United States District Court
Northern District of California

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

IN RE META PIXEL HEALTHCARE LITIGATION

This Document Relates To:

All Actions

Case No. 22-cv-03580-WHO

**ORDER ON MOTION FOR CLASS CERTIFICATION AND MOTIONS TO EXCLUDE**

Re: Dkt. Nos. 1152, 1154, 1251, 1252, 1257, 1258, 1259, 1260, 1261, 1263, 1279, 1288, 1309, 1310, 1311, 1312, 1319, 1352, 1253, 1362, 1376, 1378, 1379, 1392, 1399, 1409

Plaintiffs seek to certify four classes of Facebook users whose protected healthcare information was obtained by defendant Meta Platforms, Inc. ("Meta") or whose devices were impacted by Meta when they were on their healthcare providers' websites or applications ("apps"). Meta opposes, primarily by identifying a few instances out of presumably millions that Meta argues would require individualized determination, such as instances where someone utilized their own device to make healthcare communications on behalf of a family member or friend. At this point, however, those examples amount to de minimis instances of individuals who may or may not have been damaged by Meta's practices.

Meta also challenges the quality and completeness of its own data, arguing that even it cannot track which healthcare entities had its tracking technology set to collect protected data throughout the whole class period. Plaintiffs assert that their experts have proposed accepted methodologies that can accomplish this task in a number of ways – pointing to the default settings on Meta's products (consistent through at least some significant portions of the class period) and through the sampling of data and then extrapolating from that sampled data. As discussed below in connection with the motions to exclude, the debate between plaintiffs' experts and Meta's

witnesses and experts on these points is significant, but in the end provides grounds for cross-examination and not exclusion.

Meta's opposition confuses complexity – which undoubtedly this action presents– and individualized questions. Various accepted case management strategies can handle the complexity of this case. With limited exceptions discussed below, plaintiffs and their experts have proposed defined classes and methodologies that allow them, at this juncture, to proceed with certified classes.

## I. MOTION FOR CLASS CERTIFICATION

"Before certifying a class, the trial court must conduct a rigorous analysis to determine whether the party seeking certification has met the prerequisites of Rule 23." *Mazza v. Am. Honda Motor Co., Inc*., 666 F.3d 581, 588 (9th Cir. 2012) (internal quotations omitted). The party seeking certification has the burden to show, by a preponderance of the evidence, that certain prerequisites have been met. *See Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 348-50 (2011); *Conn. Ret. Plans & Trust Funds v. Amgen Inc*., 660 F.3d 1170, 1175 (9th Cir. 2011).

Certification under Rule 23 is a two-step process. The party seeking certification must first satisfy the four threshold requirements of Rule 23(a): (1) the class is so numerous that joinder of all members is impracticable; (2) there are questions of law or fact common to the class; (3) the claims or defenses of the representative parties are typical of the claims or defenses of the class; and (4) the representative parties will fairly and adequately protect the interests of the class. Fed. R. Civ. P. 23(a).

Next, the party seeking certification must establish that one of the three grounds for certification applies. *See* Fed. R. Civ. P. 23(b). Plaintiffs seek certification under Rule 23(b)(3), which requires them to establish that "the questions of law or fact common to class members predominate over any questions affecting only individual members, and that a class action is superior to other available methods for fairly and efficiently adjudicating the controversy." Fed. R. Civ. P. 23(b)(3). In the alternative to the (b)(3) class, plaintiffs seek certification under Rule 23(b)(2) for any issues that I determine are fit for class treatment.

The process of class-certification analysis "may entail some overlap with the merits of the

plaintiff's underlying claim." *Amgen Inc. v. Connecticut Ret. Plans & Trust Funds*, 568 U.S. 455, 465–66 (2013) (internal quotations omitted). However, "Rule 23 grants courts no license to engage in free-ranging merits inquiries at the certification stage." *Id*. at 466. "Merits questions may be considered to the extent—but only to the extent—that they are relevant to determining whether the Rule 23 prerequisites for class certification are satisfied." *Id*.

Plaintiffs seek to certify the following classes for a Class Period of June 17, 2018, to the present:

1. **The Patient Status Button-Click Class** – All Facebook users who had at least one patient portal, medical appointment, bill payment, or diagnostic assessment button click obtained by Meta from Class Healthcare Providers.[1]
2. **The Patient Health Information Class** – All Facebook users who had at least one communication or fact identifying a doctor, condition, or treatment acquired by Meta from Class Healthcare Providers, excluding Button-Click events described above.
3. **The Prescription Drug Information Class** – All Facebook users whose communications with a prescription drug website for which they have a prescription, were obtained by Meta.
4. **The Patient Device Intrusion Class** – All Facebook users for whom Meta placed an _fbp cookie and/or used computing resources by sending data to Meta through their device and/or by computing Core Setup logic on their device while at a Healthcare Provider property.

All four classes seek certification of their claims for: (1) breach of contract; (2) breach of the implied covenant; (3) intrusion on seclusion; and (4) violation of California's Comprehensive Computer Data Access and Fraud Act ("CDAFA," Cal. Penal Code § 502 *et seq*). The Patient Status Button-Click, Patient Health Information, and Prescription Drug classes also seek

[1] Plaintiffs have identified "Class Healthcare Providers," who are entities covered by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), at issue in the Patient-Statue Button-Click Class and Patient Health Information Class. Plaintiffs' motion to file their revised Class Healthcare Providers list, Dkt. No. 1377, is GRANTED.

certification of their claims under the Electronic Communications Privacy Act ("ECPA") and the California Invasion of Privacy Law ("CIPA").

### A. Rule 23(a) & Rule 23(b)(3)

There is no dispute about numerosity, adequacy, or typicality, and I find those elements of Rule 23(a) are satisfied by plaintiffs' showing. C.C. Mot. at 16-18. Similarly, there is no dispute over the existence of traditionally recognized common questions of fact and law supporting certification. C.C. Mot. at 16-17. Meta rests its challenge to certification on a lack of predominance and a lack of superiority. C.C. Oppo. at 7-29.

#### 1. Predominance

Plaintiffs explain why common issues predominate in their motion on a claim by claim and remedy by remedy basis. C.C. Mot. 18-30. In opposition, Meta collapses the different claims and makes overarching arguments that plaintiffs lack sufficient proof to show classwide: (1) that every website and app developer sent each class member's protected health information to Meta; (2) whether users consented to share information with Meta; (3) Meta's intent and knowledge to acquire the protected health information; and (4) damages.

##### a. Which Entities and What Data

###### i. HIPAA and CMIA-covered entities

Meta argues that there is no classwide way to show that "web and app developers" on plaintiffs' exhibit lists are covered HIPAA or CMIA entities. I disagree.

To start, it is worth noting that HIPAA entities are identified by plaintiffs in their Class Healthcare Provider list and their identities are relevant only to the Button-Click and Patient Status classes, which cover patient status disclosures and specific types of communications between patients and the HIPAA-covered entities. Plaintiffs will, presumably, introduce evidence at summary judgment or trial to prove that the entities in their Class Healthcare Provider lists are covered entities. Meta will, presumably, attempt to show the opposite. While this process may be time consuming, that is not surprising in a complex case like this.

Meta relies on *Frasco v. FloHealth*, Case No. 21-cv-00757-JD, where after discovery, summary judgment and trial the Hon. James Donato indicated that he was inclined to grant

judgment as a matter of law on a CMIA claim because he was not sure if a period tracking app was a provider of healthcare or the users covered by the CMIA. C.C. Oppo. at 8. Here, the issue of which entities are properly included on plaintiffs' Class Healthcare Providers or covered by CMIA will be briefed, I assume, at summary judgment. There are case management and trial management approaches that can be utilized to make sure this and other issues are resolved in an orderly and clear fashion by the appropriate trier of fact, including by stipulations or testing at summary judgment. *Flo Health* may have involved an "edge case", but that does not mean that this process will be as time consuming or difficult as Meta argues here.

Meta's other examples are likewise not persuasive. That an entity may provide public facing websites – providing news about fellowships or research articles – does not complicate this case where the classes are defined as patients whose button clicks or communications disclose their patient status or specific healthcare needs.

**ii. At-Issue Data**

Meta also argues that there is no classwide way to identify which healthcare sites sent data that is At-Issue[2] in this case about any class member to Meta given: (1) the configurability of the Pixel; (2) Meta's data retention policies; (3) Meta's efforts at filters and blocking the data; and (4) that users did different things on each site, including general research which would not be protected by HIPAA or CMIA, and not all "users" were patients so each will have to prove their patient status and that they engaged in a covered activity.

Meta's Developer-Side Defenses. For (1), Meta argues that since the Pixel is configurable and websites and apps were able to refuse the Business Tools defaults, there are some websites and apps that did not share protected healthcare data of patients with Meta despite using Meta's Business Tools. According to plaintiffs and their experts, however, common proof will show that for most of the class period Meta's "default settings" on the Business Tools allowed it to acquire

[2] Used throughout this Order, "At-Issue" data is defined by the scope of classes at issue. So, for the Patient Status Button-Click Class, the At-Issue data is information disclosing patient status, for the Patient Health Information Class At-Issue data is information disclosing a patient's doctor, condition, or treatment, and for the Prescription Drug Information Class At-Issue data is limited to communications that contain the name of the prescription drug.

At-Issue data and that Meta never disclosed to the healthcare entities that they should alter the defaults, or how to do so. *Compare* Expert Reports and Reply/Rebuttal Reports from Dr. Atif Hashmi and Dr. Zubair Shafiq (Dkt. Nos. 1317-9, 1317-10); *with* Expert Report of Dr. George Zervas, Declaration and Supplemental Declaration of Tobais Wooldridge. Dkt. No. 1367-1 & Vol. 13 Def. App'x at 4244-4477. It may be that at summary judgment or trial, there will be no dispute or the trier of fact may determine that as of a certain date, Meta did not have default settings collecting this data or that Meta had sufficiently educated healthcare entities of their ability or need to alter the default or other workflow settings. *But see* Shafiq Rebuttal ¶ 36 (citing academic research showing that Automatic Events configuration was active on 99.6 percent of healthcare websites from 2019 to 2022).[3] That may result in a narrowing of the class periods or available damages or restitution. *See Nolen v. PeopleConnect, Inc*., No. 24-3894, 2026 WL 2871735, at *17 (9th Cir. Sept. 24, 2026) (reiterating that district courts retain the flexibility to address problems with a certified class as they arise, including the ability to narrow or decertify). But those issues will be common; in particular, it will be common to specific identifiable healthcare entities.

Meta's Data. The related, and admittedly more difficult issue for plaintiffs, is (2). Meta argues that as a result of its standard retention policies the oldest classwide data is from March 2022, yet plaintiffs' proposed classes go back to June 2018. Meta admits that developer-specific information could be sought from the entities on plaintiffs' Class Healthcare Providers list to prove where and whether each relevant website or app used Meta's Business Tools during the relevant timeframe would have recorded Button-Clicks, patient statuses, or prescription communications, but argues that plaintiffs have not sought that information and presenting it would be unmanageable. Meta nevertheless undertook some efforts on this front, arguing that some of the entities on the Class Healthcare Providers list have "sworn" that they have never used

[3] Because the only technology at issue here is Meta's, this case is unlike *Ingraham v. Cap. One Fin. Corp*., No. 24-CV-05985-TLT, 2026 WL 1759155 (N.D. Cal. June 16, 2026). There, the Hon. Trina Thompson found that individualized issues predominated where plaintiffs brought claims based on the defendant allowing at least eight different types of technologies provided by eleven different third-parties to transmit at least twelve categories of "personal and financial" information back to the third-parties. *Id*. at *1, 6.

the Business Tools, including the Pixel, or that they used the Pixel only on parts of their websites for specific periods of time. C.C. Oppo. at 10; *see e.g.,* Meta Appendix, Volume 8, Ex. 128, ¶ 7 (Deaconess Illinois Red Bud Regional Hospital, which declares that "at no point since [] January 2023, has [it] purchased, obtained or otherwise utilized any Meta Business Tools for operation on Red Bud Regional Hospital's website"). According to plaintiffs and their experts, whether that is true can be tested through Meta's data that *does* exist as compared to the information Meta secured through subpoena or otherwise. Again, it can be tested at summary judgment, at trial, or through other case management techniques.[4]

Plaintiffs will have to make choices on how to try this case and manage some of the complex but not truly individualized questions.

Meta's Efforts to Block Data. Addressing (3), and as discussed below with respect to the motions to exclude, Meta's efforts at blocking the data – when they started, how they operated, and what they blocked – are disputed by the parties and their experts. That evidence is common, not individualized. At summary judgment, trial or post-trial, the scope of the classes, resulting damages or restitution (if any) can be conformed to the proof as necessary

Meta's User-Side Defenses. Addressing (4), plaintiffs' class definitions are limited to *patients* whose identified and protected information was acquired by Meta. As discussed below, plaintiffs' experts have suggested methods by which these class members can be identified. Of course, if the trier of fact finds in plaintiffs' favor, these individuals can likewise self-identify at the appropriate juncture, presumably following an aggregate damage or restitution award, as patients who disclosed the protected information covered by the class definitions on Class Healthcare Providers' websites or apps. As the Ninth Circuit just confirmed in *Nolen,* "Rule 23 does not require the lead plaintiff to demonstrate at the certification stage an 'administratively feasible' means of identifying whether someone falls within or outside the class definition." 2026 WL 2871735 at *13. Here, class members can readily identify their patient status and, if

[4] Plaintiffs may, for example, pare down their Class Healthcare Providers list to conform to the evidence secured either from the Class Healthcare Entities or from Meta's internal data, to remove Class Healthcare Providers that did not have Meta's Business Tools installed on their sites or apps at any point during the class period.

necessary, the types of information they shared with their Class Healthcare Provider.

The structure of the classes in this case, patients whose specifically identified and HIPAA or CMIA-protected information was acquired by Meta, distinguishes this case from *Smith v. Facebook, Inc*., 262 F. Supp. 3d 943, 955 (N.D. Cal. 2017), *aff'd*, 745 F. App'x 8 (9th Cir. 2018). The information in *Smith* was simply URL headers that contained "general health information that is accessible to the public at large" and nothing about the data allegedly transmitted related to a "'past, present, or future physical or mental health or condition of an individual.'" (emphasis in original). Here, it is HIPAA-protected information of patients that was acquired by Meta. *But see Cole v. Quest Diagnostics Inc*., No. 25-1449, 2025 WL 3172640, at *3 (3d Cir. Nov. 13, 2025) (fact that individuals received diagnostic services not CMIA-protected information); *Griffith v. TikTok, Inc.,* No. 5:23-CV-00964-SB-E, 2024 WL 4308813, at *5 (C.D. Cal. Sept. 9, 2024), *reconsideration denied*, No. 5:23-CV-00964-SB-E, 2024 WL 4874556 (C.D. Cal. Oct. 22, 2024) (recognizing the obvious; "[t]hat privacy concerns are not identical across all websites that use the Pixel. For example, it is not clear that a person visiting the Build-a-Bear website has the same expectation of privacy or is likely to disclose equally sensitive information as a visitor to the website for Rite Aid's pharmacy.").[5]

The cases that Meta relies on are distinguishable. The hurdle to the plaintiff's CMIA claims in *Doe v. Eating Recovery Ctr. LLC*, No. 23-CV-05561-VC, 2025 WL 2983143, at *1 (N.D. Cal. Oct. 17, 2025) was that Doe did not become a patient until after her information was shared via Meta's Pixel, defeating the CMIA claims as a matter of law. The hurdle in *Doe v. MedStar Health, Inc*., No. 24-C-20-000591, 2023 WL 4931348, at *9 (Md.Cir.Ct. Mar. 10, 2023)

[5] In *Ingraham v. Cap. One Fin. Corp*., No. 24-CV-05985-TLT, 2026 WL 1759155, at *6 (N.D. Cal. June 16, 2026), plaintiffs defined to class to include twelve broad and general categories of personal and financial information and admitted that not every plaintiff disclosed every type of personal information to defendant in their interactions with the platform. *See id*. *6 ("Plaintiff's privacy claims here depend on an individualized assessment of each prospective plaintiffs' interactions with the tracking technology and the amount and type of information included on their credit card application."). And in *Sisti v. Bosley Inc*., 831 F. Supp. 3d 979, 987 (C.D. Cal. 2026), the complaint was dismissed because the information at issue was not healthcare, patient, or other protected or highly sensitive information and "Plaintiff does not allege that any information that he entered into the scheduling form — health-related or otherwise — was disclosed to third parties."

was that the class covered situations where individuals "may have been searching for the location of the parking garage" but not seeking information about their healthcare. Those examples are not encompassed in the classes as defined by plaintiffs here. Using Meta's example of Jane Doe IV (*see* C.C. Oppo. at 12-13), any general research she engaged in prior to becoming a patient or user of a specific prescription drug would not be actionable. Plaintiffs' experts attest that they can account for, and will be required to account for, Meta's receipt of non-protected information in determining damages (or perhaps more appropriately restitution): that will be complex, but at this point it appears feasible, manageable, and significantly amenable to either classwide or subclassed resolution (*e.g.*, for all patients who button-clicked on a particular site during a particular timeframe).

To the extent that individuals may have logged onto healthcare websites or apps on behalf of others, *e.g.*, acting for a family member and not themselves as patients, Meta has not shown through expert opinion or otherwise that these occurrences present anything other than a de minimis impact on the scope of the class.[6] *See Nolen*, 2026 WL 2871735 at *12 (reaffirming that defendant cannot speculate as to impact of individualized issues on the class, the defendant must show impact on a "significant number" of proposed class members). Similarly, Meta's argument that its system may not always have "matched" HIPAA-protected data with Facebook users is disputed by plaintiffs' experts, but in any event has not been shown on this record to have anything more than a de minimis impact on the scope of the classes. Meta asserts that consumer-side options – *e.g.*, the use of ad-blocking technologies or private browsing modes – impacts the "matching" and, therefore, Article III standing of class members. *See* C.C. Oppo. at 11, 13. But the ability of third-party offered blocking mechanisms to prevent the transmission of the At-Issue

[6] Plaintiffs argue that because Meta connects household members through user IDs and serves advertisements to related household members, these family-member occurrences would still result in a patient's protected information not only being acquired by Meta but also being used. C.C. Reply at 7 (citing Shafiq Rebuttal ¶¶ 73-75). For this and other reasons, Meta's reliance on *In re Apple Iphone Antitrust Litig.*, No. 4:11-CV-6714-YGR, 2025 WL 3124160, at *12-13, *16 (N.D. Cal. Oct. 27, 2025) is unhelpful. In that case, the antitrust damages expert was excluded and the class decertified because the expert's analysis did not link the purchaser (children or those with duplicate names) to the injured payor (parents and unique payors).

data is disputed by plaintiffs' experts. *Compare* Zervas Rep. ¶¶ 84-95 (discussing third-party anti-tracking tools) *with* Shafiq Rebuttal ¶¶ 37-45 (noting the blocking tools did not block server-side Pixel transmissions, many tools had limited impact, and Meta affirmatively worked with third-parties to unblock its tracking tools). As with many of Meta's other class certification defenses, the competing evidence will be tested at summary judgment or trial and the classes or aggregate damages or restitution will be conformed accordingly.

Concerning Article III standing, Meta's reliance on *Popa v. Microsoft Corp*., 153 F.4th 784, 791 (9th Cir. 2025), where standing was questioned for a common law intrusion claim as plaintiff did not "explain how the tracking of her interactions with the PSP website caused her to experience any kind of harm that is remotely similar to the 'highly offensive' interferences or disclosures that were actionable at common law," is not persuasive. The Ninth Circuit's recent decision in *Black v. IEC Grp., Inc*., No. 25-5952, 2026 WL 3031874, at *2, 6 (9th Cir. Oct. 9, 2026), recognized that "[s]tanding must of course be shown claim by claim and is not 'dispensed in gross,'" and found that there was no "doubt that actions for breach of contract, even without any allegations of pecuniary or physical injury, were available at common law." Plaintiffs' breach of contract claim, based on promises Meta made to plaintiffs, provides a firm footing for the breach of contract claim and also informs the statutory and common law privacy claims.[7]

Finally, to the extent Meta's examples of no-Article III standing cover more than a de minimis portion of the class – which to date, Meta has not attempted to show – Meta may move to decertify all or a portion of the class. But, according to plaintiffs' theory and the testimony of

[7] The nature of the information at issue in this case, as confirmed by the *Black v. IEC Grp., Inc*. opinion, as well as the expert testimony demonstrating acquisition and matching, distinguishes this case from *Smith v. Rack Room Shoes, Inc*., No. 24-CV-06709-RFL, 2026 WL 2825524 (N.D. Cal. Sept. 21, 2026). There, the district court denied the motion for class certification for lack of Article III standing because "Plaintiffs failed to put forward evidence from which a reasonable jury could conclude that their browsing activity on Rack Room's website was sensitive enough to make the mere presence of active third-party tracking technology on rackroomshoes.com objectively offensive, without any actual tracking." *Id*. at *1. The same is true for *Gershzon v. Meta Platforms, Inc*., No. 23-CV-00083-SI, 2026 WL 2970373, at *5 (N.D. Cal. Sept. 30, 2026) (dismissing case and not reaching certification based on lack of Article III standing where "[t]he Pixel did not transmit information about whether any of these transactions were actually completed, nor did the Pixel transmit any substantive information about any transaction, such as plaintiffs' addresses, driver's license numbers, or disability status.").

their experts, Meta's business model would not work if these measures resulted in anything other than a de minimis impact.[8]

**b. User Consent**

Meta next broadly argues that consent is an individualized issue that must be addressed but is impossible to show classwide because: (1) each Class Healthcare Providers website and app provided its own disclosures to patients; (2) patients consented if they continued to use their healthcare websites and apps after they knew of Meta's conduct; and (3) many users shared their own healthcare data on their Facebook page. However, the issue of consent – and whether it truly raises predominant individualized issues – must be considered on a claim-by-claim basis.

Under the ECPA and CIPA, consent is an affirmative defense. For these claims, as well as breach of contract and the common law privacy claims, consent can be express or implied *but* it must be "actual." *Calhoun v. Google, LLC,* 113 F.4th 1141, 1147 (9th Cir. 2024) ("For consent to be actual, the disclosures must 'explicitly notify' users of the conduct at issue."). Whether a reasonable user would find Meta's disclosures gave "actual" consent is an objective question, *see id*., that will likely be resolved on summary judgment on a classwide basis. *See Johnson v. CoreCivic*, No. 4:16-CV-00947-SRB, 2018 WL 7918162, at *10 (W.D. Mo. Sept. 18, 2018) ("while Defendants contend that various forms of consent are present in the case, that suggestion only goes to inform the prevailing common legal question of whether such warnings of potential recording and monitoring of communications between attorneys and their detainee-clients rise to the level of consent, which applies to the class as a whole."); *see also Raffin v. Medicredit, Inc*., No. CV154912GHKPJWX, 2017 WL 131745, at *9 (C.D. Cal. Jan. 3, 2017) ("Because every putative class member was subject to this policy on a uniform basis, determining consent to record

[8] It is worth noting that the record in this case from the experts interpreting what Meta's data can or cannot show is vastly different from *Hinton v. Planned Parenthood Fed. of America*, *Inc*., No. 23-CV-04529-JD, 2026 WL 2959993 (N.D. Cal. Sept. 30, 2026). There, apparently, plaintiffs eschewed expert analysis and relied only on "generalized evidence about Meta and Google's business goals and promises" that failed to supply the common proof necessary to argue to a jury, on a class basis, "that 'Meta and Google *actually* linked class members' PPFA Website searches and page views concerning private healthcare concerns" to their specific identities. *Id*. at *3. Here, given the contractual promises at the heart of this case, it is not clear that "linkage" needs to be shown for the causes of action. In any event, plaintiffs' evidentiary showing in support of class certification extends far beyond public reports on Meta's business operations.

can be accomplished without resort to individualized proof" for CIPA claim).

The ECPA has an additional element, as it is a "one-party consent" statute. Meta argues that one-party consent precludes certification because for each website and app, the trier of fact must consider both (1) Meta's knowledge of what it was acquiring from each specific website or app and (2) what level of consent was secured by each website and app from the end user. Plaintiffs respond that this issue is really non-existent because none of the various disclosures made either by Meta or by the entities on the Class Healthcare Provider lists permits the entities or Meta to disclose, acquire, or use the narrow category of information at issue in this case--HIPAA and CMIA protected information.

That evidence will be largely, if not fully, common. It will include what Meta told the website and app operators about how its Business Tools generally and the Pixel specifically operated. Whether those disclosure were sufficient, in light of how Meta acquired the HIPAA-protected information about the Class Healthcare Providers' patients and then used that data for Meta's internal use or for third-party advertising, will largely be common and based on Meta's policies and common disclosures. If Meta is correct and there is evidence about what the Class Healthcare Providers knew and/or disclosed to their users about their own sharing of data with Meta or other third parties, that evidence is not *individualized.* It covers the hundreds, thousands, or tens of thousands of class members who secured healthcare from each of those entities.[9] That analysis, if necessary, could be readily accomplished with case and trial management strategies and would not outweigh the common, predominant evidence. In the end, if a particular healthcare provider actually consented on behalf of their clients despite the requirements of HIPAA and

[9] Therefore, while I may have to review disclosures of specific websites or apps to determine whether those disclosures objectively demonstrate actual knowledge that HIPAA or CMIA-protected data could be shared, that will be on behalf of many class members, not individual class members. *See, e.g., L.B. v. LinkedIn Corp.*, No. 5:24-CV-06832-EJD, 2025 WL 2899514, at *11 (N.D. Cal. Oct. 10, 2025) (finding fertility apps disclosures "so specific that there can be no reasonable expectation that the information provided to Spring Fertility is private."). Moreover, to the extent any Class Healthcare Provider disclosed the actual practice here and secured a group of class members' consent to that actual practice, how the disclosures of those Class Healthcare Providers interacts with Meta's own liability based on Meta's own contractual promises, will likewise be resolved common to the clients of those Class Healthcare Providers.

CMIA[10] to Meta's acquisition of their At-Issue data, that evidence is common to the class members who were patients of those specific healthcare providers.[11]

Meta relies on a number of cases from this District where judges found that consent created predominant, individualized issues precluding class certification in whole or in part. For example, in *In re Google Inc. Gmail Litig*., No. 13-md-2430, 2014 WL 1102660, at *14 (N.D. Cal. Mar. 18, 2014), the court considered a case where plaintiffs alleged that Google scanned the contents of their emails and thereby violated ECPA and CIPA. Because some of Google's disclosures disclosed that very practice, "there would be a myriad of individual issues with respect to consent, because Google itself had several disclosures, which could not have been uniformly viewed by Class members." *Id*. at *18. The court recognized that in privacy litigation, consent can be "express," but it can also be "implied in fact based on whether the surrounding circumstances demonstrate" that the party whose personal information was collected knew it. As a result, implied consent presented "an intensely factual question that requires consideration of the circumstances" surrounding the alleged privacy violation, precluding certification of the ECPA and CIPA claims. *Id*. at *16; *see also Brown v. Google*. 2022 WL 17961497, at *19 (Google provided "evidence that its consent defense would be based on individual, and subjective, interactions of what certain class members knew, read, saw, or encountered" and the "[e]vidence

[10] While there is no claim based on HIPAA, HIPAA is relevant to establishing reasonable consumer expectation and possibly a reasonable consumer's understanding of the meaning of Meta's contractual promises requiring partners to have "lawful rights" to the information sent to Meta. These too are common questions of law subject to common proof. By relying on HIPAA to set a floor in industry practices and consumer expectations, plaintiffs are not attempting to get around the lack of a direct claim under HIPAA. *Compare USA, Inc. v. Santa Clara Cnty., Cal*., 563 U.S. 110, 121 (2011) (recognizing incompatibility of private suits with HIPAA); *with In re Tiktok, Inc., Minor Priv. Litig*., No. MDL 3144-GW-RAOX, 2025 WL 3628598, at *14 (C.D. Cal. Nov. 5, 2025), *adopted sub nom. In re TikTok, Inc., Minor Priv. Litig*., No. MDL 3144-GW-RAOX, 2025 WL 3628448 (C.D. Cal. Nov. 6, 2025) ("Plaintiffs may, however, use COPPA as relevant context in establishing the elements of their privacy claims, particularly given the highly 'context-specific nature of the [reasonable expectation of] privacy inquiry.'") (quoting *McDonald v. Kiloo ApS*, 385 F. Supp. 3d 1022, 1035 (N.D. Cal. 2019)).

[11] Plaintiffs argue that in this unlikely scenario, they would prove that the ECPA's crime-tort exception applies in light of Meta's "further" use of the acquired data in matching it to specific Facebook users. I do not need to determine the applicability of the crime-tort exception at this juncture but note that analysis would only be required if Meta met its burden to show actual consent on behalf of identified Class Healthcare Providers.

shows variation between what users knew or did not know.").

That line of cases was followed in *In re Google RTB Consumer Priv. Litig*., No. 4:21-CV-2155-YGR, 2024 WL 2242690, at *12 (N.D. Cal. Apr. 4, 2024). There, the court also found that implied consent would raise predominant individualized issues because there were half a dozen different disclosures by the defendant itself, express disclosures by third-parties of the very practice at issue, and consumer surveys showing that a high percentage of possible class members knew and understood that the defendant traded in their personal information. *Id*. at *12-14.

These opinions preceded the Ninth Circuit's decision in *Calhoun v. Google*, which held that actual consent is required – the question is what a "reasonable" consumer would understand the disclosures to mean. *Calhoun*, 113 F.4th at 1151 ("a determination of what a 'reasonable' user would have understood must take into account the level of sophistication attributable to the general public, which uses Google's services"). Therefore, what one consumer understood – as a result of reading an article about Meta's practices or their understanding of what Meta or their healthcare entity disclosed to them – is not the question.[12] Instead, it is the common question of what a reasonable person would understand. *Torres v. Prudential Fin., Inc*., No. 22-CV-7465-CRB, 2024 WL 4894289, at *7 (N.D. Cal. Nov. 26, 2024) ("Plaintiffs are correct that the issue of how a reasonable user would understand Prudential's privacy policies is a common one that can be resolved with class-wide proof.").

In the cases on which Meta relies, there were numerous disclosures of the defendants' *actual* practices that many if not most of the proposed class members would likely have seen. Those undisputed facts created the predominant individualized issues. Here, on the other hand, plaintiffs argue that nothing in Meta's own disclosures or in the disclosures made by the Class Healthcare Providers actually disclose the conduct at the heart of this case – that Meta acquired At-Issue data connected to the individuals. And in fact, plaintiffs argue that Meta's contracts

[12] *See Rodriguez v. Google LLC*, No. 20-CV-04688-RS, 2024 WL 38302, at * 9 (N.D. Cal. Jan. 3, 2024) ("the 'relevant question' as to consent inquiry under CIPA concerns website operator's disclosures about its data collection practices, not third-party disclosures about operator's practices.").

promise exactly the opposite, that they would not secure At-Issue data unless the Class Healthcare Providers had rights to disclose it, which they could not legally do in light of HIPAA, and that Meta would block its receipt of the At-Issue data. Meta's cases are inapposite.[13]

**c. Intent and Knowledge.**

Meta notes that the ECPA, CDAFA, and privacy-tort claims require proving Meta's intent and knowing receipt of the At-Issue data. Meta argues that showing its intent would require individualized inquiries and that any classwide inference would violate its due process rights. C.C. Oppo. at 21-22. This argument is not well taken. As shown by the extensive expert discovery, some of which is discussed below in connection with the motions to exclude, the parties dispute what Meta knew about its interception of healthcare related data, when Meta knew it, what steps Meta took to attempt to prevent its acquisition of that data, and how effective those attempts were. Each of these questions is subject to common proof. Meta's defense that some healthcare providers may have altered Meta's defaults that automatically transmitted At-Issue information to Meta does not mean that Meta's intent raises predominant individualized questions. The evidence regarding how Meta's products were promoted and delivered to healthcare entities, what Meta told those entities, what Meta knew about information received back from those entities, and how Meta responded or did not respond is common evidence. It may be true that some healthcare entities took efforts on their end to block healthcare data going to Meta or that Meta may have alerted a few entities that they were sending "potentially sensitive health data." *See* C.C. Oppo. at 21. But when Meta learned that was happening, how Meta responded, and who responded, would be *common*, at least with respect to class members of that healthcare provider. That is not a predominant individualized question. At most it may demand a redefined list of Class Healthcare Providers or a subclass with a shortened class period.

**d. Claim-Specific Issues**

[13] As already noted, to the extent that Meta argues that some of the Class Healthcare Providers' disclosures differ and might show one-party consent, that consent will be determined commonly and objectively for all the clients of that provider. That is not individualized but common to class members of that specific provider. *Frasco v. Flo Health, Inc.*, 349 F.R.D. 557, 575 (N.D. Cal. 2025) (squarely placing the burden on a defendant to present evidence that implied consent required a determination on "class-member-by-class-member" basis).

Meta argues that other aspects of the causes of action at issue raise individualized issue.

**i. Interception in California**

Section 631 of CIPA[14] and CDAFA both require a California nexus. Plaintiffs and Meta dispute whether Meta's California headquarters, choice of law provisions, data access, and data storage practices suffice to provide the nexus for all class members – or only for California-based class members. Meta notes that at least with respect to the CIPA section 631 claim, Judge Donato declined to certify a section 631 class because a California nexus was lacking, but allowed the 632 claim to proceed. *Frasco v. Flo Health, Inc.*, 349 F.R.D. 557, 587 (N.D. Cal. 2025) ("Commonality and predominance are demonstrated for the CIPA § 632 claim, but not for the § 631 claim."). Plaintiffs, recognizing the issue, suggest that for section 631, if I do not certify a nationwide class I should instead certify "subclasses of patients who either communicated from California or exchanged a communication with a California-based healthcare provider." C.C. Mot. at 22 n 6. I agree.

That narrowed section 631 class would be appropriate because plaintiffs point to Meta's admission that it preserved data "corresponding to users located in California" at least as of June 19, 2021. *See* Pls. Ex. 227 [Dkt. No. 1317-3 at 5]; Shafiq Rebuttal ¶¶ 140-147. Plaintiffs also identify common evidence that "up2x data" is stored at all of Meta's data centers, including those in California, which presumably would provide the required nexus. *See* Pls. Ex. 228-232 [Dkt. Nos. 1317-4 – 1317-8]; Hashmi Reply Rep. ¶ 62. Meta may dispute whether this evidence shows what plaintiffs contend it shows (they did not address it at oral argument), but that is an issue for summary judgment or trial. At this point, plaintiffs have made a plausible showing of the required

[14] Section 631, in relevant part, imposes liability on "[a]ny person who, by means of any machine, instrument, or contrivance, or in any other manner," either: (1) willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within California; or (2) who uses or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained. Cal. Penal Code § 631(a). *See also* section 632(a) (imposing liability on any "person who, intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication.").

California-nexus for the narrowed section 631 claim and for the CDAFA claim. [15]

**ii. Contents**

Meta argues that individualized questions predominate in determining whether Meta intercepts "contents" of a protected communication under ECPA and CIPA section 631. Meta's argument ignores how the classes are defined: (1) button clicks that disclose patient status, (2) patients communicating about a specific doctor, condition, or treatment, and (3) communications with a prescription drug website for which they have a prescription. Whether these categories of information are considered contents under the ECPA or CIPA section 631 are common questions. It may be, for example, that Meta will be able to prove that the prescription drug site URLs it acquired, or its subsequent efforts to hash URLs, means that contents protected by ECPA and CIPA section 631 were not disclosed for some or all of the class period. *See also In re Google Inc. Cookie Placement Consumer Priv. Litig*., 806 F.3d 125, 137 (3d Cir. 2015) (recognizing that when "URL is instead part of the substantive information conveyed to the recipient, then by definition it is 'content'" under ECPA). But that evidence appears to be common at this juncture. Similarly, common evidence will show whether and when Meta's systems captured these categories of data, either through the provider websites and apps or from cookies placed on the patients' devices.

**iii. CDAFA**

Finally, Meta argues that each plaintiff must show that their devices were impacted by Meta's placing cookies on their devices to support the CDAFA claim.[16] Again, the impact of Meta's actions is subject to common evidence from the parties' experts. If Meta demonstrates at

---

[15] Part of that testing will, presumably, be testimony from the parties' competing experts on whether Meta's data, as well as the locations of its and the Class Healthcare Providers servers, amount to sufficient evidence of a California nexus. *See, e.g*., Shafiq Rebuttal ¶¶ 140-147 (responding to Dr. Zervas's criticisms about geolocation and other California-nexus information). This analysis, like others discussed herein, may be complex but it does not create predominant, individualized issues precluding class certification. At most it may result in a narrowing of the time period for a certified class or decertification. *See Nolen*, 2026 WL 2871735 at *17.

[16] Meta argues that Conversions API ("CAPI") and "customer lists" uploads – two types of acts by Meta that were within plaintiffs' device class definition – do not affect any plaintiffs' devices. In reply, plaintiffs agree and will amend that class. C.C. Reply at 17.

the merits stage that developer and user settings impact whether or not the cookie has more than a de minimis affect on device functions or otherwise raises arguments that call into question the certification of this claim, I will revisit the viability of this claim on a classwide basis.

**e. Damages**

Meta makes a number of arguments regarding damages. As an initial matter, differences in damages rarely defeat class certification. *Vaquero v. Ashley Furniture Indus., Inc*., 824 F.3d 1150, 1155 (9th Cir. 2016) ("the need for individual damages calculations does not, alone, defeat class certification"); *see also Nolen*, 2026 WL 2871735 at *16 ("Generally, the need to resolve individualized issues concerning damages—as opposed to liability—will not defeat certification.").

Turning to the particular claims here, statutory or punitive damages – even if discretionary – will be determined on classwide basis. *See Frasco v. Flo Health, Inc*., No. 21-CV-00757-JD, 2025 WL 2680068, at *13 (N.D. Cal. Sept. 17, 2025) (discussing statutory damages under CIPA as non-discretionary, although recognizing ECPA statutory damages might be within the discretion of the court considering various factors). Considering the statutory or punitive damages that might be available as a matter of discretion, the reprehensibility of any conduct for which Meta might be liable, and the need to avoid duplicative or excessive damages, are readily determined commonly post-trial if and as necessary. *See id*. [17]

The same is true for disgorgement or restitution, equitable remedies that as discussed below are subject to common proof that Meta may attack as being overbroad. As also discussed below, actual damages will be subject to common proof from plaintiffs' experts.

Predominance has been shown.

---

[17] I recognize that the court in *Campbell v. Facebook Inc*., 315 F.R.D. 250, 269 (N.D. Cal. 2016), concluded that determining statutory damages under the ECPA – which is a matter of discretion and requires the court to weigh multiple factors – precluded class certification because in that case it would "involve individual questions about whether each specific class member's award was excessive," a determination that turned in part on the "severity of the violation" and the "extent of any intrusion into the plaintiff's privacy." *Id*. at 268. That case is readily distinguishable. In *Campbell*, plaintiffs sought to certify a class all Facebook users who had included URLs in their private messages that they alleged were scanned by Facebook and then used for various purposes. *See id*. at 255-257. The class was not limited by the type of information scanned and used – as it is here – to protected healthcare information.

**2. Superiority**

Meta's second argument is that because the classes sought to be certified extend beyond the information Meta acquired from brick-and-mortar hospitals and their related healthcare websites and now includes healthcare apps and pharmacies, my prior rulings foreclose a finding of superiority. C.C. Oppo. at 29-30. Meta relies on my disclination – back in 2023 when the tidal wave of Pixel and related privacy cases was crashing into the Northern District – to relate cases based on similar privacy causes of action but asserted against healthcare-adjacent providers (*e.g.*, apps providing birth control, healthcare coupons, and counselling services). *Id*. at 29. While Meta is correct that I was attempting to carve limits around this case – and not become the sole Northern District judge handling any healthcare-adjacent website and app-based privacy cases – nothing in my prior orders concerned whether collective action against Meta for providing Business Tools in aid of its acquisition and subsequent use of consumer's healthcare information for its own benefit was appropriate. Instead, as I informed counsel, the shape of this case would be determined on class certification. Here we are.

Meta argues both that the novelty of the technology and questions at the heart of this case make a class action not superior, and that there is enough monetary incentive for individuals to pursue these cases. C.C. Oppo. at 29-30. This case's complexity and the novel claims asserted make the classwide resolution of those claims superior. $5,000 in statutory damages – assuming statutory damages under CIPA or otherwise are appropriate – is by no means insignificant. But I am sure that Meta's legal bills for this case – even if limited to amounts spent on discovery regarding Meta's classification systems, data pipelines, and the related expert discovery – swamps any individual's statutory or actual damages claim.

Meta's lack of superiority arguments are unsubstantial and counter-intuitive.

**B. Rule 23(b)(2)**

As something of a backup position, plaintiffs argue that if I do not certify a (b)(3) damages class, a (b)(2) injunctive relief class is also appropriate to enjoin "Meta from collecting and using Health Information communications on Healthcare Provider web-properties, using patient computer device storage and resources on healthcare provider websites [], and requiring it to make

certain disclosures, including about its data collection and advertising practices." C.C. Mot. at 30.

"Class certification under Rule 23(b)(2) is appropriate only where the primary relief sought is declaratory or injunctive." *Zinser v. Accufix Rsch. Inst., Inc*., 253 F.3d 1180, 1195 (9th Cir.), *opinion amended on denial of reh'g*, 273 F.3d 1266 (9th Cir. 2001). In *Brown v. Google, LLC*, No. 20-CV-3664-YGR, 2022 WL 17961497, at *19 (N.D. Cal. Dec. 12, 2022), after finding the "implied consent" issues there defeated predominance, the court nonetheless certified a (b)(2) class. The "plaintiffs describe the 'general contours' of the injunction they seek. Injunctive relief would (1) preclude Google from collecting further private browsing information; (2) require Google to delete the private browsing information that it previously collected and is currently storing; (3) require Google to remove any services that were developed or improved with the private browsing information; and (4) appointment of an independent third-party to verify that the injunctive relief has been implemented. These would be important changes to reflect transparency in the system. . . . Plaintiffs' description sufficiently identifies the specific course of conduct that plaintiffs seek to enjoin, and it establishes that this course of conduct applies to the entire proposed class." *Id*. at *20.

Meta's opposition that a (b)(2) class is inappropriate where plaintiffs also seek damages was rejected in *Brown*, 2022 WL 17961497 at *20, and is rejected here where, although damages are significant, so are the injunctive relief requirements plaintiffs specifically identify. Meta also argues that plaintiffs are not entitled to injunctive relief because they were not entitled to preliminary injunctive relief at the inception of this case and Meta has "improved" its efforts to prevent protected healthcare information from being intercepted. Plaintiffs' experts, however, dispute that. At this juncture, certification under both (b)(2) and (b)(3) is appropriate. If, after all evidence has been considered, the evidence overwhelmingly shows that Meta is no longer acquiring the At-Issue data alleged, and Meta has structures in place to prevent its acquisition of that data, injunctive relief would no longer be at issue.

Plaintiffs' motion for class certification is GRANTED for the reasons discussed above and in light of the rulings on the motions to exclude discussed below.

## II. DEFENDANTS' MOTION TO EXCLUDE

### A. Shafiq

Meta moves to exclude three opinions in full and one opinion in part from plaintiffs' class certification expert, Dr. Zubair Shafiq, a professor of Computer Science at University of California, Davis. Dkt. No. 1263-2. Shafiq was retained by plaintiffs to opine on the identification of healthcare provider websites using Meta's products, Meta's collection of information identifying users and the content of those users' communications, and the effectiveness of Meta's filters that purported to screen out healthcare or identifying information. Shafiq Report [Dkt. No. 1154-6], Ex. 3 to the Barnes Decl.

#### 1. Opinion 1: "Meta can and does programmatically identify healthcare provider websites and apps where it collects data via Meta Pixel and other Meta Business Tools." Shafiq Rep. ¶¶ 48-75.

Meta argues that this opinion is irrelevant to class certification because Shafiq admitted that none of Meta's internal classifications can be used to identify HIPAA or CMIA-covered entities and that Shafiq does not provide a methodology to do so. It argues that its MegaTaxon[18] classifications are not determinative of whether an entity associated with a website or app *is* covered by HIPAA or CMIA, and by using the MegaTaxon classifications as a proxy for "health-related" data, Shafiq's analysis captured non-HIPAA or CMIA covered entities and information, *e.g.*, like data associated with a newspaper article about a medical condition. Meta makes the same argument with respect to Shafiq's reliance on Meta's RDTT classification system,[19] which is part of the "signal integrity system" that Meta contends was designed to prevent receipt of potentially sensitive data.

That Meta's classifications systems might be overbroad in that they sweep in some amount of non-HIPAA or CMIA entities or information – and Meta has only pointed to a handful of examples out of hundreds, many of which were refined out in plaintiffs' revised Healthcare Provider list, Dkt. No. 1377 – does not mean that this opinion is excludable. Shafiq's opinion is

[18] MegaTaxon classifications are classifications to which ads and Pixels were "mapped." Shafiq Rep. ¶¶ 51-52.

[19] Restricted Data Taxonomy Tree ("RDTT") is a classification system developed by Meta to identify restricted data, including healthcare data.

that Meta has classified, and apparently still is classifying, healthcare related information, either to use it for its advertising purposes or to attempt to screen it out. That Meta's own systems may be overbroad in some instances presents grounds for cross-examination, not exclusion.

Meta also argues that this opinion is unreliable because Shafiq relies on plaintiffs' counsels' pre-vetted list of entities covered by HIPAA or CMIA. Meta argues that Shafiq's analysis fails to account for any "false-positives" in plaintiffs' lists and that Shafiq did not investigate false positives. Finally, Meta contends that the filtering by Shafiq of Meta's RDTT categories (in an attempt to find healthcare related filters) was "arbitrary, unexplained and unreliable." These arguments go to weight, not admissibility. The few over-inclusiveness and false positive instances identified by Meta do not undercut the opinion that Meta can programmatically identify websites and apps where it likely acquired healthcare-related data.

**2. Opinion 3(a): "Meta Collects and Can Programmatically Identify Meta Business Tool Data from Healthcare Provider Websites Related to Patient Class Member (a) Button Clicks." Shafiq Rep. ¶¶ 126-136 & 137-153.**

Meta argues that this opinion is unreliable and inapplicable to the facts of this case. The "Patient Status Button-Click Class" includes Facebook users who had at least one patient portal, medical appointment, bill payment, or diagnostic assessment button obtained by Meta from "Class Healthcare Providers." "Programmatically" means "creation of a computer program" that Shafiq performed to "classify" button clicks in Meta Pixel logs as: (1) portal, (2) payment, (3) assessment, and (4) schedule. Shafiq Rep. ¶ 139. Shafiq identified three methods of reviewing the data, based on his initial efforts looking to 7.3 million buttons associated with 1,844 domains. These included: (1) a sample manual review of data; (2) use of manually crafted "labelling patterns"; and (3) using an AI model to review the data, where data was confirmed by further manual testing. Meta argues that Shafiq essentially wants to use the AI model to accomplish the scale required to assess the up to 650,000 domains at issue in this case, but that is not a reliable method and is instead "unscientific, untestable, and unverifiable."

Meta's arguments go to weight, not exclusion. Shafiq has shown his methodology, testing, manual review, and extrapolation through use of an AI model. Each of these methodologies are,

essentially, sampling methodologies that can be run, verified, and challenged by Meta's own experts.

**3. Opinion 3(b): "Meta Collects and Can Programmatically Identify Meta Business Tool Data from Healthcare Provider Websites Related to Patient Class Member . . . (b) Health Information." Shafiq Rep. ¶¶ 154-157.**

Metal argues that this opinion is unreliable and irrelevant for the same reasons as Opinion 3(a). Meta's arguments go to weight and not admissibility.

**4. Opinion 10: "There are More Than 40 Class Members in Each of the Proposed Classes." Shafiq Rep. ¶¶ 204-209.**

Meta argues that this must be excluded as Shafiq's opinion relies solely on his work producing Opinions 1 and 3, to which Meta objects above, and Opinion 2, which is simply a "general narrative" of Meta's matching system but not, according to Meta, a replicable classwide methodology. As I have denied Meta's motion to exclude Opinions 1 and 3, the motion is denied as to Opinion 10 as well.

Meta's motion to exclude the identified opinions of Shafiq is DENIED.

**B. Singer**

Meta moves to exclude the opinions of plaintiffs' damages expert Dr. Hal J. Singer. Singer demonstrates a standard economic approach to the valuation of At-Issue data for the purpose of assessing common impact and aggregate damages to each class. Singer Report [Dkt. No. 1320-1], Ex. 14 to Kafka Decl., ¶¶ 6-10. He performed "Choice-Based Conjoint Analyses" ("CBC"), which are "controlled, survey-based experiments that objectively measure preferences though a series of 'choice tasks' that ask participants to pick among multiple product or service packages, similar to how consumers make decisions in real markets." Singer Rep. ¶ 40.

Meta argues that Singer's opinions must be excluded because they are not based on a reliable method as Singer used an unsupported "Willingness to Accept" ("WTA") survey that ignores demand and is generally recognized to produce inflated results. Meta separately asserts that Singer's surveys fail *Comcast's* "fit" requirement because they are inconsistent with plaintiffs' proposed class definitions and theory of damages.

**1. Willingness to Accept Survey**

Meta argues that because Singer's surveys measured respondents' desire for payment, and not actual market prices for healthcare data, his analyses based on those surveys do not reliably calculate damages. Meta notes that in most consumer cases, conjoint surveys have been approved to demonstrate how much consumers would have been willing to pay for a falsely advertised product (price premium) or how much less they would have paid had they known the issues with the product (willingness to pay). Here, Singer's WTA survey puts the consumer into the position of the person selling the product, asking how much they value the information that Meta improperly acquired and how much they would be willing to sell it for. Meta argues that this particular approach has never been accepted by a court, and what Singer should have done is determined the demand for the consumers' data and how much companies would have been willing to pay for that data. Meta also argues that WTA surveys are well known to inflate results, and points to an academic study (relied on by Singer) that argues against "uncritical use" of those surveys.

I find at this juncture that Singer's decision to utilize a WTA survey – an accepted methodology put to a slightly different purpose in this type of case – is admissible. Meta's criticisms go to weight, not admissibility. Meta and its experts can point out the literature expressing caution in use of the model and its risk of inflation.

**2. Fixed Demand**

Meta also argues that because Singer used a fixed demand in his conjoint analysis but did not include "real world" prices for this data, it is not similar to the many courts (including this one) that have rejected challenges to conjoint studies that used fixed supply-side factors, but only because the models used real world prices. I recognize that fixed demand without a market analysis of actual prices may be novel, but that is because no market exists for the purchase or sale of HIPAA and CMIA-protected information. The techniques used by Dr. Singer are one method of demonstrating what that market might look like, using accepted methodologies. Singer points out that for merits purposes the surveys could be adjusted in light of developments in the market and market-participant practices with respect to healthcare related data. For purposes of class

certification, Singer's surveys suffice.

**3. *Comcast* Fit**

Meta also moves to exclude Singer's analyses because his surveys asked about healthcare and prescription information "that is not at issue here." Meta points to one example: the Patient Health Class is defined as disclosing information identifying a "doctor, condition or treatment," and Singer asked respondents about disclosure of those events and about disclosure of "services" "symptoms" or "diagnoses." Meta's argument is simply wordsmithing Singer's choices. Meta may contend at the merits stage that the words Singer used or uses in his surveys convey something dramatically different from the types of information that plaintiffs contend were impermissibly acquired by Meta for each class. But this is not a labelling case involving specific use of advertising language or a case where the surveys sought and tallied responses wholly unrelated to the claims alleged by the class. On their face, Singer's terms challenged by Meta are not mis-matched to the class definitions.

Meta also argues that while plaintiffs' theories of harm are that a class members' healthcare and prescription information were obtained or acquired by Meta, Singer tested the collection and "use" of healthcare and prescription information. Meta points to preliminary or explanatory parts of Singer's surveys that explain that the questions will be about Meta's receipt and use of the information. It argues that emphasis on use – which is not implicated by the classes or the claims – and therefore the models' damage estimates do not match the theory of plaintiffs' case. Plaintiffs respond that the mentions of use were separate from the actual survey questions which focused on the acquisition of the data, and that omitting the few background mentions of use would have made the surveys less realistic. In any event, Singer can easily adjust the surveys to remove use and any ambiguity it causes.

I do not find that the "use" explanatory language undermines the showing that Singer's surveys and conjoint analysis can measure the impact of Meta acquiring this data. If Singer wants to avoid the confusion argument at the merits stage, simple adjustments to the surveys can be made.

Meta's motion to exclude Singer is DENIED.

### C. Zigrang

Meta moves to exclude in full the opinions of Todd A. Zigrang, the President of Health Capital Consultants ("HCC"), who was retained to: (1) evaluate the feasibility of calculating the value of health information that Meta intercepted; (2) evaluate the feasibility of calculating the profits to Meta from that data; (3) calculate the value of that information; and (4) calculate the profits to Meta. Zigrang relied on information produced by Meta, as well as publicly available information, to create profit models to measure and reasonably approximate profits Meta received from receipt and use of class members' data.

#### 1. Data Valuation Opinions

Meta argues that the Data Valuation opinions should be excluded as irrelevant or unreliable because Zigrang: (1) had to consider the "fair market value" of the data but admitted there is "no market for HIPAA-protected data"; (2) conceded that he did not know exactly what the At-Issue data contains but just made assumptions based on counsel's direction; and (3) rests his analysis on "factual gaps, unfounded assumptions, and erroneous inputs," including that he did not use "comparable" transactions about health data (using other types of information), the comparables used do not match (e.g., shopping data); his transactions could have been valued with a range but he set the value at the maximum possible payout, he converted non-cash consideration (gift cards or cryptocurrency) into cash value, and he improperly included instances where individuals paid to have no-ads on a service or have their data kept out of databases, which is not what this case is about. Meta also moves to exclude because (4) Zigrang failed to differentiate between value of data in each of the four classes plaintiffs seek to certify.

These attacks all go to weight and not admissibility. That Zigrang relies on Meta's own data and counsel's direction in formulating his opinions is a basis for cross-examination, not exclusion. Whether an expert used appropriately comparable variables as a proxy is a classic area of attack for cross-examination. (Plaintiffs point out that this likely resulted in lower valuation estimates for healthcare data that was associated with particular users.) While Meta argues that Zigrang should have differentiated between the data at issue in the different classes, that too is a ground for cross-examination. Overall, Meta seeks to exclude Zigrang because everyone admits

that there is no current, "legal market" for protected healthcare information, but it cannot win its arguments because of that fact. Zigrang has used methodologically sound models, based on Meta's own information and classifications – arguably its own "market" – to approximate the value of the At-Issue data.

**2. Profit Opinions**

Meta makes similar arguments regarding Zigrang's profit opinions but also attacks his failure to show a causal connection between the alleged profits he calculates and the At-Issue data. Meta contends that Zigrang's damages are overbroad because he included all monies earned by Meta from all data in "health" sounding categories, but some of that data is not protected, not At-Issue, or was secured from entities not within the class definitions. It also argues that Zigrang failed to apportion damages between At-Issue protected data and non-At-Issue data that might fall within a Meta classification but is not at issue in this case. Meta next contends that Zigrang's opinions must be excluded because he does not understand how Meta actually generates advertising revenue and instead relies on unfounded assumptions. As a result, it argues that Zigrang "cannot accurately attribute revenue to use of the At-Issue Data." Finally, as above, Meta complains that Zigrang fails to apportion damages between the different classes.

Plaintiffs respond that Zigrang has developed a reasonable approximation of the profits Meta gained through the receipt and use of At-Issue healthcare data. He did so by relying on Meta's own records and data categorizations. That approach may well result in overbroad profit estimates. For example, if Meta shows at trial that its own categorizations of healthcare-related data include a significant portion of information that is not HIPAA or CMIA-protected, Zigrang's reliance on those categorizations can be attacked. But absent evidence from Meta that Zigrang's approximations based on Meta's own categorizations are so far off the mark – which it has not shown on this record – Meta's arguments go to the weight of Zigrang's estimates not their admissibility. Similarly, disputes about which of Meta's categorizations Zigrang included in his model is really a dispute about model inputs, and likewise goes to weight, not admissibility. Finally, Zigrang's profit models are relevant to one theory of liability—unjust enrichment. If liable, the proper apportionment of a restitutionary award between or among the classes will be

subject to argument and proof on which Meta will bear the burden.

Meta's motion to exclude Zigrang is DENIED.

**D. Cohen**

Meta moves to exclude opinions from L. Glenn Cohen, a professor of law at Harvard Law School, who was retained to opine on whether the use of Meta's data collection tools on healthcare provider websites and apps in the manner alleged by plaintiffs violated medical ethics and HIPAA. Cohen concludes that Meta's conduct violates traditional customs and norms for health information. Cohen Rep. ¶ 24.

Meta moves to strike Cohen's opinions in full because: (1) he did not look at any of the data Meta acquired to determine whether it was HIPAA-protected or otherwise personal health information; (2) his testimony is irrelevant to the breach of contract claim or excludable to the extent he offers opinions on the interpretation of contracts (*i.e.*, whether Meta violated its promise that its partners have the lawful rights to collect and use and share the At-Issue data); and (3) his opinion that the data transmissions at issue violated HIPAA must be excluded as a legal conclusion.

Meta's motion to exclude is DENIED without prejudice to re-raising objections at trial. As with the other experts, simply because Cohen based his assumption that Meta acquired HIPAA-protected data at the direction of plaintiffs' counsel does not mean his opinions are excludable as unreliable. The few examples Meta identifies from Cohen's deposition – from entities included in plaintiffs' now-revised Class Healthcare Providers list (*e.g.*, yoga studios, entities operating outside the United States) or "boundary cases" (*e.g.*, genome sequencing company) that Meta relies heavily on above – are grounds for cross-examination, not exclusion. Meta's concerns about Cohen's testimony extending into impermissible legal conclusions are valid. Whether Cohen's testimony may be cabined at trial should be determined in limine or at trial depending, for example, if Meta argues that its conduct was consistent with industry "norms."

**E. Barasz & Vohs**

Meta moves to exclude the opinions of plaintiffs' experts Dr. Kate Baraz, a former business school professor, who was retained by plaintiffs to opine about whether Meta users care

about maintaining online privacy, have expectations about how their personal information is handled, would expect Meta to have obtained their information from partners who were not allowed to share it, and the effect of Meta's transparency and control tools on Meta users. In the same motion, Meta also seeks to exclude the opinions of Dr. Kathleen D. Vohs, a professor at the University of Minnesota, who was retained to opine on whether "people think of health information as more sensitive than other data" and whether "people agree and find it acceptable for communications with their healthcare providers to be: [c]ollected by a social media company? Used for marketing? Used to help a social media company train their AI model?"

**1. Reliable Methodologies**

Meta complains that Barasz did not conduct any surveys or experiments, but instead relied on cherry picked and ultimately mischaracterized documents as well as her personal experience. It similarly complains that Vohs relied only on a "black box" literature review that she did not memorialize or replicate. These arguments, however, are classic grounds for cross-examination and not exclusion.

**2. Speculative and Unreliable**

Meta next argues both experts rely on pre-existing studies regarding healthcare privacy but then fail to tie their analysis to the facts in this case. Meta claims that none of the studies Vohs relies on dealt with privacy or healthcare, much less data sharing among websites or digital sites, and Barasz cites studies that focus on general, public online activity (one of which she mistakenly attributed to Meta). Meta ignores these academics' reliance on their own original research in addition to their literature reviews. The disputes over cherry-picked literature and marginally relevant studies are likewise grounds for cross-examination. Finally, whether Barasz's testimony might stray into impermissible legal opinions can be determined in limine or at trial.

Meta's motion to exclude the opinions of Baraz and Vohs are DENIED.

**F. Reply Evidence**

Meta moves to strike reply declarations and supplemental opinions plaintiffs' experts submit with the Reply in support of class certification. Dkt. No. 1334. Meta argues that these declarations and opinions must be struck as they rely on newly conducted surveys (Singer) or

papers published after the original declarations were submitted (Shafiq), offer opinions outside their expertise (Singer), point to contradictory prior opinions of Meta's own experts (Singer on Hauser), address previously unaddressed source code (Hashmi and Shafiq), and otherwise unfairly hinder Meta's ability to oppose certification. *Id*. As a remedy, Meta asks: (1) to be able to re-depose Singer, Hashmi, and Shafiq before I rule on class certification; (2) to submit supplemental reports by Hauser (responding to Singer), Zervas (responding to Hashmi & Shafiq), and Amir (responding to Vohs who was only introduced as a rebuttal expert); and (3) allow Meta to file a supplemental declaration from Wooldridge (responding to Hashmi & Shafiq).

Plaintiffs filed a motion seeking leave to file a response to the objections on June 8, 2026. Dkt. No. 1378-3.[20] Plaintiffs argue that the reply declarations or supplemental opinions identified by Meta are rebuttal that directly respond to points made by defendants' experts. I agree that the reply declarations and opinions identified by Meta are rebuttal. That plaintiffs' experts have had "the last word" is a consequence of the briefing schedule. Meta had a full opportunity to raise points in response to this reply evidence in oral argument and will be able to further test those opinions as this case continues. There is no prejudice to Meta from this rebuttal evidence.[21]

[20] Plaintiffs' request, Dkt. No. 1379, to file a sur-reply in response to Meta's motion to strike is GRANTED.

[21] Meta also moves to strike plaintiffs reply Exhibit 87, which plaintiffs represent is "a document that compiles excerpts from about a dozen sources—primarily documents Meta produced in this case and Meta source code, but also from the report of Plaintiffs' expert Richard Smith, forensic evidence obtained by reports at 'The Markup,' and the complaint in the case *Doe v. Medstar Health*." Barnes Decl. [Dkt. No. 1312-4] ¶ 3. Plaintiff submitted the annotated compilation in order to avoid submitting hundreds of not thousands of pages of additional exhibits. Counsel also included "a simple document that, for each excerpt [] provide[d] the source and a very brief explanation of the relevance." *Id*. Meta objects and moves to strike the "mash up" complaining that any evidence therein is not "authenticated by an affidavit or declaration" and violated the rule that attorney arguments and statements are not evidence. *See* Dkt. No. 1334 (citing *Barcamerica Int'l USA Trust v. Tyfield Importers, Inc*., 289 F.3d 589, 593 n.4 (9th Cir. 2002)). Using this approach, while perhaps efficient, to support a class certification reply is novel. In ruling on these motions, I have not considered the attorney argument in Exhibit 87. Meta's motion to strike the attorney commentary and argument, but not the citations to evidence otherwise appropriately in the record, is GRANTED.

## III. PLAINTIFFS' MOTION TO EXCLUDE

### A. Weil

Plaintiffs move to strike the declaration of Christopher Weil, a litigation services consultant who used investigators and a media analytics platform, "Brandwatch," to analyze the reach of eight news articles published between February 2019 and April 2024 regarding Meta and other companies' tracking of personal information, including healthcare information. Plaintiffs argue that Weil's declaration and testimony should be struck under Rule 37 because the declaration fails to meet the requirements of that rule, including that Weil identify all opinions he is giving, identify the facts and data considered, and disclose his qualifications and compensation. While plaintiffs argue that Weil's failure to comply with Rule 37 cannot be excused as substantially justified or harmless,[22] Meta points out that this information was secured by plaintiffs in Weil's deposition. The motion to exclude based on Rule 37 is DENIED.

Plaintiffs also move to exclude under Rule 702, arguing that Weil has not demonstrated any specialized knowledge such that he is qualified to opine on the issues, that Brandwatch is a reliable tool, or that he used a reliable methodology. Meta responds that Weil is critical to a narrow point: whether class members saw and knew about the conduct and, therefore, consented to it. As noted above, that argument does not carry the day on class certification considering the nature of this case (where implied consent is not a defense to a contractual promise), where two articles were published mere days before the filing of this suit, and where Meta's own engineers who were central to the design of the systems at issue could not affirmatively determine what some of the articles' titles conveyed. *See* Dkt. No. 1309-3 at 12-13 (citing deposition testimony of Meta engineers). For purposes of class certification, I DENY plaintiffs' motion and will not exclude Weil's declaration and opinions. Whether his opinions may be relied on at summary judgment or trial will be determined at that point.

[22] Meta's counsel first asserted that Weil was not an expert during deposition when plaintiffs attempted to lay the foundation for Rule 37 requirements. After a break, Weil confirmed he was being presented as an expert but "only as to the facts" offered in his declaration.

**B. Zervas & Tadelis**

**1. Zervas**

Plaintiffs move to exclude the reports of Dr. Georgios Zervas, an Associate Professor of Marketing and Computing and Data Science at Boston University and an affiliated professor in Computer Science, who was retained to respond to the technical opinions of plaintiffs' experts. He opines that Meta implemented measures to prevent its collection of potentially sensitive healthcare information that have evolved over time and that website and app developers had tools and controls to determine whether and what to send to Meta. He also challenges plaintiffs' experts Shafiq, Hashmi (who opines on Meta's source code), and Smith (who opines on SubscribedButtonClick events).

Plaintiffs argue that Zervas is simply parroting what he heard from Meta engineer Tobias Wooldridge and read in Meta's documents, which is impermissible, not helpful to the jury, and not appropriate expert opinion evidence. They also contend that Zervas had no methodology, because he just relied on declarations, depositions, and discovery responses to reach his opinions. And they assert that many of Zervas's attempts to rely on Meta source code to bolster his opinions were erroneous, according to their expert Dr. Atif Hashmi. These arguments, similar to the ones made by Meta against plaintiffs' experts, amount to grounds for cross-examination and not exclusion.

More substantively, plaintiffs argue that testimony about the tools Meta had in place that evolved overtime should and will come in through Meta employees and Meta documents, making Zervas' testimony unnecessary. The testimony that Zervas can offer at trial will be determined in limine.

Plaintiffs also argue that Zervas's opinions challenging Shafiq's testimony should be excluded because they are based on Meta's spoliation of the click data. Zervas attacks Shafiq's testing of a limited set of healthcare websites and Meta's MegaTaxon classification system, arguing that the set of websites was too limited and pre-selected. But as plaintiffs point out, Shafiq undertook this approach because Meta did not preserve the data tables that would have allowed plaintiffs to test all relevant websites until October 2024, which plaintiffs assert is after Meta rolled out a new system to prevent the capture of sensitive health information. At this

juncture, plaintiffs cannot exclude Zervas' criticisms of Shafiq's approach. Whether and what limiting or clarifying instructions may be given at trial as a result of Meta's failure to preserve data tables will be determined in limine.

Plaintiffs' motion to exclude Zervas is DENIED.

**2. Tadelis**

Plaintiffs also move to dismiss specific opinions of Dr. Steven Tadelis, a professor at Haas Business School, who opines that plaintiffs overstate website visitors by failing to account for unintentional visits (misclicks and clickbacks) and proxy visits (by a user on someone else's behalf). Plaintiffs move to exclude his "first opinion": that a substantial portion of visits to at-issue healthcare entities' websites were unintentional.

Plaintiffs make a number of arguments attacking Tadelis's methodology. First, Tadelis is not qualified to opine on whether a particular event implicates At-Issue healthcare data because his expertise is in economics and advertising not healthcare regulation or privacy. Second, Tadelis looked only at a subset of the event data at issue in this case. Even considering that subset, plaintiffs argue that Tadelis's "dwell time" methodology is based on assumptions and introduces systemic bias because it does not capture session "end time" (when a user left the website), failed to account for single-event sessions (where only one event is recorded), and failed to recognize that the event table he studied did not include button-click events (omitting a key measurable event that would fundamentally alter his conclusion, which Meta failed to explain to Tadelis). Finally, plaintiffs contend that because Tadelis admitted that there is no accepted rule in the academic literature to determine whether a user visited a website or website page unintentionally, his methodology must be rejected, especially in the healthcare context where individuals using websites are not "browsing" but accessing the site for known purposes (*e.g.*, getting an appointment, reviewing test results).

These arguments are significant, but for purposes of class certification, I will not exclude Tadelis's first opinion. I am able to recognize its weaknesses and question its relevance to the

issues on class certification.[23] Plaintiffs' attacks present strong points for cross-examination, but not exclusion at this juncture. They may re-raise targeted objections at summary judgment or in limine to these opinions, based on the missing or spoliated button-click data or otherwise.

Plaintiffs' motion to exclude Zervas and the first opinion of Tadelis is DENIED for purposes of class certification.

## IV. MOTIONS TO SEAL

There are numerous pending motions to seal, filed in connection with plaintiffs' motion for class certification. Dkt. Nos. 1154, 1251,1252, 1263, 1279, 1288, 1309, 1312, 1319, 1352, 1353, 1362, 1365, 1376, 1378, 1392, 1399, 1409.

The parties submitted a joint chart covering the administrative motions to seal in connection with plaintiffs' motion for class certification. *See* Jt. Chart at Dkt. No. 1270. Since that time, the parties filed additional administrative motions in connection with the opposition, reply, and related motions. In the Joint Chart, the parties agreed that Meta's technical source code, path and table names, revenue figures and calculations, as well as information identifying the plaintiffs and contact information of defendant's employees should remain under seal at this juncture of the case for compelling justifications shown.

Remaining at issue in the materials covered by the Joint Chart is Meta's attempt to seal generalized, descriptive information that plaintiffs argue goes to the heart of their case--disclosures from Meta demonstrating that the "[f]ilter did essentially nothing" and after Meta knew that, it "used the at-issue data to score the Plaintiffs based on the health information and put the results in a secret user profiling table that Meta used for its own purposes." Dkt. No. 1270 at 4. Meta responds that although the information in dispute is not actual lines of its source code, its narrowed sealing request should be granted because it covers "technical explanations and architectural descriptions [], although written in plain English, reveal the same sensitive information as code itself." Dkt. No. 1270 at 5. Meta argues this risk "is particularly acute with

[23] For example, plaintiffs point out that class member "intent" in visiting a site is not at issue, dwell-time (even if measured properly) is not relevant to any intent, and plaintiffs' claims exist regardless of time a user spent on a webpage as long as a Pixel "fired" and Meta acquired At-Issue data.

respect to Meta's Signals Integrity systems, which are specifically designed to prevent the receipt or use of certain categories of potentially sensitive data." *Id*. at 6.

With respect to the remainder of the briefing filed after the Joint Chart, plaintiffs revisit their prior acquiesce to some of Meta's proposed continued sealing and argue that information related to Meta's internal classification systems that are no longer in use (*e.g.*, MegaTaxon) should not remain under seal as there is no longer a compelling justification to seal that source code or any of the table and field names or descriptions. Dkt. No. 1099-3 at 3-4. Plaintiffs also object to Meta's attempts to seal descriptions of its Core Setup and Meta's other efforts to filter healthcare information, noting how central these issues are to their claims and Meta's defenses. *Id*. at 4-5. Meta responds that it "seeks only to protect the lines of highly confidential code and plain language descriptions of the contents of Source Code which reveal how Meta's systems are engineered." Dkt. No. 1409-1 at 1.

As an initial matter, although I may have signed off on the parties' negotiated Protective Order, which has a broad definition of material the parties' consider "source code" to be treated as highly confidential, that does not bind plaintiffs or me in determining what may remain under seal. Meta's reliance on the broad definition of "source code" in the parties' Protective Order is not helpful. Similarly, that I have previously found that source code or specific "technical descriptions" could remain under seal under either the good cause or compelling justifications standard is relevant but does not mandate continued sealing. As this case progresses and the merits of the claims and defenses come more into focus, the weighing of the strong public interest in understanding the judicial process against the competitive concerns of a party who wants material to stay under seal can shift. *See, e.g., Kamakana v. City & Cnty. of Honolulu*, 447 F.3d 1172, 1179 (9th Cir. 2006).

Tuning to the information that both sides agree may remain under seal – source code, the names of tables or fields disclosure of which could allow bad actors to compromise Meta's active systems, internal contact information of employees, and personal health information of plaintiffs – the administrative motions to seal are GRANTED and that information may remain under seal.

Plaintiffs' objection to continued sealing of source code, or the names of tables or fields

from systems that Meta is no longer using, is OVERRULED at this juncture. That information may remain under seal, subject to revisiting the sealing issue on summary judgment or trial. By then, it will hopefully be clearer to what extent the source code and table and field names from classification and filtering systems Meta no longer uses can be disclosed.

That said, the highly generalized descriptive explanations of how Meta's systems operated may not remain under seal at this juncture. General descriptions of how Meta acquired data from Class Healthcare Providers, how Meta used that information within its own systems, including how Meta matched that information with its users and repurposed that information for improving its own systems or serving advertisements to its users, should be disclosed.

For instance, consider a few examples from the remaining disputes over the Expert Report of Atif Hashmi. The disclosure of the data detector labels and reference to the intent aggregator in the table of contents are too generalized to be sealed. *See* Jt. Chart at Dkt. No. 1270 & Corrected Wooldridge Declaration Dkt. No. 1271. The generalized introductory information at paragraph 19 of that Report and the conclusions in paragraph 19(c) and paragraph 20 are too generalized and central to plaintiffs' claims to be sealed. The more detailed, technical information in 19(a) and 19(b) as well as the table names in paragraph 20 may remain under seal. The generalized conclusions in paragraphs 94, 97 and 101 (other than the source code and table names) may not remain under seal, but the step by step technical descriptions in paragraph 100 may remain under seal.

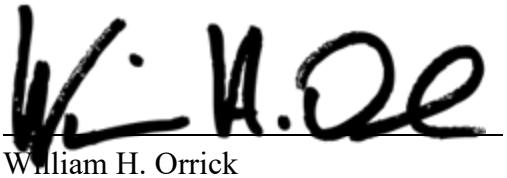
These examples are not exhaustive and hopefully provide more clarification for the parties. They shall meet and confer given this guidance, and submit one final chart covering all of the remaining class certification materials that they agree or dispute may remain under seal. To the extent they are not already publicly filed on the docket, any documents the parties agree may be unsealed or may be more narrowly redacted to prevent disclosure of the types of information identified above, shall be e-filed on the docket by the party who submitted the document originally within thirty (30) days of the date of this Order. One final joint chart, narrowing the information that Meta seeks to maintain under seal, shall be filed within thirty (30) days of the date of this Order. The parties may jointly stipulate to extend these deadlines.

## CONCLUSION

For the reasons discussed, plaintiffs' motion to certify the classes is GRANTED, except for the limited Section 631 and redefined CDAFA class. Within ten (10) days of the date of this Order, and after meeting and conferring, plaintiffs shall file a revised class definition consistent with this Order. Within thirty (30) days of the date of this Order, absent a stipulation from the parties agreeing to additional time, plaintiffs shall submit an agreed to or disputed proposed Notice Plan and forms of Notice. If the Notice Plan and forms of Notice are disputed, the competing proposal shall be addressed in one joint filing.

**IT IS SO ORDERED.**

Dated: October 30, 2026



William H. Orrick
United States District Judge

United States District Court
Northern District of California