MORGAN & MORGAN COMPLEX LITIGATION GROUP
Michael F. Ram (SBN 104805)
mram@forthepeople.com
711 Van Ness Ave, Suite 500
San Francisco, CA 94102
Tel.: (415) 358-6913

MORGAN & MORGAN COMPLEX LITIGATION GROUP
John A. Yanchunis (*pro hac vice*)
jyanchunis@forthepeople.com
Ryan J. McGee (*pro hac vice*)
rmcgee@forthepeople.com
201 N. Franklin St., 7th Floor
Tampa, FL 33602
Tel.: (813) 223-5505

CLARKSON LAW FIRM, P.C.
Ryan J. Clarkson (CA SBN 257074)
rclarkson@clarksonlawfirm.com
Yana Hart (CA SBN 306499)
yhart@clarksonlawfirm.com
Tiara Avaness (CA SBN 343928)
tavaness@clarksonlawfirm.com
Valter Malkhasyan (CA SBN 348491)
vmalkhasyan@clarksonlawfirm.com
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050

CLARKSON LAW FIRM, P.C.
Tracey Cowan (CA SBN 250053)
tcowan@clarksonlawfirm.com
95 3rd St., 2nd Floor
San Francisco, CA 94103
Tel: (213) 788-4050

Counsel for Plaintiffs and the Proposed Classes

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

PLAINTIFFS MARILYN COUSART; NICHOLAS GUILAK; PAUL MARTIN; BREONNA ROBERTS; CAROLINA BARCOS; JAIR PAZ; ALESSANDRO DE LA TORRE; VLADISSLAV VASSILEV; SEAN ALEXANDER JOHNSON; JENISE MCNEAL; N.B, a minor; LORENA MARTINEZ; JOHN HAGAN, individually, and on behalf of all others similarly situated,

Plaintiffs,

vs.

OPENAI LP; OPENAI INCORPORATED; OPENAI GP, LLC; OPENAI STARTUP FUND I, LP; OPENAI STARTUP FUND GP I, LLC; OPENAI STARTUP FUND MANAGEMENT LLC; MICROSOFT CORPORATION and DOES 1 through 20, inclusive,

Defendants.

Case No.: 23-cv-04557-VC

PLAINTIFFS' OPPOSITION TO DEFENDANT OPENAI'S MOTION TO DISMISS FIRST AMENDED CLASS ACTION COMPLAINT

Date: April 18, 2024
Time: 10:00 a.m.
Place: Courtroom 4

Judge: The Honorable Vince Chhabria

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Rules & Statutes

I. INTRODUCTION

OpenAI's motion begins by touting the virtues of Artificial Intelligence. Plaintiffs' Complaint, too, acknowledges the potential benefits to humanity. But that does not grant Big Tech a license to violate the law. Instead, two things can be true: we can invest in life-altering technologies—and not trample on individual's rights in the process. That is especially true here, where established legal protocols for the collection and subsequent commercial use of data already exist: notice, consent, and compensation. OpenAI disregarded all three.

OpenAI gave no *notice* to the world that, for years, it was secretly harvesting from the internet everything ever created and shared online, anywhere, by hundreds of millions of Americans. That, for a decade plus, every consumer's use of the internet thus operated as a gratuitous donation to OpenAI: of our insights, talents, artwork, personally identifiable information, copyrighted works, photographs of our families and children, and all other expressions of our personhood—for products that stand to concentrate the country's wealth in even fewer corporate behemoths, displace jobs at scale, and risk the future of mission-critical industries like art, music, and journalism, while creating dangerous new industries like the high-speed spawning of child pornography. It is no wonder the public is outraged by the largest-ever theft of data—to which no one *consented*.

OpenAI chastises Plaintiffs, their counsel, and by extension all the concerned everyday citizens featured in the Complaint, for being too alarmist. OpenAI's leaders, however, have raised the exact same concerns, repeatedly. But for purposes of litigation, the story is apparently different. It's all so disingenuous. And it's also not the only sign OpenAI cares nothing about the individual victims of its theft, fraud, and privacy invasions. If it did, OpenAI would be seeking to right the wrong by offering *compensation*, as it is now doing on its nationwide post-theft tour across the boardrooms of other large and powerful companies, agreeing to pay millions of dollars for content the law required it to license in the first place.

But what of all the user-generated content at issue in this litigation? To that, OpenAI's answer is reflected in its request to this Court: dismiss the people's claims outright and "with prejudice," i.e., forever. But the law as laid out below, compels a different result. And good thing. Otherwise, large companies would continue to have a seat at OpenAI's negotiating table, due to their wealth and privilege, while the individuals who were also stolen from would not. Fair compensation in the new AI economy should not depend on status and power. After all, the act of theft was the same—and the invasion of privacy even worse. OpenAI's motion should be denied in its entirety.

II. BACKGROUND

To develop its machine learning AI products, Defendants flagrantly violated established privacy and property rights, and put the entirety of the internet community at immense risk by secretly harvesting massive amounts of users' personal information. FAC at ¶¶ 3-6. Regardless of whether Defendants started their technological venture with good intentions in the name of "progress," they have become a profit-driven technology empire with an insatiable thirst for individuals' data and a conspicuous disregard for privacy, security, and ethics. *Id.* at ¶¶ 5-6. To create their AI products, including ChatGPT-3.5, ChatGPT-4.0, Dall-E, and Vall-E, Defendants willfully pilfered the internet, stealing personal data from millions of consumers worldwide, without their knowledge or consent, and without offering anything in exchange for their valuable data. *Id.* at ¶¶ 3, 6-7, 180-81. Through its wide-scale theft, Defendants have collected sensitive medical information, confidential financial information, information from private, password protected websites, users' social media interactions, and even users' private conversations. *Id.* at ¶¶ 6, 148-49, 182-83, 152-54, 197, 210-214, 374. To make matters worse, Defendants have also integrated their AI products into hundreds of other applications and platforms, which has allowed Defendants to surreptitiously track and intercept users' personal information, browser data, log-in

data, keystrokes, cookies, analytics, and more. *Id.* at ¶¶ 16, 232-33, 310, 614-625, 623-633, 633-643.

Plaintiffs all used Defendants' AI products, which unbeknownst to them, were secretly collecting all the data they inputted. *Id.* at ¶¶ 20, 30, 41, 53, 62, 72, 82, 92, 101, 106, 115, 120, 129. Plaintiffs also each used a variety of the thousands of websites Defendants scraped without permission. *Id.* at ¶¶ 184-84 (websites Defendants scraped); *id*. at ¶¶ 21-24 (Plaintiff Cousart); *id*. at ¶¶ 31-35 (Plaintiff Guilak); *id*. at ¶¶ 42-46 (Plaintiff Martin); *id*. at ¶¶ 54-57 (Plaintiff Roberts); *id*. at ¶¶ 63-67 (Plaintiff Barcos); *id*. at ¶¶ 73-77 (Plaintiff Paz); *id*. at ¶¶ 83-87 (Plaintiff De La Torre); *id*. at ¶¶ 93-96 (Plaintiff Vassilev); *id*. at ¶¶ 102-103 (Plaintiff Johnson); *id*. at ¶¶ 107-109 (Plaintiff McNeal); *id*. at ¶¶ 116-118 (Minor Plaintiff N.B.); *id*. at ¶¶ 121-124 (Plaintiff Martinez); *id*. at ¶¶ 130-132 (Plaintiff Hagan). Further, several Plaintiffs also frequently used websites that were integrated with ChatGPT API, which tracked and intercepted their personal information. *Id.* at ¶¶ 23, 33, 43, 56, 76, 85, 96, 123, 131 (Spotify); *id.* at ¶¶ 35, 66, 124 (Microsoft Teams); *id.* at ¶¶ 35, 46 (Bing). Plaintiffs did not expect that any of the information they shared with these websites would be intercepted and compiled by a third-party looking to harvest their data and repackage it for commercial purposes. *Id.* at ¶¶ 26, 37, 49, 57, 68, 78, 89, 97, 104, 110, 118, 125, 133, 197-209, 298-301. Plaintiffs also did not consent to Defendants' extensive data collection, nor could they have, since they were unaware of Defendants' predatory conduct. *Id.* at ¶ 461.

Defendants' unjust, unfair, and unlawful collection of data allowed them to realize *billions* of dollars in value. *Id.* at ¶ 127 (OpenAI's valuation); *Id.* at ¶ 144 (OpenAI's impact on Microsoft's top line). Despite their tremendous financial success, Defendants did not pay a dime to Plaintiffs or other internet users, even though doing so would have been in line with the fair business practices of competitors, who pay for data. *Id.* at ¶¶ 414-417. Indeed, Plaintiffs allege that there

are active market exchanges where internet users can monetize their own personal data. *Id.* at ¶ 411. Defendants' law-abiding competitors' business practices demonstrate the value of personal data and prove that machine learning AI can be developed and trained in a responsible and fair way. *Id.* at ¶¶ 407-412 (the value of data); *Id.* at ¶¶ 414-416 (fair data collection practices). By stealing Plaintiffs' data, Defendants impeded Plaintiffs' right to "possess, control, use, profit, sell, and exclude others from accessing or exploiting [their] information without consent or renumeration." *Id.* at ¶ 406. They also obtained an unfair competitive advantage over good corporate citizens operating in the legitimate market for training data.

The present-day harms and imminent future risks resulting from Defendants' theft and grossly negligent business practices are as varied as they are serious. *Id.* at ¶¶ 241-249 (injection and extraction attacks); *Id.* at ¶¶ 250-274 (risks presented by attacks); *Id.* at ¶¶ 315-328 (other risks); *Id.* at ¶¶ 487-493 (risks to children). For example, due to Defendants' failure to implement adequate safeguards to protect the hordes of personal information they stole, adversaries can use machine learning cyberattacks to steal Plaintiffs' sensitive personal information. *Id.* at ¶¶ 240, 243-244. Aside from these extreme privacy concerns, OpenAI also creates the potential for a myriad of other risks, such as the creation of misinformation, deepfakes, clones, scams, blackmail, child pornography, hate and bias, hypercharged malware, and autonomous weapons, to name a few. *Id.* at ¶¶ 315-328, 329-335, 336-339. Defendants were aware of and contemplated these risks, and nonetheless proceeded with their dangerous practices and widespread commercialization—in blatant violation of their duties to Plaintiffs, the law, and society at large. *Id.* at ¶¶ 235-239, 728-730.

To this day, Defendants admit that even they do not fully understand how the Products are working or what they might evolve, on their own, to "learn" or do next. Thus, by collecting

previously obscure and personal data of millions and permanently entangling it with the Products, Defendants knowingly put Plaintiffs and the Classes in a zone of risk that is *incalculable*—but unacceptable, by any measure of responsible data protection and use.

III. ARGUMENT

A motion to dismiss must be denied if the complaint "state[s] a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* The Court must "accept factual allegations in the complex as true and construe the pleadings in the light most favorable to the nonmoving party." *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008).

A. Plaintiffs' Complaint Satisfies Rule 8

Plaintiffs' well-pled allegations are sufficient to put all defendants on notice of their potential liability for the conduct complained of in the FAC, which is "all that is required under the liberal pleading standard of Rule 8(a)." *City of Los Angeles v. Wells Fargo & Co.*, 22 F. Supp. 3d 1047, 1062 (C.D. Cal. 2014). Defendants' argument that they will be left guessing what personal information that was scraped or intercepted, when and how that was done, whether it was done with *adequate* disclosures, or any other details of the well-pled FAC falls flat.

In the opening pages of the FAC, Plaintiffs describe the types of information that Defendants—together—began to take from myriad internet sources to begin developing artificial intelligence products, including "private information and private conversations, medical data, [and] information about children—essentially every piece of data exchanged on the internet it could take[.]" FAC at ¶ 6. This data was used to train and develop Defendants' Products, which

include ChatGPT, Dall-E, and Vall-E, "to analyze and generate human-like language that can be used for a wide range of applications, including chatbots, language translation, text generation, and more" (FAC at ¶ 7) which allows Defendants' Products "to, among other things, carry on human-like conversations with users, answer questions, provide information, generate next text on demand, create art, and connect emotionally with people, all like a 'real' human." FAC at ¶ 7.

With AI gaining pace, "Defendants created and continue to create economic dependency within our society, deploying the tech directly into the hands of society and embedding it into the fundamental infrastructure as quickly as possible." FAC at ¶ 13. Without speculation, Plaintiffs then articulated *at least 16 categories of data that Defendants take*, including account information, contact details, emails, payment card data, transactional data, IP and location data, social media information, usage and analytics data, cookies (that reveal a user's internet history), keystrokes, and typed (but not executed) searches, and other detailed activity in applications. FAC at ¶ 16. This data has been scraped from the internet and intercepted and collected through the integration of AI-based APIs in third-party applications, then used for profit. FAC at ¶¶ 16, 17.

The Plaintiffs also detail their allegations not only with third-party sources confirming the data has been collected and used by Defendants, but also for the applications and websites they frequent, how Defendants' Products accessed information on those websites, which of Defendants' Products that Plaintiffs interacted with, and when. FAC at ¶¶ 19–135. Plaintiffs' FAC is not the type of complaint that courts dismiss under Rule 8 where it cites scant facts and pleads the causes of action in conclusory form. Defendants have sufficient information from the FAC to be on notice of their potential liability and participate in discovery. *City of Los Angeles*, 22 F. Supp. 3d at 1062.

B. Plaintiffs Have Adequately Alleged Violations of the ECPA

Defendants' first argument relies on the illusion of consent. In *suggesting* that third-party websites consented to Defendants' conduct, Defendants take impermissible logical leaps that any (unproven) consent was commensurate with and considered what Defendants would do with the data after receipt. But Plaintiffs detailed how the theft and use of data exceeds any reasonable consent that might have been obtained (even from websites) because the practices are so widespread and pervasive that Defendants' AI has a holistic view of consumers' internet activity. *See* FAC at ¶¶ 453–56 (the third-party disclosures do not provide informed consent); FAC at ¶¶ 457–58 (how the AI plug-ins were installed with haste collecting clicks, searches, and personal information for services wholly unrelated to AI services); FAC at ¶¶ 459–62 (how the vast types and amounts of information being collected across products and websites is unknowingly used in whole to train AI); FAC at ¶¶ 463–67 (the false notion that Plaintiffs control how their data can and cannot be used even though Defendants retain some unspecified information); FAC at ¶¶ 468–71 (how Defendants' disclosures are not conspicuous); and FAC at ¶¶ 472–86 (how Defendants' use of Plaintiffs' and consumers' data exceeds any reasonable understanding).

In passing, Defendants suggest that they can consent for each others' violations of the ECPA. Mot at 8–9. But "subsequent disclosure of the contents of the intercepted conversations for the alleged purpose of further invading the [Plaintiffs'] privacy" is a tortious act that satisfies the crime-tort exception to consent. *Planned Parenthood Fed'n of Am., Inc. v. Ctr. For Med. Progress*, 214 F. Supp. 3d 808, 828 (N.D. Cal. 2016).

Defendants also improperly liken the data they tracked and intercepted through the integration of OpenAI into third-party websites to "communications in storage." Mot. at 8. To the contrary, Defendants' API integration allowed them to track and intercept communications while

they were "in transit or passing over any wire, line, or cable, or are being sent from or received at any place." FAC at ¶¶ 574, 584, 594. Further, Plaintiffs alleged the information they entered was collected *as they entered it*. FAC at ¶ 460. *See Valenzuela v. Nationwide Mut. Ins. Co.,* No. 2:22-cv-06177-MEMF-SK, 2023 U.S. Dist LEXIS 1438232 at 15 (C.D. Cal Aug. 14, 2023) (finding plaintiffs' allegation that messages were intercepted in real time were sufficient to infer that the interception happened "in transit" and "[n]othing more than this combination of plausibility and notice is required at this stage." As such, cases affording lesser protections to information in storage are distinguishable. *United States v. Smith*, 155 F.3d 1051 (9th Cir. 1998) (holding that voicemail messages were "communications in storage"); *Konop v. Hawaiian Airlines, Inc*., 302 F.3d 868, 873 (9th Cir. 2002) (finding that that accessing an already-created website was not interception "in transmission").

Lastly, Defendants contend that Plaintiffs' ECPA fails because they do not allege that any of their personal information was intercepted through ChatGPT API[1]. Mot. at 9. First, while personal information can constitute content under ECPA, ECPA violation occurs where content of communications is intercepted. Here, Plaintiff Paz, for example, has alleged that when chatting with his friends on Snapchat, he noticed that the "MyAI" feature began generating responses, and was concerned with the chatbot reading and analyzing all of his conversations without his knowledge. FAC ¶ 75. For the chatbot to generate responses, it had to analyze Paz's intercepted communications. Defendant's argument also misleadingly speculates that since Paz alleged to have used Snapchat "recently," it is *possible* that it happened after OpenAI stopped using API data. Mot. at 10. There is no reasonable basis for this inference, especially since Plaintiffs make it clear that (a) the MyAI feature was available and generated responses, and (b) OpenAI's contention that

[1] Plaintiffs also allege that interception occurs on Microsoft Platforms and ChatGPT. ¶ 560.

it purportedly stopped spying on people through GPT API is doubtful. FAC ¶ 218. Further, several Plaintiffs allege they actively use third-party websites that have ChatGPT integrated. *Id.* at ¶¶ 23, 33, 43, 56, 76, 85, 96, 123, 131 (Plaintiffs that allege using Spotify); *id.* at ¶¶ 35, 66, 124 (Plaintiffs that allege using Microsoft Teams); *id.* at ¶¶ 35, 46 (Plaintiffs that allege using Bing). Plaintiffs alleged that each of these websites integrated ChatGPT, and as such, intercepted their personal information. *Id.* at ¶ 460 (alleging that Defendants track information from "Stripe, Microsoft Teams, Bing, Zillow, Expedia, and Instacart, etc.," all of which have ChatGPT integrated); FAC at ¶ 560 (alleging that platforms that integrated ChatGPT intercepted "chats, comments, replies, searches, keystrokes, signals, mouse clicks, or other data, activity, or intelligence"). Accordingly, Plaintiffs have adequately alleged their personal data was intercepted through ChatGPT API. *See Noel v. Hall,* 568 F.3d 743, 749 (9th Cir. 2009) (interception occurs "when the contents of a wire communication are captured or re-directed in any way").

C. Plaintiffs Have Adequately Alleged Violations of the CIPA

As discussed above, Plaintiffs sufficiently alleged that their communications were intercepted during transmission, since their information was intercepted as they entered it into the websites that had OpenAI API integrated.[2] FAC at ¶¶ 460, 574, 584, 594. Similarly, Plaintiffs alleged that several Plaintiffs used websites that had ChatGPT API integrated and their personal information was thus intercepted. FAC at ¶¶ 23, 33, 43, 56, 76, 85, 96, 123, 131 (Plaintiffs that allege using Spotify); FAC at ¶¶ 35, 66, 124 (Plaintiffs that allege using Microsoft Teams); FAC at ¶¶ 35, 46 (Plaintiffs that allege using Bing). As such, Plaintiffs' allegations under CIPA are similarly sufficient.

[2] As with ECPA, OpenAI does not address interception on Microsoft platforms or ChatGPT.

Further, Plaintiffs' FAC is anything but conclusory or vague. Mot. at 11. In *Martin v. Sephora USA, Inc.*, the court dismissed a claim under CIPA after the plaintiffs block quoted CIPA and simply stated "Defendant does all three." 2023 WL 2717636, at *5 (E.D. Cal. March 30, 2023). Here, Plaintiffs detail how Defendants have engaged in conduct proscribed by CIPA. FAC at ¶¶ 614–643. For example, Plaintiffs explain how Defendants intentionally intercepted the communications, *see*, *e.g.*, FAC at ¶¶ 614–618, 623, 624, 625, 629, 634, 635, 637; how Defendants read the contents without permission and then employed them for their own financial gain, *see*, *e.g.*, FAC at ¶¶ 619, 620, 621, 627, 628, 630, 631, 638, 639; and finally how Defendants conspired to violate CIPA. FAC at ¶ 626, 632, 635, 636, 640. These spanning paragraphs, along with the FAC taken as a whole, are not the conclusory type observed in *Martin*, easily satisfy Rule 8 pleading requirements, and the Court should summarily reject Defendants' argument.

Defendants' next argument—that Plaintiffs' activities are not confidential, relying on *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330 (N.D. Cal. Oct. 23, 2019) and *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836 (N.D. Cal. 2014)—is misguided. This Court held in *Revitch* that *certain* internet communications "do not reasonably give rise to" an "objectively reasonable expectation that the conversation is not being overheard or recorded." 2019 WL 5485330 at *3. There, consumers were shopping for retail clothing, which did not qualify as confidential. *Id.* And in *Campbell v. Facebook Inc.*, the court found that internet chats *might not* be confidential because they "can easily be shared by, for instance, the recipient(s) . . . ." 77 F. Supp. 3d at 849. However, the test for "confidential" *does not require* a showing of an "additional belief that the information would not be divulged at a later time to third parties." *Mirkarimi v. Nevada Prop. 1 LLC*, 2013 WL 3761530, at *2 (S.D. Cal. July 15, 2013). Instead, to meet that test, a plaintiff need only show

a reasonable "expectation that the conversation was not being simultaneously disseminated to an unannounced second observer" when the communication occurred. *Id.*[3]

Here, Plaintiffs allege that they visited objectively sensitive and confidential websites, including those that include financial, private health information, and others that are password protected.[4] *See* FAC ¶¶ 197–216; *Flanagan*, 27 Cal. 4th 776; *Mirkarimi*, 2013 WL 3761530, at *2. These are not the kind of communications at issue in *Revitch* or *Campbell*, but more analogous to those in more recent privacy litigation that has recognized the confidential nature of online communications. *See, e.g.*, *Doe v. FullStory, Inc.*, --- F. Supp. 3d ---, 2024 WL 188101 at *8–9 (N.D. Cal. Jan. 17, 2024) (denying motion to dismiss, finding that plaintiff's sufficiently pleaded medical information was confidential under 632(a)); *Yockey v. Salesforce, Inc.*, --- F. Supp. 3d ---, 2023 WL 5519323, *6–7 (N.D. Cal. Aug. 25, 2023) (same); *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1073–74 (N.D. Cal. 2021) (denying motion to dismiss 632(a) claim where plaintiffs alleged a reasonable expectation where internet browsing involved more intimate and private browsing and distinguishing some cases involving internet chats).[5]

Finally, Defendants' suggestion that Plaintiffs have not alleged injury is wrong. Mot. at 11. Defendants rely on one case, *Graham v. Noom, Inc.*, 2021 WL 3602215, at *1 (N.D. Cal. Aug. 13, 2021), where that court had previously found where there was no wiretapping, there was no injury

[3] *See also Kight v. CashCall, Inc.*, 200 Cal. App. 4th 1377, 1397 (2011) ("that plaintiffs may have known the information discussed in their phone calls would be disclosed to other [of defendant's] employees does not mean the plaintiffs had no reasonable expectation that their telephone conversation[s] were not being secretly overheard.").

[4] Defendants suggest that some websites listed "have extensively publicly-available content that can be accessed without an account." Mot. at 12, fn. 14. This argument belies the well-pleaded factual allegations of the CAC, where even those websites (e.g., Facebook, Instagram, and Walmart) and others have information behind password-protected private ecosystems.

[5] *See also Brown v. Google LLC*, --- F. Supp. 3d ---, 2023 WL 5029899, at *16–17 (N.D. Cal. Aug. 7, 2023) (denying summary judgment and finding triable issue of fact on same).

under CIPA. *Id.* For the reasons stated throughout the FAC and Plaintiffs' responses to the motions to dismiss, that simply is not the case, and Defendants' superficial argument should be denied.

D. Plaintiffs Have Adequately Alleged Violations of the CDAFA

Defendants' first line of attack is wrong: the CDAFA has no requirement that a defendant access a plaintiff's computer. *See* Cal. Penal Code § 502(c)(2) (proscribing unpermitted taking, copying, or use "of any data . . . , whether existing or residing internal or external to a computer."); § 502(b)(8) (defining "data" to include data "in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device").

Instead, the CDAFA imposes civil liability for anyone who "[k]knowingly access[es] and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network." Cal. Penal Code § 502(c)(2). Plaintiffs detail in their FAC how they are the owners of Private Information and how Defendants unlawfully collected that data. FAC at ¶¶ 197–216, 602, 606. For example, Plaintiff Cousart alleges that Defendants illegally accessed pictures of her family stored in DropBox—which she "expected would only be accessed by a restricted audience" and "did not consent" to Defendants' access. FAC at ¶¶ 25, 197, 198. The same is true for all Plaintiffs. *See*, *e.g.*, FAC at ¶¶ 197–216. As the Ninth Circuit has held, "access" under the CDAFA includes "logging into a database with a valid password and subsequently taking, copying, or using the information in the database improperly." *United States v. Christensen*, 828 F. 3d 763, 789 (9th Cir. 2015). That Plaintiffs' data may have been shared for one purpose does not absolve Defendants of liability where the information has been taken and used improperly. *Id.*

Courts in this District have found that plaintiffs state a claim under the CDAFA where "'hidden' software that transmitted data without notice and without providing an opportunity to opt out of its functionality." *Brown*, 525 F. Supp. 3d at 1075 (citing *In re Carrier IQ*, 78 F. Supp.

3d 1051, 1101 (N.D. Cal. 2015)). In *Brown* the court found that software accessing consumers' data without permission violated the CDAFA because that software "would render ineffective any barrier Plaintiffs wished to use to prevent the transmission of their data." *Id.*

Defendants' argument concerning "damage or loss" is equally unavailing. Mot. at 12. Defendants' scant reliance on *Cottle v. Plaid Inc.* falls flat,[6] where the CDAFA claim failed because it was premised on a "lost value of their indemnification rights." 536 F. Supp. 3d 461, 487–88 (N.D. Cal. 2021). And while the *Cottle* court held that plaintiffs fell short of supporting their lost value theories under the CDAFA, *id.* at 488, here Plaintiffs have demonstrated that their Private Information has value. *See*, *e.g.*, FAC at ¶¶ 408–416 (demonstrating that a market exists where companies compensate individuals for access to their information). The Ninth Circuit has affirmed such a valuation. *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 600 (9th Cir. 2020) (finding that plaintiffs sufficiently alleged their browsing histories carried financial value). The court in *Brown v. Google LLC* similarly followed that logic in not only denying Google's motion to dismiss, but also a motion for summary judgment on this precise point. 2023 WL 5029899, at *19 (recognizing that "plaintiffs can state an economic injury for their misappropriated data" which precludes a finding "as a matter of law that plaintiffs suffered no damages under CDAFA.").

E. Plaintiffs Have Adequately Alleged Violations of the UCL

A UCL claim arises out of "any unlawful, unfair or fraudulent business act or practices." Cal. Bus. & Prof. Code § 17200. Plaintiffs have standing to seek redress under the UCL by way of Defendants' improper data interception, collection, and use. While satisfying only one prong

[6] Defendants also cite *Pratt v. Higgins*, 2023 WL 4564551 (N.D. Cal. July 17, 2023), which relied on *Cottle*. Because Defendants' reliance on *Cottle* fails, so too does *Pratt*.

under the UCL is necessary, Plaintiffs state a claim under both the unlawful and unfair prongs of the UCL. FAC at ¶¶ 647–672 (unlawful) and 673–713 (unfair).[7]

1. Plaintiffs have standing under the UCL and sufficiently plead an entitlement to restitution.

Defendants' suggestion that Plaintiffs lack standing under the UCL comes from a line of cases that predate courts' recognition that markets exist for data, or cases where the plaintiffs had not demonstrated a market for the data at issue. Mot. at 13; *cf.* FAC at ¶¶ 408–416 (demonstrating that a market exists where companies compensate individuals for access to their information). There are "innumerable ways in which economic injury from unfair competition may be shown." *Kwikset Corp. v. Superior Court*, 51 Cal.4th 310, 324 (2011). This can include "plaintiffs who [have] suffered a loss of their personal information." *Calhoun v. Google LLC*, 2021 WL 1056532, at *22 (N.D. Cal. March 17, 2021) (citing *In re Facebook Privacy Litig.*, 572 F. App'x 494, 494 (9th Cir. 2014) (harm plausibly alleged when plaintiff's personal information was disclosed in a data breach); *In re Marriott Int'l, Inc., Cust. Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 461 (D. Md. 2020 (recognizing "the growing trend across courts that have considered this issue is to recognize the lost property value of [personal] information"); *In re Yahoo! Inc. Cust. Data Sec. Breach Litig.*, 2017 WL 3727318, at *13 (N.D. Cal. Aug. 30, 2017) (same); *In re Anthem Inc. Data Breach Litig.*, 2016 WL 3029783, at *14 (N.D. Cal. May 17, 2016) (same)). Plaintiffs here have not only demonstrated there is a market for their data (FAC at ¶¶ 408–416) but also that Defendants themselves collect that data for their own enrichment. *Id*. This falls in line with recent decisions holding that plaintiffs have standing under the UCL where their data is taken and used for profit

[7] Defendants devote substantial argument to the "fraudulent" prong under the UCL. Mot. at 15–16. Plaintiffs' CAC clearly ***does not sound under the fraudulent prong***. Because Plaintiffs' UCL claims do not sound in fraud, there is no requirement to allege reliance. *See Jerome's Furniture Warehouse v. Ashley Furniture Indus., Inc.*, 2021 WL 148063, at *4 (S.D. Cal. Jan. 15, 2021).

without their permission. *See*, *e.g.*, *Brown*, 2023 WL 5029899 at *21 (denying summary judgment on similar argument, finding that "sufficient evidence exists that plaintiffs have suffered an injury in fact" after demonstrating that a market exists and surreptitious collection and subsequent use inhibited ability to participate in market and that California's Consumer Privacy Act conveys "an unopposed property interest" in their data); *see*, *e.g.*, FAC at ¶¶ 314, 364, 649–662 (explaining how consumers cannot "take back" their information once the AI has been trained on it).

Plaintiffs also plead and are entitled to *both* restitution and injunctive relief. Defendants' interception, collection, and use of Plaintiffs' data resulted in profits. *See*, *e.g.*, FAC at ¶¶ 151–170, 681, 684, 687, 689, 693, 702. The restitution that Plaintiffs seek would redress Defendants' improper interception, collection, and use of Plaintiffs' data. *See*, *e.g.*, FAC at ¶¶ 649–662; *Calhoun*, 2021 WL 1056532, at *22. An injunction would focus on prospective relief to cease that conduct and ensure that Plaintiffs and Class members alike have control over their data. These different types of relief are not at odds. *Brown*, 2023 WL 5029899 at 17.

2. Plaintiffs state a claim for unlawful business practices under the UCL.

As an initial matter, for the reasons stated in this opposition, Plaintiffs have stated their claims that serve as the "derivative UCL claim." Mot. at 14. Also, contrary to Defendants' contentions, a CCPA violation is available under the unlawful prong of the UCL. *See, e.g.*, *Mehta v. Robinhood Financial LLC*, 2021 WL 6882377, *12 (N.D. Cal. May 6, 2021).

3. Plaintiffs state a claim for unfair violations under the UCL.

A UCL violation for unfair conduct occurs when a practice "offends an established public policy or substantially injurious to consumers." *Hodsdon v. Mars, Inc.*, 891 F.3d 857, 866 (9th Cir. 2018). Some courts apply a balancing test that weighs the utility of the defendant's conduct against the gravity of the harm. *See*, *e.g.*, *Davis v. HSBC Bank Nevada, N.A.*, 691 F.3d 1152, 1169 (9th Cir. 2012). Others require that unfairness "be tethered to some legislatively declared policy or

proof of some actual or threatened impact on competition." *In re Anthem Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 989 (N.D. Cal. 2016) (quoting *Lozano v. AT&T Wireless Servs., Inc.*, 504 F.3d 718, 735 (9th Cir. 2007)). Regardless of the test, Plaintiffs satisfy their pleading burden.

First, Plaintiffs allege how Defendants' conduct was injurious. FAC at ¶¶ 314, 364, 649–662. Second, Plaintiffs also allege the gravity and permanence of the harm they suffered as a result of Defendants' conduct. FAC at ¶¶ 314, 364, 649–662. These harms are directly related to the established California public policy of maintaining ownership and control over Private Information, and Plaintiffs' UCL claim should proceed.

F. Plaintiffs Have Adequately Alleged Violations of BIPA[8]

1. Choice of Law.

Defendants chiefly premise their argument on accepting the relevant terms of service. Mot. at 17. Therefore, any members of the nonuser subclass (FAC at ¶ 525) or those in the biometric subclass who did not agree to the relevant terms of service (FAC at ¶ 525) would necessarily be exempted from Defendants' challenge based on choice of law. Mot. at 17.

Even if the terms of service have an enforceable choice-of-law provision, Defendants' arguments still fail. First, Defendants' arguments that Plaintiff Roberts accepted the choice-of-law provision (Mot. at 17) belies the preceding paragraphs that specifically state the choice-of-law provision extends to *non-statutory claims*. FAC at p. 154, ¶ 541.

Defendants' same argument—that California's passage of the CCPA, CPRA, and other statutory framework "offer robust biometric privacy protections, such that California law controls Roberts' claim" (Mot. at 18–19)—has been addressed and roundly rejected. In *Delgado v. Meta Platforms, Inc.*, Meta (f/k/a Facebook) advanced this exact argument, citing much of the same

[8] Plaintiffs have reviewed the law and decisions under Illinois' ICFA and IUDTPA and agree to pursue those claims under the California statutory laws and framework alleged in their CAC.

cases that Defendants rely on here. 2024 WL 818344, *2 (N.D. Cal. Feb. 27, 2024). In *Delgado*, the court found (and the plaintiff "did not seriously dispute") that California has a substantial relationship to the parties or their transaction where a plaintiff executes terms of service with a technology company headquartered in California. *Id.* at *2. The court accordingly turned to the second prong of a choice-of-law analysis: "whether California's law is contrary to a fundamental policy of Illinois law and, if so, whether Illinois has a materially greater interest than California in the determination of the particular issue." *Id.* at *2.

The *Delgado* court recognized that this analysis had previously been undertaken in "and determined that '[t]he answer to both questions is yes.'" *Id.* (citing *In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155, 1169 (N.D. Cal. 2016) ("*In re Facebook Biometrics*.")). And although *In re Facebook Biometrics* predates the CCPA, CPRA, and other California statutes, the *Delgado* court conducted a detailed analysis to conclude that a California choice-of-law provision does not extinguish a BIPA cause of action because: (1) Illinois has a substantial policy of protecting its citizens' right of privacy in their personal biometric data; (2) BIPA provides protections that the CCPA does not, including no application to Illinois residents, and BIPA has a private right of action while the CCPA vests sole authority for enforcement by the California Attorney General (except in the event of a security breach). *Id.* at *4–5 (citing cases).

Like in *Delgado*, Defendants' cases generally focus on consumer protection laws and not specifically BIPA. Mot. at 18 (collecting cases). None of those cases implore disagreement with *Delgado*, and the decision most analogous to the facts present in this case is inapplicable. Mot. at 19. In *Thakkar v. ProctorU Inc.*, an Alabama district court held that a BIPA claim could not survive an Alabama choice-of-law analysis. 642 F. Supp. 3d 1304, 1311 (N.D. Ala. 2022). Crucially, Alabama's conflict-of-law rules require application of Alabama law unless application of Alabama

law would violate *Alabama's* public policy. *Id.* Unlike Alabama, California's analysis focuses on *inter alia* whether application of California law is contrary the public policy of Illinois. *Delgado*, 2024 WL 818344 at *2. Thus, *Thakkar* has no application to the facts here.

Plaintiffs respectfully submit that the Court should adopt the *Delgado* analysis. Should the Court find that a more robust choice-of-law analysis should take place, Plaintiffs respectfully request additional briefing to demonstrate that Illinois applies to Roberts' statutory claims.

2. Extraterritoriality.

Whether Defendants' conduct is covered by Illinois law begins with the Illinois Supreme Court's analysis in *Avery v. State Farm Mut. Auto Ins. Co.*, to determine whether the conduct occurred "primarily and substantially" in Illinois. 216 Ill.2d 100, 835 N.E.2d 801, 854 (Ill. 2005). Courts in this District have undertaken exactly that analysis to conclude that BIPA has extraterritorial applicability. In *Colombo v. YouTube, LLC*, the court rejected the same argument for a BIPA claim where provision of access to defendant's products and services to Illinois users constituted in-state activity, despite defendant's headquarters, servers, and other activities being outside Illinois. 2023 WL 4240226 at *4 (N.D. Cal. 2023). Also, in another decision from *In re Facebook Biometric*, the court rejected similar arguments, holding that foreclosing extraterritorial application of BIPA would "effectively gut the ability of states without server sites to apply their consumer protection laws to residents for online activity that occurred substantially within their borders." 326 F.R.D. 535, 548 (N.D. Cal. April 16, 2018).

The cases that Defendants rely on are easily distinguishable. In *McGoveran v. Amazon Web Servs., Inc.*, the conduct at issue had no relationship with Illinois because plaintiffs "dialing of the phone" in Illinois was an insufficient nexus, and there was no proof that defendants even knew the calls actually came from Illinois. 2021 WL 4502089 (D. Del. Sept. 30, 2021). That is simply not

the case here, where Defendants collected *inter alia* geolocation data, IP addresses, and other data that clearly demonstrates that Plaintiffs' activities occurred in Illinois *and that Defendants knowingly collected data from Illinois*. FAC at ¶ 16; *cf McGoveran*, 2021 WL 4502089 at *5 (recognizing that courts "have been hesitant to grant motions to dismiss BIPA claims based on extraterritoriality") (collecting cases); *see also id.* (distinguishing that "Plaintiffs do not allege any direct interaction with [defendants] that might plausibly be imputed to Illinois . . . only [direct] interactions with [a defendant] in Massachusetts, who in turn interacted with Defendants.").

Archey v. Osmose Utility Services, Inc. fares no better. In *Archey*, an Illinois resident interviewed with a Georgia corporation, and while the interview took place in Illinois, there was no evidence that the data provided to the defendant was provided when the plaintiff was located in the state of Illinois. 2022 WL 3543469, *5 (N.D. Ill. Aug. 18, 2020) ("Nor does Archey allege that Osmose asked for, or that he provided his personal information to Osmose in Illinois"). Indeed, the *Archey* court even acknowledged that the plaintiff failed to address that argument. *Id.* Finally, in *International Equipment Trading, Ltd. v. Illumina, Inc.*, the tortious conduct complained of resulted in an alleged lost sale in Florida. 312 F. Supp. 3d 725, 733 (N.D. Ill. 2018).

These cases are different at the core compared with the conduct here, where Defendants knowingly collected data from Illinois. *See*, *e.g.*, FAC at ¶ 16 (geolocation data and IP address); *In re Facebook Biometrics*, 326 F.R.D. at 548; *Colombo*, 2023 WL 4240226 at *1.

3. Plaintiff Roberts States a Cause of Action under BIPA.

Defendants first challenge to Plaintiff Roberts' BIPA claim is that there are no allegations that Defendants possess biometric data. Mot. at 20. This is a misreading of both the FAC and the cases that Defendants rely on to form their flawed argument.

The FAC clearly details Plaintiff Roberts' allegations concerning the specific photographs and other data that Defendants took, and how that data is used in AI models (including Defendants' DALL-E product) to refine AI-generated images. FAC at ¶¶ 3, 16, 52–60, 154, 175, 201, 236, 325, 429, 716. This includes Plaintiff Roberts' face and voice scraped from third-party websites and social media platforms like Facebook, Instagram, and TikTok, which were subsequently ingested into Defendants' AI Products that generate, *inter alia*, images. FAC at ¶¶ 54–56.

The cases that Defendants rely on are inapposite. Mot. at 21. In *Barnett v. Apple, Inc.*, the allegation was that biometric data may have only existed on a smartphone that the plaintiff used, but there was no allegation that Apple possessed that data. 225 N.E.3d 602, 610 (Ill. Ct. App. 2022). The *Barnett* court required more than Apple's development of the software existing on phone; Apple needed to actually possess (rather than store on a phone locally) the data at issue. *Stauffer v. Innovative Heights Fairview Heights, LLC*, dismissed a claim under BIPA because there was no "active step" to use (*i.e.*, access) the fingerprint data after the defendant stored it. 2022 WL 3139507 (S.D. Ill. Aug. 5, 2022). In both *Jones v. Microsoft Corporation*, 649 F. Supp. 3d 679 (N.D. Ill. 2023) and *Carpenter v. McDonald's Corporation*, 580 F. Supp. 3d 512 (N.D. Ill. 2022), unlike here, the plaintiffs failed to provide any allegations of what or how data was misused.

Defendants' second challenge to Plaintiff Roberts' BIPA claim is that the data that Defendants collected is not actually biometric data under BIPA. This argument likewise fails because Defendants have scanned the aforementioned faces and voices which, married together with the other categories of data would allow Defendants to identify Plaintiff Roberts and other Illinois residents. *See, e.g.*, *Daichendt v. CVS Pharmacy, Inc.*, 2023 WL 3559669, at *1 (N.D. Ill. May 4, 2023 ("*Daichendt II*") (holding that plaintiffs "plausibly alleged that defendant collected and stored their personal contact data ('real-world identifying information'), such as their names

and email addresses, which made [CVS] *capable* of identifying them *when associated with* scans of their face geometry ('biometric identifiers."). Like in *Daichendt II*, where eyes, smiles, and other features were scanned, "the relevant inquiry is whether defendant's collected data makes defendant *capable of* identifying plaintiffs." *Id.* Because that data was associated with other information that made CVS capable of identifying individuals, dismissal was denied. *Id.*

Here, Defendants scanned faces and voices from social media and other websites that contained Plaintiff Roberts' audio and visual data. FAC at ¶ 3, 16, 52–60, 154, 175, 201, 236, 325, 429, 716. That data is also associated with location, account information, contact details, browsing history, and other data that can easily identify an individual. FAC at ¶ 16.

Finally, courts do not require plaintiffs at the pleading stage "to plead technical details about [a] defendant's device or software." *Daichendt II*, 2023 WL 3559669, at *2 (citing *Pruitt v. Par-A-Dice Hotel Casino*, 2020 WL 5118035 (C.D. Ill. Aug. 31, 2020) and *Kukovec v. Estee Lauder Cos., Inc.*, 2022 WL 16744196 (N.D. Ill. Nov. 7, 2022)). Defendants' reliance on *Clarke v. Aveda Corporation* (Mot. at 22) is distinguishable from *Daichendt II*, *Pruitt*, and *Kukovec* because there were no plausible "allegations that Aveda was capable of identifying individuals" who used the product. --- F. Supp. 3d. ---, 2023 WL 9119927, at *2 (N.D. Ill. Dec. 1, 2023). The *Clarke* court explicitly recognized a factually-different case that would compel denial of dismissal. *Id.* at *3, FN2. Specifically, in *Melzer v. Johnson & Johnson Consumer Inc.*, the court denied a motion to dismiss where the scanned data was "tied to individuals' names, birthdates, and other personally identifying information." 2023 WL 3098633, *1 (D.N.J. Apr. 26, 2023).

Plaintiff Roberts has alleged that relationship here (FAC at ¶¶ 3, 16, 52–60, 154, 175, 201, 236, 325, 429, 716) and the Court should accordingly deny Defendants' challenge to BIPA.

G. Plaintiffs Have Adequately Alleged Their Negligence Claim

"To state a claim for negligence in California, a plaintiff must establish the following elements: (1) the defendant had a duty, or an 'obligation to conform to a certain standard of conduct for the protection of others against unreasonable risks,' (2) the defendant breached that duty, (3) that breach proximately caused the plaintiff's injuries, and (4) damages." *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1038–39 (N.D. Cal. 2019) (quoting *Corales v. Bennett*, 567 F.3d 554, 572 (9th Cir. 2009)).

1. Defendant owed a duty to Plaintiffs and Class Members.

Defendants first contend that Plaintiffs have not adequately alleged that OpenAI owed them a duty of care. This argument is unavailing.

"Under California law, each person has a general duty 'to exercise, in his or her activities, reasonable care for the safety of others.'" *In re Accellion, Inc. Data Breach Litig.*, 2024 WL 333893, at *3 (N.D. Cal. Jan. 29, 2024) (quoting *Brown v. USA Taekwondo ("USAT")*, 11 Cal. 5th 204, 214 (Cal. 2021), *reh'g denied* (May 12, 2021)); Cal. Civ. Code § 1714(a)). Despite this, the law recognizes that there is "no duty to control the conduct of another, nor to warn those endangered by such conduct." *Id.* (quoting *Regents of Univ. of California v. Superior Ct.*, 4 Cal. 5th 607, 619 (Cal. 2018)). However, the "no-duty-to-protect rule is not absolute.... In a case involving harm caused by a third party, a person may have an affirmative duty to protect the victim of another's harm if that person is in what the law calls a 'special relationship' with either the victim or the person who created the harm." *Id.* (quoting *USA Taekwondo*, 11 Cal. 5th at 215).

The California Supreme Court has set forth a two-step inquiry in determining whether to recognize a duty to protect: "First, the court must determine whether there exists a special relationship between the parties or some other set of circumstances giving rise to an affirmative

duty to protect. Second, if so, the court must consult the factors described in *Rowland* to determine whether relevant policy considerations counsel limiting that duty." *USAT*, 11 Cal. 5th at 209 (citing *Rowland v. Christian*, 69 Cal. 2d 108, 113 (Cal. 1968)).

As Judge Davila noted, California courts have routinely found that a "special relationship" exists "between data companies and the owners of the data." *In re Accellion, Inc. Data Breach Litig.*, 2024 WL 333893, at *5 (N.D. Cal. Jan. 29, 2024). "Specifically, there is abundant authority that California law recognizes a duty on companies to take reasonable steps to protect all sensitive information it obtains from individuals." *Id.* (citing *Stasi v. Inmediata Health Grp. Corp.*, 501 F. Supp. 3d 898, 915 (S.D. Cal. 2020); *Castillo v. Seagate Tech., LLC*, 2016 WL 9280242, at *3 (N.D. Cal. Sept. 14, 2016); *In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 799 (N.D. Cal. 2019); *Bass*, 394 F. Supp. 3d at 1039). Importantly, "federal courts applying California law have not hesitated to extend a data company's duty of care beyond those with whom it shares privity or exceeds some threshold level of interactions." *Id.* (citing *Stasi*, 501 F. Supp. 3d at 915; *Castillo*, 2016 WL 9280242, at *3).[9]

Here, Plaintiffs have alleged that they are all users of ChatGPT and that OpenAI harvested the sensitive information it acquired through their interactions with Defendants' products. *See* FAC ¶¶ 20, 30, 41, 53, 62, 72, 82, 92, 101, 106, 115, 120, 129, 453, 456, 460. Defendants also secretly harvested massive amounts of personal data from the internet, including private information and private conversation, medical data and other data – all without notice or consent of the affected individuals. *Id.* ¶ 6. Plaintiffs thus allege that Defendants owed a duty to exercise care in collecting,

[9] Nevertheless, it should be noted that while Defendants deny any duty in negligence to Plaintiffs on the basis that it has no preexisting relationship with Plaintiffs, in the section of their brief addressing Plaintiffs' unjust enrichment claim, Defendants note that "the parties have an enforceable agreement" that "encompass[es] OpenAI's collection, storage, use, and sharing of individuals' data." ECF 50 at 33 (citing CAC ¶¶ 218, 476).

storing, and safeguarding their private information, instead of misusing such data to power Defendant's AI products. *Id.* ¶¶ 728-30. As illustrated by Judge Davila's analysis in *Accellion*, OpenAI's collection of its users' data and sensitive information is sufficient to establish a special relationship between Plaintiffs and Defendant and, thus, a duty to protect that information. 2024 WL 333893 at *5.

The second prong of the "duty to protect" inquiry is whether any of the *Rowland* factors would limit the duty Defendant owed on account of its special relationship with its users. The *Rowland* factors include: "the foreseeability of harm to the plaintiff, the degree of certainty that the plaintiff suffered injury, the closeness of the connection between the defendant's conduct and the injury suffered, the moral blame attached to the defendant's conduct, the policy of preventing future harm, the extent of the burden to the defendant and consequences to the community of imposing a duty to exercise care with resulting liability for breach, and the availability, cost, and prevalence of insurance for the risk involved." 69 Cal. 2d at 113. Again, as Judge Davila recognized in *Accellion*, "courts analyzing duties to protect data under *Rowland* have typically found that, '[f]rom a policy standpoint, to hold that [the company] has no duty of care here 'would create perverse incentives for businesses who profit off the use of consumers' personal data to turn a blind eye and ignore known security risks.'" 2024 WL 333893 at *6 (quoting *Bass*, 394 F. Supp. 3d at 1039). Thus, based on the "overall weight of *Rowland* analyses in data protection cases … the *Rowland* factors do not warrant any further limitation of the duty imposed by the 'special relationship' found above." *Id.* The *Rowland* factors definitely do not warrant any limitation on the duty of the "special relationship" in this case, especially in light of the Complaint's extensive recitation of the moral quandaries associated with Defendants' products, the risk of future harm to

users, and the consequences of a failure to put any checks on the behavior of corporate actors like Defendants.

Accordingly, Plaintiffs have properly alleged a duty of care in this case.

2. Plaintiffs have pleaded cognizable damages.

Defendants next argue that Plaintiffs have not alleged damages as a result of the breach. Defendants begin their argument by stating Plaintiffs allege only "unspecified damages." ECF 50 at 26. A mere paragraph later, however, Defendants acknowledge that the FAC does specify what damages they have suffered, including loss of value, loss of control over their sensitive personal information, and emotional distress. *Id.* at 26-27. They contend that these are not cognizable damages in this case, but they are wrong.

Defendants contend that Plaintiffs' loss of value theory is barred by the economic loss rule. But, as Defendants note, there are several exceptions that make the economic loss rule inapplicable to negligence claims, including when "a special relationship exist[s] between the parties." *Id.* at 26. As set forth above, a special relationship exists between Defendants and Plaintiffs. Accordingly, the economic loss rule does not bar Plaintiffs' claims for loss of the value of their private information. *See Accellion*, 2024 WL 333893 at *8 (N.D. Cal. Jan. 29, 2024); *Huynh v. Quora, Inc.*, 508 F. Supp. 3d 633, 654 (N.D. Cal. 2020); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 313 F. Supp. 3d 1113, 1132 (N.D. Cal. 2018) (economic loss rule did not bar plaintiffs' negligence claim for breach of duty to protect their PII).

Moreover, courts have recognized that damages for loss of control of private information are cognizable and not barred by the economic loss rule in data privacy cases. *See Accellion*, 2024 WL 333893 at *8; *Brooks v. Thomson Reuters Corp.*, 2023 WL 9316647, at *5 (N.D. Cal. Aug. 10, 2023) ("As a matter of state law, the California Supreme Court has also recognized the

tremendous harm that can result from a loss of control over one's personal information."); *Mehta v. Robinhood Fin. LLC*, 2021 WL 6882377, at *6 (N.D. Cal. May 6, 2021).

H. Plaintiffs Have Properly Alleged Invasion of Privacy

In considering whether a plaintiff has stated a claim for invasion of privacy under California law, courts consider "whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive." *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020). Both requirements are met here.

"To meet the first element, the plaintiff must have had an 'objectively reasonable expectation of seclusion or solitude in the place, conversation, or data source.'" *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1076 (N.D. Cal. 2021) (quoting *Shulman v. Group W. Prods., Inc.*, 18 Cal. 4th 200, 231 (Cal. 1998)). "[T]he relevant question here is whether a user would reasonably expect that [Defendants] would have access to the ... data." *Id.* (quoting *Facebook Tracking*, 956 F.3d at 602).

Defendants argue that Plaintiffs did not have a reasonable expectation of privacy because the information allegedly misappropriated by OpenAI was voluntarily posted by Plaintiffs on public websites. This argument misses the mark and fails to appreciate the scope of Defendants' surreptitious taking of massive amounts of personal data, including *private* information, *private* conversations, *medical data,* and even information about children from private websites with password protection and restricted access. In *Facebook Tracking*, the plaintiffs, who were Facebook users, alleged that Facebook improperly used plug-ins on third-party websites to track logged-out Facebook users' browsing histories when they visited third-party websites and then, unbeknownst to the users, compiled their browsing histories into personal profiles that Facebook sold to advertisers to generate revenue. The Ninth Circuit was called to consider whether the

plaintiffs had adequately pleaded that they had a reasonable expectation of privacy. 956 F.3d at 602. The fact that the plaintiffs voluntarily visited third-party websites and potentially posted information on those websites did not foreclose their claims against Facebook. The Ninth Circuit explained that "the relevant question here is whether a user would reasonably expect that Facebook would have access to the user's individual data after the user logged out of the application." *Id.* Similarly, here, the relevant question is whether users would reasonably expect that by using the internet daily in communicating with friends, family, or colleagues, or seeking or reaching advice from others, that they were giving Defendants unfettered permission to scrape their entire internet use and browsing histories to power yet-to-be-created AI products capable of permanently altering society in profound ways. No user could have even imagined—decades after integrating the Internet in every daily activity—that their information would be used to develop such AI products.

In *Facebook Tracking*, the Ninth Circuit concluded the plaintiffs had adequately pleaded that they had a reasonable expectation of privacy based on the amount of the data collected, the sensitivity of the data collected, the nature of the data collection, and Facebook's representations to users about their privacy. 956 F.3d at 602-03. With regard to the first three factors, the Ninth Circuit found "the amount of data allegedly collected was significant[;]" the plaintiffs alleged that "Facebook obtained a comprehensive browsing history of an individual" and "then correlated that history with the time of day and other user actions on the websites visited," resulting in "an enormous amount of individualized data." *Id.* at 603. The court also found relevant that some of the alleged data collected was sensitive, such as information about a user's visits to sensitive websites. *Id.* Finally, the court found it significant "[t]hat this amount of information can be easily collected without user knowledge." *Id.* The Ninth Circuit also considered the fact that Facebook's

representations to its users failed to acknowledge its tracking of logged-out users and would not have given users reason to suspect that any such activity might be taking place. *Id.*

Other courts have reached similar conclusions where defendants have surreptitiously gathered vast amounts of information about their users. *See In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 934 F.3d 316, 325 (3rd Cir. 2019) ("In an era when millions of Americans conduct their affairs increasingly through electronic devices, the assertion ... that federal courts are powerless to provide a remedy when an internet company surreptitiously collects private data ... is untenable."); *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 151 (3d Cir. 2015) (finding plaintiffs had a reasonable expectation of privacy under California law based on "how Google accomplished its tracking," which involved "overriding the plaintiffs' cookie blockers, while concurrently announcing in its Privacy Policy that internet users could 'reset your browser to refuse all cookies.'"); *In re Nickelodeon Cons. Priv. Litig.*, 827 F.3d 262, 293–94 (3d Cir. 2016) (holding, under analogous New Jersey law, that a reasonable expectation of privacy existed when Nickelodeon promised users that it would not collect information from website users, but then did); *Brown*, 525 F. Supp. 3d at 1076–77 ("[L]ike in *Facebook Tracking*, Plaintiffs allege that a vast amount of data was collected secretly, without any notice to users.).

Here, the Court should employ the same analysis used by the Ninth Circuit in *Facebook Tracking* to find that Plaintiffs have demonstrated a reasonable expectation of privacy. As set forth in the FAC, Defendants collected vast amounts of information on its users, including nearly their entire digital and online footprints. A lot of this information was incredibly sensitive, including information about their dating and romantic lives, their political and religious affiliations, online chats with other individuals, and websites they visited. And Defendants collected this information

surreptitiously, without giving users any notice that this practice was occurring or providing them the opportunity to withhold their consent. Based on "[t]he amount of data collected, the sensitivity of the data collected, and the nature of the data collection … Plaintiffs had a reasonable expectation of privacy." *Brown*, 525 F. Supp. 3d at 1077.

Furthermore, the intrusion was highly offensive. "While analysis of a reasonable expectation of privacy primarily focuses on the nature of the intrusion, the highly offensive analysis focuses on the degree to which the intrusion is unacceptable as a matter of public policy." *Id.* at 1079 (quoting *Facebook Tracking*, 956 F.3d at 606). In *Facebook Tracking*, the Ninth Circuit held that "[t]he ultimate question of whether Facebook's tracking and collection practices could highly offend a reasonable individual is an issue that cannot be resolved at the pleading stage." *Id.* In concluding that the plaintiffs' allegations of surreptitious data collection were sufficient to survive the motion to dismiss on the issue of whether the intrusion was highly offensive, the Ninth Circuit emphasized that "Plaintiffs have alleged that internal Facebook communications reveal that the company's own officials recognized these practices as a problematic privacy issue." 956 F.3d at 606.

Similarly, here, the FAC is rife with allegations of the fears and concerns numerous individuals and organizations had about Defendants' data scraping practices, to the extent that AI researchers have written papers and published them in hope of warning Defendants about the risks posed by its products. *See*, *e.g.*, FAC ¶¶ 9, 159, 182-85, 188, 259, 270, 282-84, 290-94, 442. And, significantly, individuals directly associated with the development of Defendants' products have voiced their fears about the existential threat posed by the products, Defendants' inability to understand the full scope of the risks posed by their products, and Defendants' failure to fully consider the ramifications of the impact the products will have. *Id.* ¶¶ 11, 14, 157, 160-65. Even

the Federal Trade Commission has recognized the risks of Defendants' technology to consumers and launched an investigation into their deceptive privacy and data security practices. *Id.* ¶ 262, 287-88. These facts are sufficient at this stage to provide a basis from which a factfinder could find that Defendants' invasion of Plaintiffs' privacy was highly offensive. *Brown*, 525 F. Supp. 3d at 1079–80. To the extent Defendants argue otherwise, those factual and legal issues cannot be resolved at this early stage of the litigation.

I. Plaintiffs Have Sufficiently Stated Their Claim for Conversion.

California law defines conversion as "any act of dominion wrongfully asserted over another's personal property in denial of or inconsistent with his rights therein." *In re Bailey*, 197 F.3d 997, 1000 (9th Cir.1999). To establish conversion, a plaintiff must show "ownership or right to possession of property, wrongful disposition of the property right[,] and damages." *G.S. Rasmussen & Assocs., Inc. v. Kalitta Flying Serv., Inc.*, 958 F.2d 896, 906 (9th Cir.1992). "Property is a broad concept that includes 'every intangible benefit and prerogative susceptible of possession or disposition.'" *Kremen v. Cohen*, 337 F.3d 1024, 1030 (9th Cir. 2003) (quoting *Downing v. Mun. Court*, 88 Cal.App.2d 345, 350, 198 P.2d 923 (Cal. Ct. App. 1948)).

Defendant relies upon several early data privacy cases—*Yunker v. Pandora Media, Inc.*, 2013 WL 1282980, at *1 (N.D. Cal. Mar. 26, 2013); *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1030 (N.D. Cal. 2012); and *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1074 (N.D. Cal. 2012)—to support its argument that Plaintiffs' personal information is not "property." But more recent decisions have noted that this is an outdated position. For instance, Judge Koh authored the decision in *Low*, which dismissed a conversion claim based on the defendant's alleged disclosure of the plaintiffs' personal browsing history and other PII because "the weight of authority holds that a plaintiff's 'personal information' does not constitute property." 900 F. Supp. 2d at 1030. But

nine years later, in *Calhoun v. Google LLC*, Judge Koh rejected Google's reliance on *Low*, finding that—consistent with a "growing trend across courts"—the taking of personal information is sufficient to allege deprivation of a property interest. *See e.g.* 526 F. Supp. 3d 605, 635 (N.D. Cal. 2021) (holding that courts have recognized the "growing trend across courts . . . to recognize the lost property value" of personal information) (collecting cases); *see also In re Facebook Privacy Litigation*, 572 F. App'x 494, 494 (9th Cir. 2014) (holding that plaintiffs' allegations that they were harmed by the dissemination of their personal information and by losing the sales value of that information were sufficient to show damages for their breach of contract and fraud claims); *Griffith v. TikTok, Inc.*, 2023 WL 7107262, at *9-10 (C.D. Cal. Oct. 6, 2023) (following Judge Koh's analysis in rejecting the defendant's argument that plaintiff failed to allege a property interest in her personal information).).[10]

Furthermore, California courts have also acknowledged that users have a property interest in their personal information. *See CTC Real Estate Servs. v. Lepe*, 140 Cal. App. 4th 856, 860, 44 Cal.Rptr.3d 823 (2006) ("A person's identifying information is a valuable asset."); accord *Facebook Tracking*, 956 F.3d at 600 (citing *Lepe* and holding that the plaintiffs had suffered economic injury after Facebook allegedly took their personal information in a similar process to that alleged here).

As set forth above, Plaintiffs have sufficiently alleged that their personal information was converted in a "wrongful act," due to the highly offensive nature of the way in which Defendants

[10] *Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 798–99 (N.D. Cal. 2011) (plaintiffs' names were misappropriated and thus lost value which constituted an injury to plaintiffs); *In re Anthem Inc. Data Breach Litig.*, 2016 WL 3029783, at *14 (N.D. Cal. May 17, 2016) (plaintiffs' personal information was stolen in a data breach and thus lost value which constituted an injury to plaintiffs); *In re Yahoo! Inc. Cust. Data Sec. Breach Litig.*, 2017 WL 3727318, at *13 (N.D. Cal. Aug. 30, 2017) (same).

surreptitiously took their information. Finally, as discussed *supra* at Section G2, Plaintiffs have properly alleged that they have been damaged by the wrongful conversion of their personal information due to their loss of control of that information and the loss of value of that information now that it is out of their control. Accordingly, they have properly alleged all the elements of their conversion claim.

J. Plaintiffs' Claim for Unjust Enrichment is Adequately Pleaded

As the Ninth Circuit recognized in *Facebook Tracking*, "California law recognizes a legal interest in unjustly earned profits" and thus "requires disgorgement of unjustly earned profits regardless of whether a defendant's actions caused a plaintiff to directly expend his or her own financial resources or whether a defendant's actions directly caused the plaintiff's property to become less valuable." 956 F.3d at 600. "Under California law, this stake in unjustly earned profits exists regardless of whether an individual planned to sell his or her data or whether the individual's data is made less valuable." *Id.* Thus, where, as here, plaintiffs allege that their internet and browsing histories carry financial value, that the defendants profited from this valuable data, and that they "did not provide authorization for the use of their personal information, nor did they have any control over its use to produce revenue," the "unauthorized use of their information for profit would entitle Plaintiffs to profits unjustly earned." *Id.* at 601.

Defendants argue that to recover on their unjust enrichment claim, Plaintiffs must allege that a benefit was conferred through "mistake, fraud, coercion or request." Mot. at 32. But "the scope of unjust enrichment under California law is [not] so narrow." *Thane Int'l, Inc. v. 9472541 Canada Inc.*, 2020 WL 7416171, at *8 (C.D. Cal. Nov. 16, 2020) (relying on the Ninth Circuit's analysis in *Facebook Tracking* and rejecting defendant's identical argument). That is because such a "narrow definition of unjust enrichment would lead to absurd results. For example, a victim of

theft or conversion would not be entitled to restitution because the wrongdoer did not obtain the benefit by 'fraud, mistake, coercion or request.' This is not the law in California." *Id.* "All that unjust enrichment requires is that defendant has inured some benefit from plaintiff and it is somehow unjust for defendant to retain that benefit." *Id.* (quoting *Minx Int'l, Inc. v. M.R.R. Fabric*, 2015 WL 12645752, at *5 (C.D. Cal. Feb. 11, 2015)). Plaintiffs have thus satisfied their pleading burden. *Greenley v. Kochava, Inc.*, 2023 WL 4833466, at *4 (S.D. Cal. July 27, 2023) (relying on *Facebook Tracking*).

K. Plaintiffs' UCL and Common Law Claims Are Not Superseded by California's Uniform Trade Secrets Act

Defendants' position on California's UTSA contravenes arguments in other sections of its motion, primarily that Plaintiffs' Personal Information has value. *Compare*, *e.g.*, Mot. at 33 (citing cases where CUTSA supersedes certain causes of action where the data has value) *with* Mot. at 13 (arguing that Plaintiffs did not lose money or property and that "[m]isappropriation of personal information is not an 'economic injury . . . .'"). Nevertheless, Plaintiffs' common law and UCL claims are not superseded by the CUTSA; CUTSA has no place here, where the torts alleged are more akin to a data misuse/data breach claim, as opposed to misappropriation of "confidential business and proprietary information." *See e.g. Erhart v. Bofi Holding, Inc.*, 612 F. Supp. 3d 1062, 1119 (S.D. Cal. 2020) (holding that an "unauthorized taking of customer financial information" is "more akin to a data breach claim" than a disguised trade secret claim premised on the wrongful taking and use of "confidential business and proprietary information") (citing *K.C. Multimedia, Inc. v. Bank of Am. Tech. & Operations, Inc.*, 171 Cal. App. 4th 939, 958, 90 Cal. Rptr. 3d 247 (2009)); *Chromadex, Inc. v. Elysium Health, Inc.,* 369 F. Supp. 3d 983, 989 (C.D. Cal. 2019) (holding that CUTSA "serves to preempt all claims premised on the wrongful taking and use of

confidential business and proprietary information . . .") (emphasis added; citation omitted; collecting cases).

Where CUTSA supersedes non-CUTSA claims, the reasoning is based on the "nucleus of facts test" where non-CUTSA claims *in the same case* are superseded by CUTSA because they are both based "on the same nucleus of facts as trade secret misappropriation." *Genasys Inc. v. Vector Acoustics, LLC*, 638 F. Supp. 3d 1135, 1155 (S.D. Cal. 2022). "The nucleus of facts test does not focus on whether a non-CUTSA claim requires the pleading of different elements than the CUTSA claim, but rather on whether there is a *material distinction* between the wrongdoing alleged in a CUTSA claim and that alleged in the non-CUTSA claim." *Id.* (citing *Beckton, Dickinson & Co. v. Cytek Bioscis. Inc.*, 2018 WL 2298500, at *5 (N.D. Cal. May 21, 2018)) (emphasis in original). In *Vector Acoustics*, the court dismissed a CUTSA claim but declined to dismiss a UCL claim because "[w]ithout knowing which allegations—if any—contain valid trade secrets, the Court is not able to determine whether those claims are preempted by CUTSA." *Id.*

Crucially, the *Vector Acoustics* court recognized that "until the distinction is made between [the plaintiff]'s allegedly misappropriated *trade secret information* and its *confidential or non-confidential proprietary non-trade secret information*, the question of preemption should not be addressed." *Id.* (citing *Amron Int'l Driving Supply, Inc. v. Hydrolinx Diving Commc'n, Inc.*, 2011 WL 5025178, at *10 (S.D. Cal. Oct. 21, 2011)) (emphasis added). It logically follows that absent a finding that trade secrets are at issue (as opposed to confidential non-trade secret information), the CUTSA cannot supersede or otherwise preempt Plaintiffs' claims in this case.

Separately, Defendants' cases are unavailing and do not support CUTSA superseding Plaintiffs' claims. Notably, none of Defendants' cases involve a consumer's information (private, confidential, or otherwise) being taken and misappropriated by a defendant. Instead, these cases

involve business-to-business disputes where the plaintiff specifically averred that intellectual property (in one form or another) was taken in violation of trade secret laws. Mot. at 33.[11] This included misappropriation of technologies exceeding the scope of licensing agreements, theft of confidential intellectual property subject to non-disclosure agreements, disputes about the unauthorized dissemination of customer and supplier lists from former employers to competitors, and similar violations that squarely fall within traditional trade secret disputes. *Ibid.*

IV. CONCLUSION

Plaintiffs have met their burden at the pleading stage and respectfully request that the Court deny Defendants' motion to dismiss. To the extent the Court is inclined to grant any portion of Defendants' motion to dismiss, Plaintiffs respectfully request leave to amend.

[11] Citing *Mattel, Inc. v. MGA Ent., Inc.*, 782 F. Supp. 2d 911, 987 (C.D. Cal. 2011) (misappropriation of intellectual property that former employee created during employment and brought to competitor); *Heller v. Cepia, L.L.C.*, 2012 WL 13572, at *7 (N.D. Cal. Jan. 4, 2012) (misappropriation of toy hamster project); *K.C. Multimedia, Inc. v. Bank of Am. Tech. & Operations, Inc.*, 171 Cal.App.4th 939, 954 (2009) (misappropriation of technology used in banking applications); *Silvaco Data Sys. v. Intel Corp.*, 184 Cal.App.4th 210, 239 (Cal.App.6th 2010) (misappropriate of technology used in software products); *NetApp, Inc. v. Nimble Storage, Inc.*, 41 F. Supp. 3d 816, 839 (N.D. Cal. 2014) (misappropriation of trade secrets and poaching employees related to technology); *Digital Enjoy, Inc. v. Google, Inc.*, 370 F. Supp. 2d 1025, 1035 (N.D. Cal. 2005) (dispute over the scope of a licensee's rights for digital technology); *Callaway Golf Co. v. Dunlop Slazenger Grp. Ams., Inc.*, 318 F. Supp. 2d 216, 221 (D. Del. 2004) (patent infringement); *MedImpact Healthcare Sys., Inc. v. IQVIA Inc.*, 2020 WL 5064253, at *20 (S.D. Cal. Aug. 27, 2020) (misappropriation of trade secrets in violation of NDAs); *Race Winning Brands, Inc. v. Gearhart*, 2023 WL 4681539, at *6 (C.D. Cal. Apr. 21, 2023) (violation of employment contract with non-compete, non-disclosure, and anti-poaching covenants); *Farmers Ins. Exchange v. Steele Ins. Agency, Inc.*, 2013 WL 3872950 (E.D. Cal. July 25, 2013) (insurance companies engaged in dispute over their captive agents' alleged violations of non-disclosure agreements); *New Show Studios LLC v. Needle*, 2014 WL 2988271 (C.D. Cal. June 30, 2014) (former employee violated employment agreement by misappropriating intellectual property); *Glam and Glits Nail Design, Inc. v. #NotPolish, Inc.*, 2021 WL 2317410 (S.D. Cal. June 7, 2021) (former employee left for competitor and misappropriated confidential customer list).

DATED: March 7, 2024

/s/ Ryan J. Clarkson
CLARKSON LAW FIRM, P.C.
Ryan J. Clarkson, Esq.
Yana Hart, Esq.
Tiara Avaness, Esq.

DATED: March 7, 2024

/s/ Michael F. Ram
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
Michael F. Ram
John A. Yanchunis
Ryan J. McGee