UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

RONDA COOPER, CORAL FRASER, DAVID GITLIN and GILBERT MANDA, *on behalf of themselves and all others similarly situated,* Plaintiffs, -v- MOUNT SINAI HEALTH SYSTEMS, INC., Defendants.	23 Civ. 9485 (PAE) OPINION & ORDER

PAUL A. ENGELMAYER, District Judge:

Plaintiffs Ronda Cooper, Coral Fraser, David Gitlin, and Gilbert Manda ("Plaintiffs") bring this putative class action against defendant Mount Sinai Health Systems, Inc. ("Mount Sinai"). They allege that Mount Sinai, through internet tracking technologies, improperly disclosed their private health-related information to Meta Platforms, Inc., d/b/a Meta ("Facebook") for monetary gain.

Pending now is Mount Sinai's motion to dismiss under Federal Rule of Civil Procedure 12(b)(6). For the reasons that follow, the Court denies the motion in substantial part, granting it only as to Plaintiffs' claims for unjust enrichment and invasion of privacy.

I. Background

A. Factual Background[1]

Mount Sinai owns and operates eight hospitals and over a dozen medical centers in the New York City area, and employs more than 43,000 staff members, including 7,400 primary and

[1] The underlying facts which form the basis of this decision are drawn from the FAC. Dkt. 16. *See DiFolco v. MSNBC Cable LLC*, 622 F.3d 104, 111 (2d Cir. 2010) ("In considering a motion to dismiss for failure to state a claim pursuant to Rule 12(b)(6), a district court may consider the

specialty care physicians. Dkt. 16 ("FAC") ¶ 1. As part of the medical services it provides, Mount Sinai controls and maintains a website, https://mountsinai.org/, and a web-based MyChart patient portal (together, the "Web Properties"). *Id.* ¶ 3.[2] Mount Sinai encourages its patients to use its Web Properties to "communicate with their healthcare providers, access lab and test results, manage prescriptions and request refills, manage medical appointments, search medical conditions and treatment options, sign up for events and classes," and so forth. *Id.* ¶ 4. Mount Sinai also invites patients to "share and search for personal medical information about their own physical and mental health" using the Web Properties. *Id.*

Plaintiffs, all residents of New York, accessed Mount Sinai's Web Properties on their computers and mobile devices to look for providers, review conditions and treatment options, make appointments, and communicate with their healthcare providers. *Id.* ¶¶ 31–35. They allege that, using two tracking technologies, the Facebook Tracking Pixel (the "Pixel") and Facebook's Conversions Application Programming Interface ("CAPI"), Mount Sinai transmitted their personally identifiable information ("PII") and protected health information ("PHI") (together, "Private Information") to Facebook without their knowledge, consent, or express written authorization. *Id.* ¶¶ 6–11, 19.

---

facts alleged in the complaint, documents attached to the complaint as exhibits, and documents incorporated by reference in the complaint."). For the purpose of resolving a motion to dismiss under Rule 12(b)(6), the Court presumes all well-pled facts to be true and draws all reasonable inferences in favor of plaintiff. *See Koch v. Christie's Int'l PLC*, 699 F.3d 141, 145 (2d Cir. 2012).

[2] Although Mount Sinai owns its website, it licenses its MyChart patient portal from Epic Software Systems, a privately-owned healthcare software company. FAC ¶ 1, n.3.

1. Facebook's Tracking Technologies

Facebook operates the world's largest social media company. In 2021, it generated $117 billion in revenue, roughly 97% of which came from selling advertising space. *Id.* ¶ 109. In conjunction with its advertising, Facebook encourages and promotes entities and website owners, such as Mount Sinai, to use its "Business Tools" to market products and services to individuals. *Id.* ¶ 110. Facebook's Business Tools, including the Pixel, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling interception and collection of user activity on those platforms. *Id.* ¶ 111. The Pixel transmits information from users' browsers to third parties, including Facebook and Google, Inc. (collectively, "Pixel Information Recipients"). *Id.* ¶ 16.

Website owners like Mount Sinai which use Facebook's Business Tools must agree to Facebook's Business Tools Terms. In these, Facebook requires website owners to "represent and warrant" that they have adequately and prominently notified users about the collection, sharing, and usage of data through Facebook's Business Tools (including the Pixel and CAPI) and that website owners "will not share Business Tool Data . . . that [websites] know or reasonably should know… include health or financial information or other categories of sensitive information." *Id.* ¶ 117. Facebook does not take other steps to verify that businesses using Pixel have obtained the required consent, but instead relies on this "honor system." *Id.* ¶ 126.

The Pixel is customizable and programmable, meaning that the website owner controls which of its web pages contain the Pixel and which events are tracked and transmitted to Pixel Information Recipients. *Id.* ¶¶ 59, 114. The Pixel is automatically configured to transmit "Standard Events," such as when a user visits a particular webpage, the webpage's Universal Resource Locator ("URL") and metadata, and button clicks. An advertiser can also build

"custom events" to track other user actions. *Id.* ¶¶ 119–120. The Pixel prompts users' web browsers to instantaneously and surreptitiously duplicate and transmit users' communications with the host webpage to Facebook's servers. *Id.* ¶ 121. This simultaneous transmission contains the original electronic communications (GET requests) sent to the host website, plus additional data that the Pixel is configured to collect. *Id.* ¶ 122.

Because internet users with technical know-how can circumvent the browser-based technology, Facebook offers CAPI as a workaround *Id.* ¶ 131. Unlike the Pixel, CAPI does not cause a user's browser to transmit information directly to Facebook. Rather, it tracks the user's website interactions, records and stores that information on the website owner's servers, and then transmits that data from the website owner's servers to Facebook. *Id.* ¶ 19. Because CAPI functions from the website owner's servers, it cannot be stymied by the use of anti-pixel software or other mechanisms such as ad blockers. *Id.* ¶ 20.

When the website visitor is a Facebook user, the information collected is associated with that user's Facebook ID. The Facebook ID captures the user's name and Facebook profile, which contains demographic and other information about the user, including pictures, personal interests, work history, and relationship status. *Id.* ¶¶ 127, 129. The Business Tools collect data regardless of whether the visitor has a Facebook account; Facebook maintains "shadow profiles" on users without Facebook accounts. *Id.* ¶ 128. After receiving these transmissions, Facebook processes, analyzes, and assimilates the data into datasets like Core Audiences and Custom Audiences. *Id.* ¶ 127. A website owner can create a "Custom Audience" to target ads to users who have shown interest in its business or product and measure the success of its marketing campaigns. *Id.* ¶¶ 143–47.

Facebook advertises its Pixel as a piece of code "that can help you better understand the effectiveness of your advertising and the actions people take on your site, like visiting a page or adding an item to their cart. You'll also be able to see when customers took an action after seeing your ad on Facebook and Instagram, which can help you with retargeting." It tells its customers: "when you use the Conversions API alongside the Pixel, it creates a more reliable connection that helps the delivery system decrease your costs." *Id.* ¶ 217 (emphasis removed). The Pixel thus enables "retargeting"—online marketing that targets users with ads based on previous internet communications and interactions. *Id.* ¶ 218. Facebook's purpose in collecting user data is to make money. *Id.* ¶ 134.

2. Mount Sinai's Privacy Policies

Mount Sinai publishes several privacy policies that represent to its patients and visitors to its Web Properties that it will keep their Private Information private and secure. *Id.* ¶ 148. The published Mount Sinai Privacy Policy states: "[Mount Sinai] employs a variety of online security measures to safeguard and keep your information private." *Id.* ¶¶ 149–50. It adds that:

> [Mount Sinai] does not share your personally identifiable information with third parties without your consent, except for third–party suppliers that perform essential business or administrative services for us (for example, our web hosting provider). [Mount Sinai] provides these suppliers with information they need to perform such services and asks that they either comply with this Privacy Policy or maintain comparable privacy policies that protect your personally identifiable information.

Id. Mount Sinai's Notice of Privacy Practices explains its legal duties with respect to Private Information and sets out the limited exceptions for when it can legally use and disclose Private Information. *Id.* ¶ 151.[3] Mount Sinai's Privacy Policy does not permit it to use or disclose

[3] As listed by Mount Sinai, these exceptions include:

> Treatment; Payment; Business operations; Appointment reminders, treatment alternatives, benefits and services; Fundraising ("We will not sell your PHI without

Private Information for marketing purposes. *Id.* ¶ 152. Mount Sinai acknowledges that it is "required by law to protect the privacy of [] health information." *Id.* ¶ 153.

3. Mount Sinai's Use of Facebook's Tracking Technologies

The FAC alleges that Mount Sinai used Facebook's Business Tools to intercept, duplicate, and re-direct their Private Information to Pixel Information Recipients. *Id.* ¶ 136. Mount Sinai tracked users through "PageView" (which identifies the User as having viewed the particular webpage), "Microdata" (which contains page metadata), and "SubscribedButtonClick" (which tracks each click on the webpage and shares the metadata of buttons clicked by the User, such the "inner text" of the button) events, and through custom events such as those reflected on the patient's "My Chart" portal, accessible through an app. Mount Sinai disclosed users' search queries, when they used the MyChart app, clicked to access and view the bill page, clicked to request an appointment, and when they accessed and viewed their care and treatment options. *Id.* ¶¶ 97, 123. Mount Sinai routinely provided Facebook with its patients' Facebook IDs, IP addresses and/or device IDs, and other information the patients entered into Mount Sinai's

---

> your authorization."); Business associates ("we will have a written contract with them that requires the BA and any of its subcontractors to protect the privacy of your PHI. They and their subcontractors are independently required by federal law to protect your information."); In-Patient Directory; Family and friends involved in your care; As required by law; Public health activities; Victims of abuse, neglect or domestic violence; Health oversight activities, Product monitoring, repair and recall; Lawsuits and disputes; Law enforcement; To avert a serious and imminent threat to health or safety; National security and intelligence activities or protective services; Military and veterans; Inmates and correctional institutions; Workers' compensation; Coroners, medical examiners and funeral directors; Organ and tissue donation; Research; Completely de-identified of partially de-identified information; Incidental disclosures ("While we will take reasonable steps to safeguard the privacy of your PHI, certain disclosures of your PHI may occur during or as an unavoidable result of our otherwise permissible uses or disclosures of your PHI").

FAC ¶ 151.

website, including their medical searches, treatment requests, the webpages they viewed, and their names, email addresses, and/or phone numbers. *Id.* ¶ 124. The FAC alleges that plaintiffs were easily identifiable based on this information. They contend that the Health Insurance Portability and Accountability Act ("HIPAA") requires Mount Sinai to anonymize such information to protect patients' privacy. *Id.* ¶ 125.[4]

The FAC alleges that a primary reason Mount Sinai decided to embed the Pixel and other tracking technologies on its Web Properties was to improve its marketing campaigns and reduce its marketing costs. *Id.* ¶ 213. Facebook, after receiving Private Information communicated on Mount Sinai's Web Properties, forwards this data and its analysis of this data to Mount Sinai to use for commercial purposes. *Id.* ¶¶ 214–15. Mount Sinai realizes a commercial benefit from using Facebook's Business Tools because the collected information enables it to target ads to existing and prospective patients. *Id.* ¶ 216. Insofar as patients' Private Information allows companies to gain insight into customers, targeted ads, and boost revenues, this data is valuable and monetizable. *Id.* ¶¶ 221, 231. In exchange for disclosing patients' Private Information, Mount Sinai is compensated by the Pixel Information Recipients, such as Facebook, in the form of enhanced advertising services and more cost-efficient marketing on their platforms. *Id.* ¶ 222.

[4] HIPAA's Privacy Rule, codified in 42 U.S.C. § 1320, requires any "covered entity"—which includes health care providers—to maintain appropriate safeguards to protect privacy of PHI and set limits and conditions on the disclosure of PHI. FAC ¶ 161. Of the approximately 18 HIPAA "identifiers" that are considered PII, those relevant here are names, dates related to an individual, email addresses, device identifiers, web URLs, and IP addresses. *Id.* ¶¶ 204–05. The statute states that a "person … shall be considered to have obtained or disclosed individually identifiable health information … if the information is maintained by a covered entity … and the individual obtained or disclosed such information without authorization." *Id.* ¶ 166. Violation of 42 U.S.C. § 1320(d)(6) is subject to criminal penalties where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." *Id.* ¶ 167.

4. Each Plaintiff's Use of Web Properties and Receipt of Targeted Ads[5]

The FAC alleges that each named Plaintiff was aware of Mount Sinai's duty of confidentiality and reasonably expected that the Private Information he or she provided to Mount Sinai would remain private and would not be shared with third parties for commercial purpose unrelated to patient care. *Id.* ¶¶ 197–99.

i. Plaintiff Ronda Cooper

Beginning in or around 2021, Cooper began using Mount Sinai's Web Properties on his phone and computer to research conditions, treatments, doctors, and specialists, and to schedule appointments. *Id.* ¶ 251. As recently as May 2023, Cooper disclosed his Private Information to Mount Sinai, including information about his specific medical conditions. *Id.* ¶¶ 252, 254. After disclosing his Private Information to Mount Sinai, Cooper began receiving targeted ads, including ads related to these conditions, on his social media accounts such as Facebook. *Id.* ¶ 262.

ii. Plaintiff Coral Fraser

Beginning in or around 2017, Fraser started to use Mount Sinai's website on her phone to research conditions, treatments, doctors, specialists, and to schedule appointments. *Id.* ¶ 267. As recently as May 2022, Fraser disclosed her Private Information to Mount Sinai, including information about her specific medical conditions. *Id.* ¶¶ 268–79. After disclosing her Private Information to Mount Sinai, Fraser began receiving targeted ads, including ads related to these conditions, on her social media accounts such as Facebook and/or Instagram. *Id.* ¶¶ 279–80.

---

[5] In a putative class action, to survive a motion to dismiss, the complaint must state a claim based on the facts alleged as to the named plaintiffs, not the putative class. *NECA-IBEW Health & Welfare Fund v. Goldman Sachs & Co.*, 693 F.3d 145, 159 (2d Cir. 2012); *Cent. States Se. & Sw. Areas Health & Welfare Fund v. Merck-Medco Managed Care, L.L.C.*, 504 F.3d 229, 241 (2d Cir. 2007).

iii. Plaintiff David Gitlin

Beginning in or around 2015, Gitlin started to use Mount Sinai's website on his phone and computer to research conditions, treatments, doctors, and specialists. *Id.* ¶ 283. Beginning in or around 2020, Gitlin started to use Mount Sinai's patient portal to schedule appointments. *Id.* ¶ 284. As recently as September 2023, Cooper disclosed his Private Information to Mount Sinai, including information about his specific medical conditions. *Id.* ¶¶ 285, 287. After disclosing his Private Information to Mount Sinai, Cooper began receiving targeted ads, including ads related to these conditions, on his social media accounts such as Facebook. *Id.* ¶¶ 295–96.

iv. Plaintiff Gilbert Manda

Beginning in or around August 2022, Manda started to use Mount Sinai's website on his phone and computer to receive healthcare services from Mount Sinai. *Id.* ¶ 300. Beginning in or around April 2023, Manda started to use Mount Sinai's patient portal. *Id.* ¶ 301. As recently as September 2023, Manda disclosed his Private Information to Mount Sinai, including information about his specific medical conditions. *Id.* ¶¶ 302, 304. After disclosing his Private Information to Mount Sinai, Manda alleges that he began receiving targeted ads, including ads related to his medications, conditions, treatments, and specific medical diagnoses, on his social media accounts such as Facebook. *Id.* ¶ 312.

***

Out of respect for privacy, the Court, heeding the redactions from the FAC as publicly filed, has not identified any individual plaintiff's health condition(s). It suffices to say that the conditions the FAC alleges were divulged by one or more plaintiffs in using Mount Sinai's web

services, but which later were the subject of that plaintiff's targeted Facebook ads, included anxiety/depression, pregnancy, and high cholesterol. *See generally id.* ¶¶ 252–312.

B. Procedural History

On October 27, 2023, Plaintiffs filed this action. Dkt. 1. On December 22, 2023, Mount Sinai filed a motion to dismiss. Dkt. 13. On December 28, 2023, the Court ordered Plaintiffs to oppose the motion or amend the complaint, pursuant to Federal Rule of Civil Procedure 15(a). Dkt. 15. On January 12, 2024, Plaintiffs filed the FAC, the operative complaint. Dkt. 16 ("FAC").

The FAC brings 10 claims, each on behalf of a putative class. These include one claim under federal law, under the Electronic Communications Privacy Act (the "ECPA" or "Wiretap Act"), 18 U.S.C. §§ 2510, *et seq.* FAC ¶¶ 341–70. It also contains a statutory claim for deceptive practices under New York General Business Law § 349, FAC ¶¶ 447–65, and eight claims under New York State common law: for negligence, *id.* ¶¶ 371–80, invasion of privacy, *id.* ¶¶ 381–94, breach of implied contract, *id.* ¶¶ 395–405, breach of fiduciary duty, *id.* ¶¶ 406–412, unjust enrichment, *id.* ¶¶ 413–20, breach of confidence, *id.* ¶¶ 421–28, constructive bailment, *id.* ¶¶ 429–37, and breach of the implied covenant of good faith and fair dealing, *id.* ¶¶ 438–46.

On January 26, 2024, Mount Sinai filed a motion to dismiss the FAC and a memorandum of law in support. Dkts. 18, 19 ("Def Br."). On February 9, 2024, Plaintiffs filed an opposition. Dkt. 20 ("Pl. Br."). On February 16, 2024, Mount Sinai filed a reply. Dkt. 21 ("Def. Reply Br.").[6]

[6] Both parties have since filed notices of supplemental authority and responses to each other's notices. Dkts. 22–26.

II. Legal Standards Governing Motions to Dismiss

To survive a motion to dismiss under Rule 12(b)(6), a complaint must plead "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 the plaintiff pleads factual content that allows 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). A complaint is properly dismissed where, as a matter of law, "the allegations in a complaint, however true, could not raise a claim of entitlement to relief." *Twombly*, 550 U.S. at 558. When resolving a motion to dismiss, the Court must assume all well-pleaded facts to be true, "drawing all reasonable inferences in favor of the plaintiff." *Koch*, 699 F.3d at 145. That tenet, however, does not apply to legal conclusions. *See Iqbal*, 556 U.S. at 678. Pleadings that offer only "labels and conclusions" or "a formulaic recitation of the elements of a cause of action will not do." *Twombly*, 550 U.S. at 555.

III. Discussion

Mount Sinai moves to dismiss the FAC in its entirety. The Court considers each claim in turn.

A. Federal Wiretap Act

Mount Sinai argues that the claim under the ECPA fails because the FAC does not adequately allege that Mount Sinai intercepted communications with the requisite intent. Def. Br. at 6–10. The FAC adequately so alleges.

The ECPA provides for a private right of action against "any person who . . . intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept wire, oral, or electronic communication." 18 U.S.C. § 2511. "Intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral

communication through the use of any electronic, mechanical, or other device." *Id.* § 2510(4). The statute excepts from liability interceptions where the intercepting person "is a party to the communication or where one of the parties to the communication has given prior consent to such interception." *Id.* § 2511(2)(d). But that exception does not apply where the "aggrieved individual . . . has had her oral communications intentionally intercepted by a party to those communications for the purpose of committing a crime or tort." *Caro v. Weintraub*, 618 F.3d 94, 97 (2d Cir. 2010) (citing 18 U.S.C. §§ 2520, 2511(1), 2511(2)(d)).

This "crime-tort exception" is "construed narrowly." *In re DoubleClick Inc. Privacy Litig. ("DoubleClick")*, 154 F. Supp. 2d 497, 515 (S.D.N.Y. 2001); *United States v. Jiau*, 734 F.3d 147, 152 (2d Cir. 2013). The crime or tort must have been the "primary motivation" or "a determinative factor" for the defendant's conduct. *DoubleClick*, 154 F. Supp. 2d at 514–15; *United States v. Tarantino*, 617 Fed. App'x. 62, 65 (2d Cir. 2015). Thus, the defendant must have a criminal or tortious purpose at the time of the interception that is "independent of the act of recording itself." *Caro*, 618 F.3d at 100 ("If, at the moment he hits 'record,' the offender does not intend to use the recording for criminal or tortious purposes, there is no violation. But if, at the time of the recording, the offender plans to use the recording to harm the other party to the conversation, a civil cause of action exists under the Wiretap Act."). That a defendant's conduct was criminal or tortious does not suffice. *Id.* But "the mere existence of [a] lawful purpose alone does not "sanitize a[n interception] that was also made for an illegitimate purpose." *DoubleClick*, 154 F. Supp. 2d at 514 (quoting *Sussman v. ABC*, 186 F.3d 1200, 1202 (9th Cir. 1999)).

The parties' dispute here centers on whether the crime-tort exception is adequately pled. For purposes of its motion, Mount Sinai does not dispute that it "intercepted" Plaintiffs'

communications (*i.e.*, their user activity on Mount Sinai's Web Properties). And Plaintiffs do not dispute that Mount Sinai is alleged to have been a party to the communications at issue, requiring the crime-tort exception to apply for it be liable.[7] FAC ¶ 362.

Plaintiffs argue that the exception applies because, as pled, Mount Sinai intercepted their communications with the purpose of disclosing them to Facebook and other third parties without Plaintiffs' consent "in violation of the laws of the United States and New York," FAC ¶¶ 363–64, in particular, with the criminal purpose to violate HIPAA, *id.* ¶ 165.[8]

---

[7] There is a division of authority whether the party exemption applies when defendants receive communications via third-party tracking devices that simultaneously duplicate and forward GET requests. *Compare In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 608 (9th Cir. 2020) (simultaneous duplication and forwarding of GET requests does not qualify for the party exemption), *with In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 142–43 (3d Cir. 2015) (simultaneous duplication and forwarding of GET requests does qualify for the party exemption). That issue is not implicated here because, as pled, Mount Sinai controlled and maintained its Web Properties.

[8] The Court puts aside as ill-pled the FAC's separate theory of criminality: that Mount Sinai engaged in a "scheme or artifice to defraud," FAC ¶ 366, by placing "the 'fbp' cookie on patient computing devices disguised as a first-party cookie on Mount Sinai's Web Properties rather than a third-party cookie from Meta." *Id.* ¶¶ 367–68. Mount Sinai argues that these fail Rule 9(b)'s standard for pleading fraud. Def. Br. at 10. It is not clear that Rule 9(b) applies here. It requires that "[i]n all averments of fraud or mistake, the circumstances constituting fraud or mistake shall be stated with particularity," but it states that "[m]alice, intent, knowledge, and other condition of mind of a person may be averred generally." Regardless, the FAC's theory of fraud fails, because there is no statutory basis to find the § 2511(2)(d) exception inapplicable to fraudulently induced communications. *See In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 143 (3d Cir. 2015) ("Though we are no doubt troubled by the various deceits alleged in the complaint, we do not agree that a deceit upon the sender affects the presumptive non-liability of parties under § 2511(2)(d)."); *Clemons v. Waller*, 82 F. App'x 436, 441 (6th Cir. 2003) (rejecting theory that defendant's "use of fraud and deceit vitiated his claim to be a party to the communication."); *United States v. Pasha*, 332 F.2d 193, 198 (7th Cir. 1964) ("We believe that impersonation of the intended receiver is not an interception within the meaning of the statute."); *see also Caro,* 618 F.3d at 100.

The Court also puts aside the FAC's allegation that Mount Sinai had a tortious purpose to invade patients' privacy. FAC ¶ 357. The FAC pleads that New York law applies to all Plaintiffs (and the putative class). FAC ¶ 333. Under New York law, that is insufficient to trigger the crime-tort exception. Invasion of privacy is a common law tort that may satisfy the crime-tort

HIPAA makes it a crime for a "covered entity"—which includes health care providers—to knowingly disclose individually identifiable heath information without authorization "with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320d-6; 45 C.F.R. § 160.103. Such information is "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and either (i) "identifies the individual;" or (ii) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

A defendant's criminal or tortious purpose of "knowingly . . . disclos[ing] individually identifiable health information to another person," 42 U.S.C. § 1320d-6, in violation of HIPAA, may satisfy the crime-tort exception. *See Kane v. Univ. of Rochester*, No. 23 Civ. 6027 (FPG), 2024 WL 1178340, at *7 (W.D.N.Y. Mar. 19, 2024) ("Plaintiffs have plausibly alleged that Defendant's purpose was to commit an act that is punishable as a crime under 42 U.S.C. § 1320d-6: knowingly disclosing [individually identifiable health information] without

---

exception. *Caro*, 618 F.3d at 100 ("The only tort [plaintiff] asserts in his complaint that could plausibly provide the intent necessary to bring the recording under the Wiretap Act is invasion of privacy, a tort recognized under Connecticut common law."). But New York law does not recognize a legal claim for invasion of privacy. *Howell v. N.Y. Post Co., Inc.*, 81 N.Y.2d 115, 123 (1993) ("[I]n this State, the right to privacy is governed exclusively by section 50 and 51 of the Civil Rights Law; we have no common law of privacy."); *see also Burke v. Dollar Tree Stores, Inc.*, 2022 WL 15523465, at *4 (W.D.N.Y. Oct. 27, 2022) ("New York does not recognize a common law right to privacy claim."). Presumably for this reason, Plaintiffs, in the course of briefing this motion, withdrew their common-law claim of invasion of privacy. Pl. Br. at 18 n.11.

authorization for marketing purposes."); *In re Grp. Health Plan Litig.*, No. 23 Civ. 267 (JWB), 2023 WL 8850243, at *8 (D. Minn. Dec. 21, 2023) (crime-tort exception plausibly applies where defendant's primary motivation was to use patient data for marketing, in violation of HIPAA); *Kurowski v. Rush Sys. for Health*, No. 22 Civ. 5380, 2023 WL 8544084, at *3 (N.D. Ill. Dec. 11, 2023) ("All of these allegations, taken together, are sufficient to invoke the HIPAA exception-to-the-party-exception[.]"); *see also Cousin v. Sharp Healthcare*, No. 22 Civ. 2040 (MMA) (DDL), 2023 WL 8007350, at *5 (S.D. Cal. Nov. 17, 2023) (denying motion to dismiss [California Invasion of Privacy Act] claim, noting that analysis tracks that under the federal Wiretap Act, where complaint plausibly alleged that defendants conveyed their private health information); *cf. Doe v. Kaiser Found. Health Plan, Inc.*, No. 23-Civ. 02865 (EMC), 2024 WL 1589982, at *10 (N.D. Cal. Apr. 11, 2024) (dismissing wiretap claim because "[v]iolation of HIPAA was not the purpose of the alleged interception."); *Okash v. Essentia Health*, No. 23 Civ. 482 (JRT) (LIB), 2024 WL 1285779, at *4 (D. Minn. Mar. 26, 2024) ("[Plaintiff] alleges that [defendant] acted for the purpose of criminally violating HIPAA and tortiously invading [his] privacy. But because neither the alleged HIPAA nor privacy violations were independent of the interception, the crime-tort exception does not apply.").

With all reasonable inferences drawn in its favor, the FAC plausibly alleges that Mount Sinai knowingly disclosed individually identifiable health information to Pixel Information Recipients and thereby violated HIPAA. With respect to individually identifiable health information, the FAC alleges that Mount Sinai disclosed Plaintiffs' names, emails, computer IP addresses, device identifiers, web URLs, and the days on which they sought treatment, as well as the services they selected, and their patient statuses, medical conditions, treatments, and provider and appointment information. FAC ¶ 206. The FAC alleges that Plaintiffs thereafter received

targeted ads on Facebook keyed to their confidential health conditions. *See id.* ¶¶ 251–315. These allegations make plausible that at least some information transmitted was individually identifiable health information. *Cf. Santoro v. Tower Health*, No. 22 Civ. 4580, 2024 WL 1773371, at *4 (E.D. Pa. Apr. 24, 2024) ("As best as we can tell from the allegations and undisputed representations, whether individually identifiable health information is intercepted could depend upon how the particular user interacts with the website, including how long they spend on a page, what links are clicked on, and what search terms they input—as well as the nature of the user's health condition and treatment plan. We need not define what constitutes HIP[A]A-protected information or otherwise flesh out plaintiffs' speculation. It is plaintiffs' responsibility to make factual allegations that plausibly state a claim for relief, and they have not done so here . . . For that reason, we conclude that plaintiffs fail to state a claim for a violation of the Wiretap Act."); *Kurowski v. Rush Sys. for Health*, 683 F. Supp. 3d 836, 843 (N.D. Ill. 2023) (complaint did not allege sufficient facts to support inference of disclosure of individually identifying health information; court contrasts defendant's disclosure of "metadata" with case in which a plaintiff "entered data relating to her heart issues and high blood pressure in MyChart and later received advertisements on Facebook, including at least one advertisement relating to high blood pressure medication." (citing *Doe v. Regents of Univ. of California*, 672 F. Supp. 3d 813, 816 (N.D. Cal. 2023))); *Smith v. Facebook, Inc.*, 745 F. App'x 8, 9 (9th Cir. 2018) ("Information available on publicly accessible websites stands in stark contrast to the personally identifiable patient records and medical histories protected by these statutes—information that unequivocally provides a window into an individual's personal medical history."). The claim that Plaintiffs were sent targeted ads keyed to distinct health conditions after they entered

information disclosing those conditions into Mount Sinai's Web Properties plausibly alleges that Mount Sinai illegally disclosed their private medical information.

The FAC also plausibly alleges that Mount Sinai engaged in such disclosures knowingly and deliberately. It alleges that the process of adding the Pixel to a webpage is a multi-step process that must be undertaken by the website owner—here, Mount Sinai. FAC ¶ 114. And it alleges that Mount Sinai configured Facebook's Business Tools, to capture "PageView," "Microdata," and "SubscribedButtonClick" events, and to create a patient-customized "MyChart" event that would be transmitted to Facebook. *Id.* ¶ 123. By deciding to track these events, the FAC alleges, Mount Sinai routinely sent Facebook individually identifiable information that the Plaintiffs had had entered into Mount Sinai's Web Properties. *Id.* ¶ 124. And the FAC plausibly alleges that Mount Sinai had an economic motive—to improve its marketing—to install the Pixels and CAPI. FAC ¶¶ 11 ("[Mount Sinai] installed tracking technologies on its Web Properties to collect and disclose to unauthorized third parties their Private Information for its own pecuniary gain."), 26 ("Mount Sinai chose to use the Pixel and CAPI data for marketing purposes to bolster its revenue."), 213 ("One of the primary reasons that Mount Sinai decided to embed Pixels and other tracking technologies on its Web Properties was to improve marketing by creating campaigns that maximize conversions and thereby decrease costs to Mount Sinai and boost its revenues."), 358 ("Mount Sinai intentionally used wire or electronic communications to increase its profit margins.").

Mount Sinai will be at liberty to attempt to establish in discovery facts supporting, *inter alia*, that, to the extent it took the above actions, it did so without intending to facilitate Facebook's receipt of confidential patient information or to financially benefit. Mount Sinai may be able to establish, at summary judgment or trial, that it acted without the requisite knowledge

and intent. But, taking the FAC's allegations as true, as the Court must at the motion to dismiss stage,[9] they plausibly support the inference that Mount Sinai, for commercial ends, intentionally disclosed individually identifiable patient health information, and thus violated HIPAA, which makes it a crime for a health care provider to disclose individually identifiable health information for commercial gain. 42 U.S.C. § 1320d-6.[10] *See Caro*, 618 F.3d at 99 ("At the time of the recording the offender must intend to use the recording to commit a criminal or tortious act."); *In re DoubleClick Inc. Priv. Litig.*, 154 F. Supp. 2d at 515 ("[T]he legislative record suggests that the element of 'tortious' or 'criminal' mens rea is required to establish a prohibited purpose under § 2511(2)(d)."); *Cohen v. Casper Sleep Inc.*, No. 17 Civ. 9325, 2018 WL 3392877, at *4 (S.D.N.Y. July 12, 2018) ("[Plaintiff] fails to demonstrate that Defendants' primary purpose was to commit a tort. Instead, he claims that Defendants' conduct amounted to a tort."); *Doe v. Meta Platforms, Inc.*, 690 F. Supp. 3d 1064, 1078 (N.D. Cal. 2023) ("Determination of whether actual consent was given depends on what Meta disclosed to healthcare providers, how it described and trained healthcare providers on the Pixel, and how the healthcare providers understood the Pixel worked and the information that then could or would be collected by Meta. These evidence-bound determinations are inappropriate to reach on this motion.").

---

[9] *See, e.g., In re Grp. Health Plan Litig.*, 2023 WL 8850243, at *8 ("While Plaintiffs have alleged [Defendant's] motivations, determination of [Defendant's] actual purpose . . . requires a factual undertaking. Plaintiffs, without the benefit of discovery, have met the pleading requirements to plausibly allege the crime-tort exception applies."); *Kane v. Univ. of Rochester*, 2024 WL 1178340, at *8 ("Defendant may be able to show that, as a factual matter, that they did not intercept Plaintiffs' communications for that purpose. But at this stage of the proceedings, Plaintiffs, without the benefit of discovery, have plausibly alleged that the tort-crime exception applies."); *cf. In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778 (N.D. Cal. 2022) (declining to issue preliminary injunction but noting that "[t]here is a not-insignificant chance, then, that plaintiffs may be able to show that the crime-tort exception applies.").

[10] Where the defendant acted with such a motive in disclosing individually identifiable health information, HIPAA makes such a crime. 42 U.S.C. § 1320d-6.

Mount Sinai's two arguments to the contrary are unavailing.

First, relying on statements in out-of-circuit cases applying the ECPA to conduct not alleged to violate HIPAA, it argues the mere fact that it acted for monetary gain does not mean that it had a criminal or tortious purpose. *See In re Google Inc. Gmail Litig.*, 13 Civ. 2430 (LHK), 2014 WL 1102660, at *18 n.13 (N.D. Cal. Mar. 18, 2014); *Rodriguez v. Google LLC*, 20 Civ. 4688 (RS), 2021 WL 2026726, at *6 n.8 (N.D. May 21, 2021); *Katz-Lacabe v. Oracle Am.*, Inc., 668 F. Supp. 3d 928, 945 (N.D. Cal. 2023). But where a covered person intentionally disclosed patients' individually identifiable health information, HIPAA makes such a crime, and indeed imposes enhanced penalties when such was done for, *inter alia*, a "commercial advantage" or "personal gain." 42 U.S.C. § 1320d-6 ("A person who knowingly and in violation of this part—(1) uses or causes to be used a unique health identifier; (2) obtains individually identifiable health information relating to an individual; or (3) discloses individually identifiable health information to another person, shall . . . if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both."). Mount Sinai's broad theory that the presence of a primary financial motive inoculates a defendant from liability under the ECPA is wrong. *See DoubleClick*, 154 F. Supp. 2d at 514 (quoting *Sussman v. ABC*, 186 F.3d 1200, 1202 (9th Cir. 1999)); *see also R.C. v. Walgreen Co.*, No. 23 Civ. 1933 (JGB) (SPX), 2024 WL 2263395 at *15 (C.D. Cal. May 9, 2024) ("But even where a defendant is arguably motivated by monetary gain, the crime-tort exception may nonetheless apply if plaintiffs have adequately alleged that the defendant's conduct violated state law"). And none of the ECPA cases on which Mount Sinai relies in advancing this improbable theory involved alleged violations of HIPAA (or like statutes criminalizing disclosure of private

information for commercial purposes). *See In re Google Inc. Gmail Litig.*, 2014 WL 1102660, at *18 n.13 (alleged interception of Gmail messages); *Rodriguez*, 2021 WL 2026726, at *6 n.8 (alleged interception of communications with company's software development kit); *Katz-Lacabe v. Oracle Am.*, Inc., 668 F. Supp. at 945 (alleged tracking of web browsing activities).

Second, Mount Sinai argues that the FAC does not allege a criminal or tortious purpose on its part, on the ground that it is not proper to infer such intent from a defendant's actions. In so arguing, it relies on *DoubleClick*, in which Judge Buchwald rejected an attempt "to meet § 2511(2)(d)'s 'purpose' requirement by arguing that [Plaintiffs'] six non-Wiretap Act claims against DoubleClick 'plead conduct that has underlying it a tortious purpose and/or that translates into tortious acts." *See* 154 F. Supp. 2d at 515. But the FAC's basis for inferring a criminal purpose here is not merely the fact of Mount Sinai's wiretapping—its interception of Plaintiffs' communications with Mount Sinai's Web Properties. It is also that Mount Sinai's business arrangement with Facebook reveals its intent to profit commercially from exploiting Private Information, in violation of HIPAA. These allegations supply an adequate basis on which to infer criminal intent.

In sum, the FAC thus plausibly alleges that the crime-tort exception applies. It thus states a claim under the Wiretap Act.

B. New York G.B.L. § 349

The FAC alleges that Mount Sinai is liable for deceptive consumer acts and practices under New York General Business Law ("NYGBL") § 349. To state a claim under § 349, "a plaintiff must allege that a defendant has engaged in (1) consumer-oriented conduct that is (2) materially misleading and that (3) plaintiff suffered injury as a result of the allegedly deceptive act or practice." *Orlander v. Staples, Inc.*, 802 F.3d 289, 300 (2d Cir. 2015) (quoting *Koch v.*

Acker, Merrall & Condit Co., 944 N.Y.S.2d 452, 452 (2012)). A plaintiff must allege actual injury, although that need not take the form of a pecuniary harm. *See Stutman v. Chem. Bank*, 709 N.Y.S.2d 892, 896 (2000).

The FAC's § 349 claim is based on Mount Sinai's "promising to maintain the privacy and security of Plaintiff's and Class Members' PHI" and "failing to disclose or omitting material facts . . . regarding disclosure of [] Private Information to Facebook" in its Privacy Policy and HIPAA Privacy Notice. FAC ¶ 448; *see also id.* ¶¶ 449–65. In moving to dismiss, Mount Sinai argues that the FAC fails to allege (1) any deceptive, as opposed to unfair, practice, and (2) that Mount Sinai's deceptive acts, if any, caused an actual injury. Def. Br. at 10–13; Def. Reply at 4–6. These arguments are easily put aside.

Mount Sinai ultimately appears to relent on the first argument, in that it tacitly concedes—as is clearly correct—that the FAC does not pursue a statutorily unavailable theory of "unfair" practices. *See* Def. Reply Br. at 4. And the facts recited above adequately plead what the statute requires for liability, to wit, consumer-oriented conduct that was materially misleading to a reasonable consumer. The FAC pleads, with factual support, that Mount Sinai's Privacy Policy and HIPAA Privacy Notice were flatly false in representing that the hospital would not collect (or share with outsiders like Facebook) patient's confidential personal health data.

Mount Sinai, however, contends that privacy injuries are not cognizable under the statute. Def. Reply Br. at 5–6. That is wrong. New York courts have held that a privacy injury can be the basis for a § 349 claim "where confidential, individually identifiable information—such as medical records or a social security number—is collected without the individual's knowledge or consent." *Mount v. PulsePoint, Inc.*, 684 Fed. App'x 32, 35 (2d Cir. 2017) (citing *Meyerson v.*

Prime Realty Servs., LLC, 796 N.Y.S.2d 848, 850 (Sup. Ct. N.Y. Cty. 2005); *Anonymous v. CVS Corp.*, 728 N.Y.S.2d 333, 335 (Sup. Ct. N.Y. Cty. 2001) (deceptive practice of disclosing prescription information to third party injured plaintiffs). The FAC so pleads here. It pleads that Mount Sinai, via the Facebook Pixel, collected confidential, individually identifiable information constituting medical records without the Plaintiffs' knowledge or consent. FAC ¶¶ 456–62. And it pleads that Mount Sinai's deceptive representations that it would not disclose such information to third parties caused the cognizable privacy injury, by inducing Plaintiffs to submit private medical data and thereby lose control of it. *Id.* ¶¶ 461–62. *See, e.g.*, *Stutman*, 709 N.Y.S.2d at 898 (causation adequately pled where complaint alleged that defendant promised there would not be a prepayment charge for loan, but assessed a charge anyhow); *Kane*, 2024 WL 1178340, at *18 (causation pled where relevant provisions of privacy policies deceived plaintiff "into providing [private information] to Defendant").

The FAC thus states a claim under § 349.

C. New York Common Law Claims

Mount Sinai next moves to dismiss the FAC's New York state common law claims.[11]

1. Negligence

Mount Sinai argues that the FAC's negligence claim must be dismissed because the FAC, while alleging negligent conduct, *see* FAC ¶¶ 371–80, alternatively alleges Mount Sinai's willful, knowing, and/or intentional conduct, *id.* ¶¶ 381–94. *See* Def. Br. at 14–15. That is wrong. Under Federal Rule of Civil Procedure 8, a complaint may plead in the alternative, in this case, by alleging intentional and negligent conduct on Mount Sinai's part. *See, e.g.*, *In re*

[11] Plaintiffs, in their response brief, have withdrawn the FAC's claim for invasion of privacy. Pl. Br. at 18 n.11. The Court dismisses that claim on consent.

Livent, Inc. Noteholders Sec. Litig., 151 F. Supp. 2d 371, 406–07 (S.D.N.Y. 2001) ("Rule 8(e) permits a plaintiff to make two or more 'statements of a claim' alternatively. . . . In addition, plaintiffs may state as many separate claims as they have regardless of consistency."); *Henry v. Daytop Village, Inc.*, 42 F.3d 89, 95–96 (2d Cir. 1994) ("Pursuant to Rule 8(e)(2) . . . we may not construe Henry's first claim as an admission against another alternative or inconsistent claim."). The claim that Mount Sinai failed to take due care not to violate the law by divulging Plaintiffs' private health information, *see* FAC ¶¶ 371–80, may thus stand alongside the claim that Mount Sinai intentionally interfered with Plaintiffs' "interest in solitude and/or seclusion," *id.* ¶¶ 381–94. And the FAC pleads a factual basis for the negligence claim, as it must. *See In re Livent, Inc.*, 151 F. Supp. 2d at 407 (claim pled in alternative "must be sufficient standing on its own."). Mount Sinai does not dispute that point. *See* Def. Br. at 15 (quoting FAC ¶ 373).

Mount Sinai does argue that, because the FAC incorporates by reference in this claim its factual allegations of intentional conduct, its negligence claim is deficient. Def. Reply Br. at 6–7 (noting that FAC ¶ 371 commences its pleading of the negligence claim by "repeat[ing] and re-alleg[ing]" each preceding factual allegation). Mount Sinai does not cite any legal authority for dismissal on that basis. And its bid for dismissal on that asserted technicality is inconsistent with a plaintiff's established right under Rule 8(e) to plead inconsistent claims in the alternative.

2. Breach of Implied Contract; Breach of Fiduciary Duty; Breach of Confidence; Constructive Bailment; Implied Covenant of Good Faith & Fair Dealing

Mount Sinai next argues that the FAC's claims of breach of implied contract, FAC ¶¶ 406–12, breach of fiduciary duty, *id.* ¶¶ 413–20, breach of confidence, *id.* ¶¶ 421–28, constructive bailment, *id.* ¶¶ 429–37, and breach of the implied covenant of good faith and fair

dealing, *id.* ¶¶ 438–46, all duplicate, and must be dismissed in favor of, a claim for breach of physician-patient confidentiality. Def. Br. at 15–17. That argument fails.

The FAC does not bring a claim for breach of physician-patient confidentiality. New York courts have recognized a common-law cause of action arising from a physician's breach of doctor-patient confidentiality. *See Fedell v. Wierzbieniec*, 485 N.Y.S.2d 460, 461–62 (Sup. Ct. 1985), *aff'd*, 498 N.Y.S.2d 1013 (1986) (recounting history of this cause of action). But the FAC does not claim this tort. The legal principle commanding—in some circumstances—the dismissal of a claim as duplicative of another based on the same facts and seeking the same relief, *see, e.g.*, *IKB Int'l, S.A. v. Wells Fargo Bank, N.A.*, 197 N.Y.S.3d 719, 728–29 (2023) (where plaintiffs bring a tort claim based on a theory, also pursued, of contract damages, the tort claim should be dismissed as duplicative); *Campbell v. Whole Foods Mkt. Grp., Inc.*, 516 F. Supp. 3d 370, 393–94 (S.D.N.Y. 2021) (claim for unjust enrichment should be dismissed where duplicative of other claims), thus does not apply here.

In any event, even had the FAC pursued a claim for breach of physician-patient confidentiality, it is not clear that such would require dismissal of the other common-law claims as duplicative. Mount Sinai cites cases that it contends support that dismissal of other claims in favor of the complaint's more "appropriate" physician-patient confidentiality-breach claim. *See* Def. Br. at 15–17 (citing *MacDonald v. Clinger*, 446 N.Y.S.2d 801 (1982); *Fedell*, 485 N.Y.S.2d 460)). But these holdings either turn on comparisons between the claims pled in those cases, which led the court to find that the physician-patient claim alone adequately captured the injury alleged and supported the damages sought, or consist of theoretical discussions of the claims available to a New York plaintiff. *See MacDonald*, 446 N.Y.S.2d at 486 (pure breach of contract action would not fully capture injury caused by a breach of a doctor's duty of confidentiality);

Fedell, 485 N.Y.S.2d at 462 (holding claim of breach of doctor-patient confidentiality most appropriate in case where plaintiff's doctor in personal injury lawsuit allegedly wrongfully gave defense confidential information about plaintiff). With no such claim pled here, the Court is ill-equipped to say whether such a claim, if pled, would necessarily be held more appropriate than the common claims that Plaintiffs do plead. And Mount Sinai has not cited cases dismissing common law claims of the nature at issue here (breach of implied contract, breach of fiduciary duty, breach of confidence, constructive bailment, and breach of the implied covenant of good faith and fair dealing) as duplicative of a claim for breach of doctor-patient confidentiality.

Mount Sinai, finally, contends that the FAC does not plead facts sufficient to support a claim of a breach of physician-patient confidentiality because, *inter alia*, it does not tie its claims to any particular physician, and thus the information at issue can not necessarily be viewed as from a "patient." Def. Br. at 17–20. That argument is a non-starter as there is no such claim to dismiss. If anything, Mount Sinai's discussion may help explain Plaintiffs' decision not to claim such a tort.

Accordingly, the Court denies Mount Sinai's motion to dismiss the above common-law claims.

3. Unjust Enrichment

Finally, Mount Sinai moves to dismiss the FAC's claim for unjust enrichment (1) as duplicative of its implied contract claim, and (2) because it does not adequately allege that Mount Sinai was enriched at Plaintiffs' expense. Def. Br. at 20–22.

Unjust enrichment "lies as a quasi-contract claim" that "contemplates 'an obligation imposed by equity to prevent injustice, in the absence of an actual agreement between the parties.'" *Georgia Malone & Co. v. Rieder*, 950 N.Y.S.2d 333, 336 (2012) (citation omitted).

But "unjust enrichment is not a catchall cause of action to be used when others fail." *Corsello v. Verizon N.Y., Inc.*, 944 N.Y.S.2d 732, 740 (2012). The claim "is available only in unusual situations when, though the defendant has not breached a contract nor committed a recognized tort, circumstances create an equitable obligation running from the defendant to the plaintiff." *Id.* "An unjust enrichment claim is not available where it simply duplicates, or replaces, a conventional contract or tort claim." *Id.*

Here, the conduct underlying the FAC's unjust enrichment claim is the same underlying its implied contract claim (and its other tort claims). All are based on Mount Sinai's allegedly wrongful collection and disbursement of Plaintiffs' confidential medical information. *See* FAC ¶¶ 413–20 (alleging unjust enrichment on the basis that "Plaintiffs and Class Members conferred a benefit upon Mount Sinai in the form of the monetizable Private Information that Mount Sinai collected from them and disclosed to third parties, including the Pixel Information Recipients, without authorization and proper compensation").

The FAC does appear to plead distinct damages arising from this claim, insofar as the claim contends that, having unjustly profited from the mining and sale of Plaintiffs' data, Mount Sinai should have to "disgorge into a common fund for the benefit of Plaintiffs and the Class." *Id.* ¶ 420. "But the opportunity for plaintiffs to glean a larger damage award does not distinguish the violative conduct alleged under the rubric of unjust enrichment from that underlying the other claims." *Patellos v. Hello Prods., LLC*, 523 F. Supp. 3d 523, 537–38 (S.D.N.Y. 2021) (dismissing unjust enrichment claim as duplicative of other tort and contract claims despite fact that damages on unjust enrichment claim alone could have entailed disgorgement of defendants' total revenue on sales of a product).

The Court accordingly dismisses this claim as duplicative. *See, e.g.*, *Emps. Ins. v. Zemlyansky*, No. 13 Civ. 4966 (MKB) (SMG), 2015 WL 5692899, at *2 (E.D.N.Y. Sept. 27, 2015) ("[A]n unjust enrichment claim is not available where it simply duplicates, or replaces, a conventional contract or tort claim." (internal alteration omitted)); *Cont'l Cas. Co. v. Contest Promotions NY, LLC*, No. 15 Civ. 501 (MKB), 2016 WL 1255726, at *3–4 (E.D.N.Y. Mar. 28, 2016) (denying motion for default judgment where unjust enrichment claim duplicative of breach of contract claim).

CONCLUSION

For the forgoing reasons, the Court denies Mount Sinai's motion to dismiss except as to the FAC's unjust enrichment claim, which the Court dismisses as duplicative, and its claim for invasion of privacy, which is dismissed on consent. In a separate order today, the Court will schedule an initial pre-trial conference.

The Clerk of Court is respectfully directed to close all pending motions.

SO ORDERED.

Paul A. Engelmayer
United States District Judge

Dated: July 30, 2024
New York, New York