Opp’n at 4–5. They also rely upon the FAC’s allegations that defendants profited economically from monetizing their PII, harmed plaintiffs’ electronic device “resources,” and caused a loss of control of their data. Zeta Opp’n at 4–9; DotDash Opp’n 4–10. The Court takes up each theory of harm in turn.

1. Plaintiffs’ Privacy-Related Injuries

Plaintiffs’ principal asserted injury—underpinning their federal and state claims—is that defendants’ interception, collection, and monetization of their PII violated their “privacy” rights. Zeta Mem. at 3–4; DotDash Mem. at 4–5. The FAC’s allegations along these lines, however, do not make out a cognizable injury in fact.

At the threshold, the decisive issue concerns the standing of the three named plaintiffs. In a putative class action, the named plaintiffs “must allege and show that they personally have been injured, not that the injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent.” *Lewis v. Casey*, 518 U.S. 343, 357 (1996) (citation omitted). Thus, for every named defendant, there must be a named plaintiff who can assert a “assert a claim directly against [that] defendant” that she was injured in a “personal and individual” way. *NECA–IBEW Health & Welfare Fund v. Goldman Sachs & Co.*, 693 F.3d 145, 159 (2d Cir. 2012) (citation omitted); *Ross v. AXA Equitable Life Ins. Co.*, 115 F. Supp. 3d

424, 432 (S.D.N.Y. 2015) (same), *aff'd*, 680 F. App'x 41 (2d Cir. 2017) (summary order). It does not suffice to allege that an absent member of the putative class experienced a cognizable injury. *Menking ex rel. Menking v. Daines*, 287 F.R.D. 174, 178–79 (S.D.N.Y. 2012).

That is consequential here, because the facts alleged as to the personal information obtained from the three named plaintiffs are sparse. As to R.E.A., the FAC alleges that she provided her email address and other information to create an account with Horoscope.com, a Zeta client. FAC ¶¶ 24–26. It alleges that, through pixels hosted on Horoscope.com and other sites, Zeta intercepted R.E.A.'s "PII" and interacted with the "content of R.E.A.'s searches," but it does not specify what information of hers Zeta collected (or disclosed). *Id.* ¶¶ 26–27. As to K.G., the FAC states that she visited the websites of Zeta clients Horoscope.com, All Recipes, Food & Wine, MyRecipes, Southern Living, and U.S. Weekly, supplying her "email address and other information," to create an account with one such site, and that Zeta intercepted her "PII." *Id.* ¶¶ 32–33. But it does not specify the "other information" K.G. supplied these clients, what this "PII" consisted of, or what information Zeta collected (or disclosed). As to Ayerdi, the FAC states that she provided her email address and other information to create an account with People.com, which is affiliated with Zeta and DotDash. *Id.* ¶¶ 39–40. It alleges that the information about Ayerdi transmitted to Zeta's subsidiary included her "email address, campaign identifiers, device and client information, [] unique impression IDs," "browser . . . information," and "campaign context," as well as "PII from online services she used." *Id.* ¶¶ 40, 103–04, 109–11. It does not elaborate on these terms, including "unique impression ID" or "PII."

a. Disclosure of Private Information

A plaintiff claiming injury from the disclosure of her personal information must either demonstrate "actual injuries" resulting from the disclosure or "a substantial risk of harm." *See FritzCo LLC v. Verizon Commc'ns Inc.*, No. 21 Civ. 10432, 2026 WL 734776, at *4 (S.D.N.Y.

Mar. 16, 2026) (cleaned up). As to the latter, the critical inquiry is “whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud.” *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 303 (2d Cir. 2021)

Under the case law, whether the information of the named plaintiffs shared with Zeta’s clients was the type of “private information” that can support a cognizable claim of injury, *TransUnion*, 594 U.S. at 425, turns on whether it constituted sensitive information. In *Cooper v. Bonobos, Inc.*, No. 21 Civ. 854, 2022 WL 170622, at *6 (S.D.N.Y. 2022) (“*Cooper*”), Judge Furman applied this line of case law to a plaintiff who claimed his data had been intercepted by Bonobos, a chain of men’s clothing stores, and disclosed following a data breach. The data disclosed included the plaintiff’s addresses, telephone numbers, email addresses, order history, Internet Protocol (“IP”) addresses, encrypted passwords, and partial credit card numbers. *Id.* at *1–2. Judge Furman held that the plaintiff had not pled an injury in fact supporting his state statutory or common law claims, given the nature of this data and its age. *Id.* at *1, 4. He distinguished between the disclosure of plaintiff’s “less sensitive data” (addresses, phone numbers, email addresses, and IP addresses) and his “partial credit card numbers” and “password histories.” *Id.* at *3–4. As to the former, he found the risk of harm “entirely speculative, if not fanciful, and thus insufficient to support standing.” *Id.* at *4. And as to the latter, he found the disclosure unlikely to cause an injury that was “certainly impending” or suggesting a “substantial risk the harm will occur” in light of the fragmented nature of the data and the age of the information (e.g. old passwords—that were captured. *Id.* at *6. This Court held similarly in *Liau v. Weee! Inc.*, No. 23 Civ. 1177, 2024 WL 729259 (PAE), at *5 (S.D.N.Y. Feb. 22, 2024), finding customers’ names, email addresses, and phone numbers not to constitute sensitive information to support standing. *See also McMorris*, 995 F.3d at 298–301 (finding disclosure of

home addresses, dates of birth, telephone numbers, educational degrees, and dates of hire did not support finding injury in fact); *Yankovich v. Applus Techs., Inc.*, 621 F. Supp. 3d 269, 272–74 (D. Conn. 2022) (declining to find standing where plaintiffs alleged dates of births, addresses, and Social Security numbers could have been exposed but did not plead with particularity the “extent to which” it actually had been); *United States v. Morel*, 922 F.3d 1, 8–9 (1st Cir. 2019) (same as to IP address information).

In contrast, in *FritzCo LLC v. Verizon Commc'ns Inc.*, Judge Oetken found that the disclosure of plaintiff's credit card information—which, along with other purloined personal information, enabled third parties to complete unauthorized transactions—to support standing in a case involving state-law claims arising from a widespread data breach. 2026 WL 734776, at *4. And in *Cooper v. Slice Techs., Inc.*, No. 17 Civ. 7102, 2018 WL 2727888, at *2–3 (S.D.N.Y. June 6, 2018), Judge Oetken likewise held that, where the defendant sold the content of plaintiffs' emails, the information disclosed was sufficiently sensitive to support standing on the federal and state common law claim. *See also Bohnak v. Marsh & McLennan Co., Inc.*, 79 F.4th 276, 281, 283–88 (2d Cir. 2023) (finding disclosure of plaintiff's “Social Security or other federal tax identification number[s] driver's license or other government issued identification, and passport information” was sufficiently sensitive so as to support standing); *In re Christie's Data Breach Litig.*, 767 F. Supp. 3d 12, 16–18 (S.D.N.Y. 2025) (finding disclosure of plaintiffs' full names, passport numbers, and driver's license numbers sensitive); *In re USAA Data Sec. Litig.*, 621 F. Supp. 3d 454, 465–66 (S.D.N.Y. 2022) (same as to history of military service and driver's license numbers).

Measured against these standards, the allegations in the FAC relating to the three named plaintiffs do not come close to pleading the disclosure of sensitive information. Although using

the term “PII” for all three plaintiffs, it does not specify concretely what this information was. As to all three plaintiffs, it does not allege any PII that was disclosed. It alleges the disclosure of their email addresses, but nothing more save the generic term “other information.” It does not allege that credit card information, medical information, Social Security numbers, or any other data otherwise recognized by courts as sensitive—was disclosed. It hypothesizes that Zeta might possess “2,500” pieces of information about these plaintiffs, and that “Zeta has likely stored more information than what is publicly known.” FAC ¶¶ 67, 85. But such conjecture cannot support standing. *See Hernandez v. Hernandez*, No. 24 Civ. 8614, 2026 WL 318291, at *6 (E.D.N.Y. Feb. 5, 2026) (citing *Lujan*, 504 U.S. at 560). As to Ayerdi, the FAC generically alleges the disclosure of her “email address,” “campaign identifiers,” “campaign context,” “device and client information,” and “browser . . . information,” FAC ¶¶ 40, 103–04, 109–11, but such is the “less sensitive data” that *Cooper*, synthesizing the case law, held insufficient to support standing, 2022 WL 170622, at *3, and that *Liau* found unlikely to be “susceptible to misuse,” *Liau*, 2024 WL 729259, at *4–5. And the FAC’s allegation that “unique impression IDs” were disclosed, without amplification as to concretely to what this expression refers, does not enable a court to find the disclosure of sensitive information either. FAC ¶ 109.

The FAC thus does not plead injury in fact from the alleged disclosure of plaintiffs’ data. And federal courts have widely rejected claims that, without more, the disclosure of email addresses or IP addresses presents a cognizable injury. *See, e.g., United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (“Internet users have no expectation of privacy in . . . the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.”); *Bradshaw v. Lowe’s Cos.*, No. 25 Civ. 742, 2025 WL 3171740, at *5 (S.D. Cal.

Nov. 12, 2025) (collecting cases and observing combination of browser information with other information captured by tracking pixels did not demonstrate a concrete injury to show Article III standing); *Morel*, 922 F.3d at 9 (party has no “reasonable expectation of privacy” in IP address information); *Smidga v. Spirit Airlines, Inc.*, No. 22 Civ. 1578, 2024 WL 1485853, at *4 (W.D. Pa. Apr. 5, 2024) (“[C]ourts have held that even the collection of basic contact information by [] software or where the plaintiffs merely visited the website are not [] concrete harms.”). Such holdings have come in cases, like this, bringing claims under the ECPA. *See, e.g., Magliocca v. United Healthcare Servs.*, No. 25 Civ. 3388, 2026 WL 878694, at *4 (E.D. Cal. Mar. 31, 2026) (“button clicks, page visits, session lengths, URLs, and IP addresses” were the kind of “non-sensitive browsing activity on a single website” that courts have repeatedly found insufficient to establish a concrete injury under the ECPA and state law); *Anghel v. Publishers Clearing House*, No. 22 Civ. 452, 2022 WL 11725995, at *3 (D. Conn. Oct. 20, 2022) (“The ECPA does not protect disclosure of an e-mail address.”).

Nor does the FAC viably plead that the named plaintiffs were exposed to a substantial risk of harm from the disclosure of this information. To the extent it elaborates, the FAC alleges, as to each named plaintiff, that “Zeta processed and stored [her] data to target Plaintiff [] with its business clients’ ads.” FAC ¶¶ 27 (R.E.A.), 34 (K.G.), 41 (Ayerdi). But this broad declaration that the information Zeta collected *could* have exposed plaintiffs to “targeted advertising” is not accompanied by any pleading of such occurrence. *See id.* ¶¶ 6, 8, 29, 36, 43. And its broad claim that “Zeta and its business clients profited from this data collection apparatus” and were positioned to “serve targeted ads” to the named plaintiffs, *id.* ¶¶ 29 (R.E.A.), 36 (K.G.), 43 (Ayerdi), is generic and does not plead any injury either. *See FritzCo*, 2026 WL 734776, at *4. It does not allege that any named plaintiff received any targeted advertising or were otherwise

affected, let alone harmed, by it. *See Xu v. Reuters News & Media Inc.*, 2025 WL 488501, at *3–4.

The Court accordingly rejects plaintiffs’ theory of an injury in fact based on the disclosure of their data to Zeta’s clients.

b. Intrusion Upon Seclusion

The Supreme Court has recognized a distinct but closely related harm to the disclosure of private facts which can support Article III standing: “intrusion upon seclusion.” *TransUnion LLC*, 594 U.S. at 425; *Packer on behalf of 1-800-Flowers.Com, Inc. v. Raging Cap. Mgmt., LLC*, 105 F.4th 46, 51 (2d Cir. 2024). The Court and the Second Circuit have not yet defined the showing necessary to plead such an injury. *See, e.g. Bohnak*, 79 F.4th at 284–86 (recognizing “intrusion upon seclusion” and “disclosure of private information” as independent bases for standing in case challenging improper disclosure of PII, but, because former was well pled, not reaching latter); *Salazar v. Nat’l Basketball Ass’n*, 118 F.4th 533, 541 n.5 (2d Cir. 2024) (not reaching issue), *cert. denied*, 146 S. Ct. 880 (2025). In a summary order, the Circuit has recognized that the unauthorized “accessing and monitoring of plaintiffs’ web-browsing activity implicates harms similar to those associated with the common law tort of intrusion upon seclusion.” *Mount v. PulsePoint, Inc.*, 684 F. App’x 32, 34–35 (2d Cir. 2017) (summary order).

Here, however, even liberally imagining the contours of such a viable injury, the named plaintiffs’ sparsely-pled injuries of this nature fall well short of cognizable. The FAC does not contain specific allegations as to any of the three. As to each, it instead makes the general claim that each named plaintiff’s subscription to a Zeta-affiliated newsletter enabled Zeta’s pixel tracking to “track and profile” her. FAC ¶¶ 26–28 (R.E.A.), 33–35 (K.G.), 40–42 (Ayerdi). It is devoid of specifics, either as to the maleficent mechanism by which such tracking was enabled or the data thereby obtained. That pleading falls far short of the intrusion pled in *Mount*, where

the defendant “deployed code in ads that caused [plaintiff’s] Safari browsers to ‘drop the default protection and accept tracking cookies.’” *Mount v. PulsePoint, Inc.*, No. 13 Civ. 6592, 2016 WL 5080131, at *4 (S.D.N.Y. Aug. 17, 2016); *accord In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 134 (3d Cir. 2015) (injury in fact pled based on “highly specific allegations” that defendants took covert actions to circumvent privacy settings on Safari and other browsers in order to deposit third-party cookies). The FAC states generally that Zeta was aware of “new tools used by consumers to limit data collection,” but it does not specify these or how, if at all, they were circumvented. FAC ¶ 16. And although it alleges that “88% of Apple devices” employ a “Do Not Track” feature limiting data collection, it does not plead Zeta circumvented this feature either, in a manner that might approximate intrusion. *Id.* ¶ 125. The FAC therefore does not plead a cognizable intrusion upon seclusion.

c. Traceability

Even if the FAC had pled a cognizable injury from the disclosure of the named plaintiffs’ information, they would still need to plead that such was traceable to defendants. *California v. Texas*, 593 U.S. 659, 668–69 (2021). The FAC does not clear that hurdle either. It acknowledges that plaintiffs voluntarily disclosed data (email addresses and “other information”) in exchange for services offered by defendants, such as access to sites and newsletters. FAC ¶¶ 26 (R.E.A., as to Horoscope.com), 32 (K.G., as to All Recipes), 40 (Ayerdi, as to People.com). But a person does not have a legitimate expectation of privacy in material it “voluntarily turned over to a third party in order to access its website.” *Xu*, 2025 WL 488501, at *5. And the FAC pleads ignorance about how the named plaintiffs’ data traveled to Zeta, observing that plaintiffs:

still are not publicly aware of *how* and *where* Zeta collects data. This is because Zeta’s technology is designed to function secretly in a manner consumers cannot detect, such that they have no reason to suspect Zeta’s technology is lurking in the

background of websites they visit or email correspondence that they open or to review Zeta’s policies.

FAC ¶ 100 (emphasis added). Without a concrete pleading to the effect that private data that plaintiffs had not willingly relinquished was transferred from partner websites to Zeta, the FAC cannot be said to have concretely pled an injury traceable to unlawful conduct.

Moreover, the FAC raises the confounding possibility that plaintiffs’ data came to Zeta not by the legal wrongs alleged, but via “other data aggregators who also traffic in this type of sensitive information.” *Id.* ¶¶ 11, 59. These pleadings make plaintiffs’ claims of an injury traceable to the wrongs alleged too speculative to stand. *See, e.g., Food & Drug Admin. v. All. for Hippocratic Med.*, 602 U.S. 367, 390 (2024) (finding standing allegations suffered from a lack of causation where plaintiff’s alleged injuries were “too speculative” to support standing); *Ateres Bais Yaakov Acad. of Rockland v. Town of Clarkstown*, 88 F.4th 344, 352–53 (2d Cir. 2023) (same); *Informed Consent Action Network v. Becerra*, 595 F. Supp. 3d 70, 81 (S.D.N.Y. 2022) (citing *Garellick v. Sullivan*, 987 F.2d 913, 919 (2d Cir. 1993)).

2. Plaintiffs’ Economic Harm

Plaintiffs’ claim they suffered two economic harms—from the “diminished value” of their data and defendants’ economic profits—that support a cognizable injury in fact. Zeta Opp’n at 7; DotDash Opp’n. at 11. As to each, however, the FAC’s allegations fall short.

As to diminution in value, a plaintiff pleads a “cognizable economic injury” where the disclosure of her private information causes such information to lose value. *De Medicis v. Ally Bank*, No. 21 Civ. 6799, 2022 WL 3043669, at *4–6 (S.D.N.Y. Aug. 2, 2022). To do so, the plaintiff must also allege “the existence of a market for that information and how the value of such information could have decreased due to its disclosure.” *Id.* at *5. Where, however, a plaintiff conclusorily or speculatively claims a diminution in value from disclosure of her private

information, or does not plead an intent to ever monetize that information, courts have declined to find a cognizable injury. *See, e.g., Wallace v. Health Quest Sys., Inc.*, 20 Civ. 545, 2021 WL 1109727, at *2, 8 (S.D.N.Y. Mar. 23, 2021) (no cognizable injury where plaintiffs pled only “speculative allegations” regarding diminution in value from disclosure of their names, financial account information, dates of medical treatments, and Social Security numbers); *Rudolph v. Hudson’s Bay Co.*, No. 18 Civ. 8472, 2019 WL 2023713, at *7–8 (S.D.N.Y. May 7, 2019) (declining to find cognizable injury where plaintiff did not allege “how the value of such data could have decreased” from disclosure); *Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d 735, 748 (W.D.N.Y. 2017) (finding no standing on diminished value theory where plaintiffs did not allege “any” facts as to how the disclosure of their private information decreased its value).

At the threshold matter, this theory is problematic because—as with plaintiffs’ claim of the disclosure of sensitive personal information—the FAC does not specify any particular private information that was disclosed as to the named plaintiffs. But even assuming that email addresses, the one species of information whose disclosure the FAC pleads, so qualified, the FAC does not marshal any facts supporting that it (or even the “other information” that the FAC generally pleads was disclosed) diminished in value. The FAC repeatedly pleads that the information collected by Zeta had great, and seemingly increasing, value to its clients. *See, e.g.*, FAC ¶¶ 118, 120–23 (describing Zeta’s “multibillion-dollar business,” investor reports and prices of datasets sold by non-Zeta entities). It does not allege that the value—in plaintiffs’ hands or Zeta’s—has diminished in value following Zeta’s alleged acquisition and use of it. It does not, for example, allege that, in some market in which plaintiffs’ data might be salable, Zeta’s actions have saturated the market with this data that it might have lost value or that the market value of this data has dropped. Nor does the FAC claim that plaintiffs ever intended to

“sell their personal information for value.” *Rudolph*, 2019 WL 2023713, at *7 (citation omitted). Absent a well-pled such intention, courts have declined to find standing on a diminution in value theory. *See id.* at *7–8 (declining to find standing on this theory based on disclosure of plaintiff’s credit card information where plaintiff did not plead an intent to sell this information); *Khan v. Children’s Nat’l Health Sys.*, 188 F. Supp. 3d 524, 533–34 (D. Md. 2016) (same where plaintiff did not assert that she sought to monetize her PII); *Mount*, 684 F. App’x at 35–36 (same as to browsing information). “[W]ithout allegations about how her [personal] information lost value, [plaintiffs] do[] not have standing on this ground.” *Whalen v. Michael Stores Inc.*, 153 F. Supp. 3d 577, 582 (E.D.N.Y. 2015), *aff’d sub nom. Whalen v. Michaels Stores, Inc.*, 689 F. App’x 89 (2d Cir. 2017) (summary order).

As to an economic injury to plaintiffs arising from defendants’ increased profits, the FAC does not more than broadly claim increased earnings for defendants. FAC ¶¶ 117–24; *See, e.g., id.* ¶ 124 (“Zeta makes a substantial amount of quantifiable revenue based on the data it collects”). That does not plead a cognizable injury to plaintiffs. *See, e.g., Xu*, 2025 WL 488501, at *3–4 (plaintiff did not plead injury by alleging that defendant who unlawfully collected and disclosed his data “increas[ed] its revenue”); *In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 804 (N.D. Cal. 2019) (plaintiffs did not plead cognizable lost-profits injury by alleging that Facebook’s gained money as a result of use of their data); *Hazel v. Prudential Fin., Inc.*, 2023 WL 3933073, at *6 (N.D. Cal. June 9, 2023) (same). This theory of injury thus also fails.

3. Defendants’ Impact on Plaintiffs’ Devices and Systems

The FAC next claims injury from the impact Zeta’s actions allegedly had on their electronic devices and computer systems. *See* FAC ¶ 234; Zeta Opp’n at 7–8.

This injury claim is also impermissibly speculative. The FAC alleges no more than that defendants’ practices could “impact[] CPU load time, and take[] up bandwidth.” FAC ¶ 234. It bases this claim on generalizations about electronic devices and network systems. *See id.* (noting certain “device batteries have only a finite number of charges before they need to be replaced” and “most data plans have bandwidth caps”). The FAC lacks, however, any allegations particular to the named plaintiffs. It does not allege that they experienced any issues arising from bandwidth capacity, that their devices exceeded any capacity limit, or that their batteries’ health was harmed. Standing cannot be sustained based on such speculative contentions about the impact on devices and networks. *See, e.g., Rudolph*, 2019 WL 2023713, at *5 (“mere possibility” of future injury or damage “not enough” to support injury in fact); *Mount*, 2016 WL 5080131 at *9–10 (speculative or *de minimis* marginal effect on electronic device operation does not support finding harm); *In re USAA Data Sec. Litig.*, 621 F. Supp. 3d at 466 (same). The Court accordingly rejects this theory of injury.

4. Plaintiffs’ Loss of Control of Data

The FAC next claims injury because Zeta’s actions caused them to lose “control” over their “valuable” data. FAC ¶¶ 184, 233, 251.

This injury, too, is inadequately pled. The FAC does not plead that the information collected from the named plaintiffs was “valuable” information in which a consumer possesses a right of “control.” *Compare Xu*, 2025 WL 488501, at *5 (rejecting injury-in-fact claim where plaintiff claimed deprivation of the “right to control his personal information” where defendant collected his IP address), *with Pena v. British Airways, PLC (UK)*, 18 Civ. 6278, 2020 WL 3989055, at *2 (E.D.N.Y. 2020) (recognizing cognizable interest in controlling dissemination of Social Security Number), *aff’d*, 849 F. App’x 13 (2d Cir. 2021) (summary order). As noted, the information the FAC alleges was obtained from the named plaintiffs consisted of “email

address,” “campaign identifiers,” “campaign context,” “device and client information,” and browser information. *See, e.g.*, FAC ¶¶ 24–26, 32–33, 40, 103–04, 109–11. But this “less sensitive data” has not been held an adequate basis, without more, to support an injury claim based on loss of control from dissemination. *See, e.g., De Medicis*, 2022 WL 3043669, at *5 (no injury in fact where plaintiff alleged unauthorized access or loss of control over username and password of his account with defendants); *United States v. Kidd*, 394 F. Supp. 3d 357, 362–68 (S.D.N.Y. 2019) (consumer had no reasonable expectation of control over IP address); *Morel*, 922 F.3d at 9 (same); *Liau*, 2024 WL 729259, at *5 (same as to customers’ names, email addresses, and phone numbers).

Even where a defendant has alleged breach of an obligation to reasonably safeguard a plaintiff’s valuable information, courts have required plaintiffs to plead an injury flowing from the loss of such control, such as paying a premium for data security protection or being exposed to added risk. *Cf. In re LinkedIn User Privacy Litig.*, No. 12 Civ. 3088, 2014 WL 1323713, at *6–7 (N.D. Cal. Mar. 28, 2014) (sustaining standing claim where plaintiff alleged he had purchased a premium subscription based on the company’s representation that this would secure his data consistent “with industry standards and technology”); *see, e.g., Whalen*, 153 F. Supp. 3d at 581 (no injury where loss of control of plaintiff’s financial data was not pled to have exposed her to risk from unauthorized charges or blocked bank access). The FAC never alleges that Zeta or any other defendant made representations to the named plaintiffs as to the security of the data they submitted in signing up for their respective newsletters or that the named plaintiffs paid a premium to do so. The Court accordingly rejects plaintiffs’ injury theory based on an asserted loss of control of “valuable” data.

5. Defendants' Statutory Violations

Plaintiffs next point to the FAC's allegations of violations of the federal and state statutes. *See, e.g.*, FAC ¶¶ 154, 197. But it is black letter law that pleading a statutory violation is not tantamount to pleading an injury in fact. *TransUnion*, 594 U.S. at 425–26. As the Supreme Court has emphasized in recent decisions involving alleged violations of consumer privacy statutes, Article III standing “requires a concrete injury even in the context of a statutory violation.” *Spokeo*, 578 U.S. at 341. A complaint does not “automatically” satisfy the injury-in-fact requirement whenever “a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right.” *Id.*; *see also Hacopian v. BlackRock, Inc.*, 788 F. Supp. 3d 552, 557 (S.D.N.Y. 2025) (“A plaintiff cannot ‘allege a bare [statutory] procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III’” (citation omitted)); *Maddox v. Bank of New York Mellon Tr. Co.*, 19 F.4th 58, 64 (2d Cir. 2021) (same).

Here, as noted, plaintiff assert violations of their statutory rights under the ECPA and New York and California statutes. *See, e.g.*, FAC ¶¶ 160, 165, 224, 241. But, for the reasons above, the FAC does not plead cognizable injuries in connection with these violations. As courts considering allegations of the same statutory violations have held, the bare fact of statutory violations, even assuming these to have been well-pled, does not satisfy Article III. *See, e.g., Whalen*, 153 F. Supp. 3d at 582 (plaintiff did not have standing where she “merely asserted” violation of N.Y. G.B.L. § 349 without elaboration); *Lightoller v. Jetblue Airways Corp.*, 2023 WL 3963823, at *3–4 (S.D. Cal. June 12, 2023) (dismissing claims under CIPA for lack of standing where plaintiff did not allege an injury separate from a statutory violation); *Byars v. Sterling Jewelers, Inc.*, No. 22 Civ. 1456, 2023 WL 2996686, at *3 (C.D. Cal. Apr. 5, 2023) (same); *Howard v. Octagon, Inc.*, 2013 WL 5122191, at *7 (N.D. Cal. Sept. 13, 2013) (same as

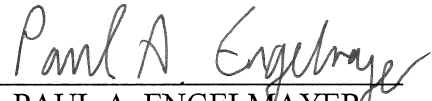
to Cal. Bus. & Prof. Code § 17200 claim); *Shah v. Cap. One Fin. Corp.*, 768 F. Supp. 3d 1033, 1048 (N.D. Cal. 2025) (same as to CDAFA claim).

CONCLUSION

For the above reasons, the Court grants in full the defendants' motions to dismiss under Rule 12(b)(1). Because this dismissal is for lack of subject matter jurisdiction, it is without prejudice to plaintiffs' ability to file a new action with a proper jurisdictional basis. *See Carter v. HealthPort Techs., LLC*, 822 F.3d 47, 54–55 (2d Cir. 2016) (“where a complaint is dismissed for lack of Article III standing, the dismissal must be without prejudice, rather than with prejudice”).

The Clerk of Court is respectfully directed to terminate the motions pending at dockets 43 and 48 and to close this case.

SO ORDERED.



PAUL A. ENGELMAYER
United States District Judge

Dated: August 5, 2026
New York, New York