UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

IN RE META HEALTHCARE PIXEL LITIGATION

Case No. 22-cv-03580-WHO

ORDER ON MOTION TO DISMISS AND STRIKE

Re: Dkt. Nos. 387, 388

In my September 7, 2023 Order, I denied defendant Meta Platform, Inc.'s motion to dismiss certain claims, but granted it with leave to amend plaintiffs' claims for invasion of privacy/intrusion on seclusion, California's Comprehensive Computer Data Access and Fraud Act ("CDAFA"), negligence per se, trespass, larceny, Unfair Competition Law ("UCL"), and California's Consumers Legal Remedies Act ("CLRA"). *Doe v. Meta Platforms, Inc*., No. 22-CV-03580-WHO, 2023 WL 5837443, at *17 (N.D. Cal. Sept. 7, 2023). In their First Amended Consolidated Class Action Complaint ("FAC," Dkt. No. 334-3) plaintiffs did not reallege their negligence per se, larceny, or UCL claims and amended and realleged their privacy/intrusion of seclusion, CDAFA, trespass and CLRA claims. Meta moves again to dismiss. Plaintiffs voluntarily withdraw their CLRA claim, but contest dismissal of the other claims. Meta's motion is DENIED. [1]

LEGAL STANDARD

I. CONSTITUTIONAL PRIVACY AND INTRUSION ON SECLUSION

In the September 2023 Order, I rejected most of Meta's challenges to plaintiffs' privacy claims but recognized:

[1] The factual and procedural background have been outlined in my prior Orders and will not be repeated here. Meta's administrative motion to seal its discussion of healthcare information of plaintiffs is GRANTED. Dkt. No. 388.

United States District Court
Northern District of California

> Given the nature of this case – where plaintiffs allege that both unprotected and constitutionally protected information was captured by Meta's Pixel – plaintiffs are required to amend to describe the types or categories of sensitive health information that they provided through their devices to their healthcare providers. That basic amendment (which can be general enough to protect plaintiffs' specific privacy interests) will allow these privacy claims to go forward.

September 2023 Order, 2023 WL 5837443 at *8.

In the FAC, plaintiffs identify the specific types of information they provided to their healthcare providers that they believe Meta collected without their consent. FAC ¶¶ 24-38. For the most part, plaintiffs identify the health conditions for which they sought treatment or services, as well as examples of their queries, appointment requests, or other information and services about which they communicated with their providers.

Meta takes another pass at arguing that these disclosures are insufficient to plausibly plead their privacy-based claims. Mot. at 1, 4. But the allegations suffice at this juncture because they identify generally the types of sensitive information plaintiffs shared with their healthcare providers that was plausibly collected by Meta.

Meta also attacks on these claims because the plaintiffs transmitted some or all of their healthcare information to their providers' websites through "publicly accessible" URLs, meaning URLs that were accessible without a user logging in. It contends that its retrieval of plaintiffs' information from those unprotected or public pages cannot support an invasion of privacy claim. *Smith v. Facebook, Inc.*, 745 F. App'x 8, 9 (9th Cir. 2018) ("The data show only that Plaintiffs searched and viewed publicly available health information that cannot, in and of itself, reveal details of an individual's health status or medical history. Moreover, many other kinds of information are equally sensitive. We conclude that the practice complained of falls within the scope of Plaintiffs' consent to Facebook's Terms and Policies. . . . Information available on publicly accessible websites stands in stark contrast to the personally identifiable patient records and medical histories protected by these statutes—information that unequivocally provides a window into an individual's personal medical history. . . . Put simply, the connection between a person's browsing history and his or her own state of health is too tenuous to support Plaintiffs' contention that the disclosure requirements of HIPAA or section 1798.91 apply.").

United States District Court
Northern District of California

In the Preliminary Injunction Order, I distinguished the *Smith* district court decision:

> Meta does not challenge plaintiffs' assertion that patient status is protected information under HIPAA, but instead relies on *Smith v. Facebook*, 262 F. Supp. 3d 943 (N.D. Cal. 2017). But *Smith* does not forestall my conclusion that patient status is protected health information. It dealt with the question of whether Facebook users had consented to Facebook collecting information about them via their browsing through certain health-related websites (such as http://www.cancer.net) that had an embedded Facebook "Like" button. *Smith*, 262 F. Supp. 3d at 948. Smith concluded that there was no protected health information because the information transmitted to Facebook when a user visited the http://www.cancer.net page was the same kind of information transmitted to Facebook any time a user visited any page on the internet that contained a Facebook button. *Id*. at 954. In other words, the URLs did not "relate[ ] specifically to Plaintiffs' health." *Id*. at 954. *Smith* further explained:
>
>> The URLs at issue in this case point to pages containing information about treatment options for melanoma, information about a specific doctor, search results related to the phrase "intestine transplant," a wife's blog post about her husband's cancer diagnosis, and other publicly available medical information. These pages contain general health information that is accessible to the public at large. The same pages are available *793 to every computer, tablet, smartphone, or automated crawler that sends GET requests to these URLs. Nothing about the URLs, or the content of the pages located at those URLs, relates "to the past, present, or future physical or mental health or condition of an individual." 45 C.F.R. § 160.103 (emphasis added). As such, the stricter authorization requirements of HIPAA (as well as Cal. Civ. Code § 1798.91) do not apply.
>
> *Id*. at 954–55 (underline in original).
>
> This case is different than *Smith*. Unlike the "general health information that is accessible to the public at large," the URLs and other information transmitted through the Pixel establish that a user is about to log in to a healthcare provider's website. Smith Decl. ¶¶ 31–37. Unlike in *Smith*, then, the Pixel captures information that connects a particular user to a particular healthcare provider—i.e., patient status—which falls within the ambit of information protected under HIPAA. Smith involved users browsing through websites providing healthcare information to the public at large, not users navigating to patient portals on healthcare providers' websites. The act of navigating to a patient portal on a healthcare provider's website is not the general internet browsing contemplated in Smith. As a result, *Smith* does not bear on the question of whether the information at issue here constitutes patient health information.

In re Meta Pixel Healthcare Litig., 647 F. Supp. 3d 778, 792–93 (N.D. Cal. 2022). Meta contends that based on the additional allegations of the FAC, this case falls within the *Smith* line and the privacy claims should be dismissed.

Plaintiffs counter that because they and their healthcare providers have a "privileged" relationship and because their searches were not random web searches but submission of information by patients to their healthcare providers, they can state invasion of privacy claims even if the submissions were made through the publicly available pages of their providers' websites. Plaintiffs identify published cases that are more recent than *Smith* that have accepted privacy tort claims where information was transmitted to Meta from "public" sites, including *In re Facebook, Inc. Internet Tracking Litig*., 956 F.3d 589 (9th Cir. 2020). There, "[p]laintiffs alleged that Facebook continued to collect their data after they had logged off the social media platform, in order to receive and compile their personally identifiable browsing history. As alleged in the complaint, this tracking occurred "no matter how sensitive" or personal users' browsing histories were. . . . According to Plaintiffs, by correlating users' browsing history with users' personal Facebook profiles—profiles that could include a user's employment history and political and religious affiliations—Facebook gained a cradle-to-grave profile without users' consent."). *Id*. at 598-99; *see also Cousin v. Sharp Healthcare*, No. 22-CV-2040-MMA-DDL, 2023 WL 8007350, at *3 (S.D. Cal. Nov. 17, 2023 ("the Court finds that their interactions on Defendant's website, while 'unauthenticated' or publicly facing, plausibly involve PHI," sufficient to please invasion of privacy claims).

Plaintiffs' privacy claims are not foreclosed at this juncture in whole or part simply because their communications with their healthcare providers may have been through publicly available webpages. That fact is not irrelevant to the question of whether plaintiffs will ultimately be able to prove an invasion of privacy when considering the totality of the circumstances,[2] but at this juncture and given that plaintiffs were communicating with their healthcare providers about their healthcare needs, plaintiffs have alleged enough for this claim to proceed to discovery.

[2] *See, e.g., Hill v. Nat'l Collegiate Athletic Assn*., 7 Cal. 4th 1, 26 (1994) (to determine whether an intrusion is actionably offensive courts consider: "the degree of the intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded.").

II. CDAFA

A. Damage or Loss

I dismissed this claim in the September 2023 Order so that plaintiffs could plead facts regarding "impairment of their computing devices" required under CDAFA. I rejected plaintiffs' prior theories of damage or loss based on the "diminished value of information" and their alleged "'inability' to use their computer devices to communicate with their healthcare providers in the future." *Doe v. Meta Platforms, Inc*., 2023 WL 5837443 at *9. I recognized that what plaintiffs might be able to plead on amendment regarding impairment would also inform whether plaintiff could satisfy a separate CDAFA element – to plausibly allege facts establishing the Pixel as "a contaminant that 'usurps' the normal operation of plaintiffs' devices." *Id.* at *10.

Plaintiffs now plead the following injuries: (i) Meta occupied storage space on their devices without authorization; (ii) Meta's acts caused their devices to work slower; (iii) Meta's acts used computer resources of the device; and (4) Meta unjustly profited from the data taken. AC ¶ 536. Meta argues that the amended claim must nonetheless be dismissed because all plaintiffs have not alleged sufficient damage or loss as a result of Meta's actions. But "CDAFA does not define 'damage' or 'loss' and does not contain a specific monetary threshold for loss related to violations of the statute." *Cottle v. Plaid Inc.*, 536 F. Supp. 3d 461, 487 (N.D. Cal. 2021); *see also Facebook, Inc. v. Power Ventures, Inc*., No. C 08-05780 JW, 2010 WL 3291750, at *4 (N.D. Cal. July 20, 2010) ("Although Defendants contend that any steps that Facebook took to block Power's access to the Facebook website were *de minimus* . . . Section 502 sets no threshold level of damage or loss that must be reached to impart standing to bring suit. Under the plain language of the statute, any amount of damage or loss may be sufficient."). Plaintiffs' revised allegations identifying the measureable impact on their devices is sufficient at this juncture.

B. Merits

Moving beyond damage or loss, Meta argues that plaintiffs have failed to allege facts sufficient to plausibly state violations of (c)(1) and (c)(8) of CDAFA.

Under (c)(1), the parties dispute whether mere "use" of data suffices or whether plaintiffs must, instead, plead that Meta altered, damaged, deleted or destroyed plaintiffs' data or devices.[3] Meta relies on two Central District cases that have required allegations that a defendant altered, damaged, deleted, or destroyed data and rejected the sufficiency of allegations of "mere use" of data. *Ticketmaster L.L.C. v. Prestige Ent. W., Inc.*, 315 F. Supp. 3d 1147, 1175 n.5 (C.D. Cal. 2018) ("The Court will not read the phrase "or otherwise uses" in section 502(c)(1) as prohibiting anything other than use that is similar to alteration, damage, deletion, or destruction."); *see also McGowan v. Weinstein*, 505 F. Supp. 3d 1000, 1020 (C.D. Cal. 2020) (following *Ticketmaster*). Plaintiffs rely on Northern District cases that have entered judgment *in favor of Meta* on data scraping cases based on mere use. *See, e.g.*, *Meta Platforms, Inc. v. Soc. Data Trading Ltd.*, No. 21-CV-09807-AGT, 2022 WL 18806267, at *4 (N.D. Cal. Nov. 15, 2022), *report and recommendation adopted*, No. 21-CV-09807-CRB, 2022 WL 18806265 (N.D. Cal. Dec. 8, 2022) (default judgment entered in Meta's favor based on allegations defendant exceeded consent and engaged in mere use of Meta's data, by data scrapping); *Meta Platforms, Inc. v. Ates*, No. 22-CV-03918-TSH, 2023 WL 4035611, at *6 (N.D. Cal. May 1, 2023), report and recommendation adopted, No. 4:22-CV-3918-YGR, 2023 WL 4995717 (N.D. Cal. June 27, 2023) ("California Penal Code section 502 prohibits the unauthorized access and use of any data from a computer, computer system, or computer network").

In addition, plaintiffs argue that Meta has altered plaintiffs' devices, in violation of (c)(1) by (i) "usurp[ing] the[ir] normal operation" (FAC ¶ 528); (ii) "surreptitiously plac[ing] the _fbp cookie" on them (¶ 530); and (iii) "caus[ing]" the computers to "redirect Plaintiffs' . . . data to Meta." *Id*. ¶ 530. Meta responds that this conduct is "no different" than obtaining and copying data that its Central District court cases have rejected. Reply at 14. I conclude that plaintiffs' allegations regarding the operation and impacts of the _fbp cookie are sufficient at this juncture. If Meta is right that, after discovery, all plaintiffs can point to is the mere copying of data and no alteration to plaintiffs' data or devices, then Meta may re-raise its "'mere use' is not sufficient"

[3] Cal. Penal Code § 501(c)(1) penalizes someone who "accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data."

argument.

Under (c)(8), Meta argues that plaintiffs' allegations about the Pixel do not suffice to qualify it as a prohibited contaminant under (c)(8).[4] However, plaintiffs allege that the Pixel records and transmits information to Meta. They say that Meta designed the Pixel to log and track website visitors' actions (FAC ¶¶ 53-57), that Meta disguises the Pixel as a first-party cookie to allow it to be placed on website visitors' devices and avoid detection (*id.* ¶¶ 74-75, 79), and that the Pixel usurps the normal operation of website visitors' devices. *Id.* ¶¶ 524, 528. These are sufficient to allege that the Pixel, as Meta puts it, transmits information without permission in violation of (c)(8). Whether that was Meta's intent or whether Meta's intent was not to secure sensitive tracking information without consent should be tested on an evidentiary basis.

The motion to dismiss the CDAFA claims is DENIED.

III. TRESPASS TO CHATTELS

I dismissed the trespass to chattels claim because plaintiffs failed to allege the required impact to the functionality of their devices from Meta's conduct, noting:

> there are no allegations that any functionality inherent in their computing devices has been impacted by Meta's conduct. Nor are there allegations that plaintiffs purchased any specific computing device with the purpose in whole or part of using that device to communicate with their healthcare providers. That these plaintiffs may have valued using their personal devices to communicate with their healthcare providers does not sufficiently impair the value of those devices to allow the plaintiffs to state a trespass to chattels claim.

September 2023 Order, 2023 WL 5837443 at *14.

In the FAC, plaintiffs allege the impairment as: (i) placement of the _fbp cookie/tracking tool, as the tool takes up a "measurable" amount of available storage that would otherwise be

[4] Cal. Penal Code § 502(c)(8) prohibits "Knowingly introduces any computer contaminant into any computer, computer system, or computer network." Cal. Penal Code § 502(b)(12) defined "Computer contaminant" as "any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, that are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network."

available to the devices, FAC ¶ 496; (ii) Meta source code that "used a measurable amount of resources" that slow the speed of user devices, *id.* ¶ 499; and (iii) the lost time caused by Meta's slowing communications exchanged with their healthcare providers, causing "measurable" increases in web-page loading time. *Id.* ¶ 502; *see also id.* ¶¶ 497-502. As a result, plaintiffs seek nominal damages as well as damages for the loss of storage space and loss of time caused by Meta's slowing of communications between plaintiffs and their healthcare providers. *Id.* ¶ 504.

Meta argues that the *de minimis* nature of the resource usage and slowed communications cannot support the trespass claim. In *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342 (2003), the California Supreme Court addressed a trespass to chattels claim based on a former Intel employee sending thousands of emails repeatedly to current Intel employees through Intel's email system. The Court confirmed that there must be some damage that results from the trespass, explaining that "'[t]respass remains as an occasional remedy for minor interferences, resulting in some damage, but not sufficiently serious or sufficiently important to amount to the greater tort' of conversion." *Id.* at 1351. Noting that some impact must be shown, the Court held that trespass to chattels "does not encompass, and should not be extended to encompass, an electronic communication that neither damages the recipient computer system nor impairs its functioning." *Id.* at 1347.

Hamidi did not specify how major the minor interference must be or how big the impact, other than saying that there must be some "appreciable effect on the operation of its computer system from" the defendant's conduct or a risk that the defendant's "actions will be replicated by others if found not to constitute a trespass." *Id.* at 1356. The *Hamidi* court also recognized, with respect to a claim of loss of use, that "an actionable deprivation of use 'must be for a time so substantial that it is possible to estimate the loss caused thereby. A mere momentary or theoretical deprivation of use is not sufficient unless there is a dispossession.'" It concluded that merely that defendant's email "messages temporarily used some portion of the Intel computers' processors or storage is [ ] not enough; Intel must, but does not, demonstrate some measurable loss from the use of its computer system." *Id.* at 1342.[5]

Meta argues that plaintiffs cannot plausibly make that showing here because none has alleged that the small use of their storage and other resources impacted their ability to communicate with their healthcare providers and because the miniscule delays in communications time cannot suffice. But plaintiffs have alleged a measurable impact on their devices that is not, as in *Hamidi*, temporary. The _fbp cookies remain on users' devices and continue to use storage and resources, if only a small amount. That is a significant distinction from *Hamidi*.

Meta also asserts that the alleged slowing of communications amounts, at most, to seconds of delay (Reply at 10) and that is an insufficient to establish a "significant" "loss of use" as required by *Hamidi*. The parties dispute whether these admittedly small impacts suffice under *Hamidi*. Meta says no, relying on *In re iPhone Application Litig*., 844 F. Supp. 2d 1040 (N.D. Cal. 2012). There, addressing and relying on *Hamidi*, the district court rejected plaintiffs trespass claim based on the placement of geolocation data on devices, because plaintiffs could not show a "significant reduction in service constituting an interference with the intended functioning of the system." *Id.* at 1069; *see also Yunker v. Pandora Media, Inc*., No. 11-CV-03113 JSW, 2013 WL 1282980, at *16 (N.D. Cal. Mar. 26, 2013) (following *In re IPhone Application Litigation*).

But as discussed above, the "significant" impact language was used in *Hamidi* only in connection with a deprivation of use. *See supra* n. 3. Following *Hamidi*, it is questionable whether the "slowing of communications" for a matter of seconds is significant enough for actionable "loss of use." Unlike in *Hamidi*, however, plaintiffs allege Meta's placement of the _fbp cookie on their devices is *not* a temporary trespass (as the cookie stays until it is discovered or removed) and creates a measureable impact on the functioning of the systems' memory sufficient to satisfy damage for the trespass.

[5] *Hamidi* referred to "substantial" in quoting the Restatement in connection to measuring the necessary length of deprivation of use. *See Hamidi*, 30 Cal. 4th at 1357 ("intermeddling is actionable only if 'the chattel is impaired as to its condition, quality, or value, or [¶] ... the possessor is deprived of the use of the chattel for a substantial time." (Rest.2d Torts, § 218, pars. (b), (c).) In particular, an actionable deprivation of use "must be for a time so substantial that it is possible to estimate the loss caused thereby. A mere momentary or theoretical deprivation of use is not sufficient unless there is a dispossession....'" (citing Rest.2d Torts, § 218, pars. (b), (c)).

United States District Court
Northern District of California

Plaintiffs spend much of their opposition arguing that I should not focus on damage or loss of use because courts are increasingly adopting a "digital trespass" theory that considers access in excess of consent, as opposed to harm. Oppo. at 11-13. The main decisions plaintiffs rely on pre-date the California Supreme Court's *Hamidi* decision in 2003 and were rejected by *Hamidi* to the extent they did not require a showing of harm from the trespass. *See, e.g., eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1060 (N.D. Cal. 2000) and *Oyster Software, Inc. v. Forms Processing, Inc.*, No. C-00-0724 JCS, 2001 WL 1736382, at *1 (N.D. Cal. Dec. 6, 2001). The other cases plaintiffs rely on for their digital trespass/exceeding scope of consent theory all alleged measurable damage to plaintiffs from the trespass and do not answer the question of how measurable or significant a "minor" impact must be to support a trespass to chattels claim. *See, e.g., In re Apple Inc. Device Performance Litig.*, 347 F. Supp. 3d 434, 455 (N.D. Cal. 2018), *on reconsideration in part*, 386 F. Supp. 3d 1155 (N.D. Cal. 2019 (allegations that updates "impaired the functioning of their iPhones by substantially slowing their processing speed (by as much as 50%)"); *Parziale v. HP, Inc.*, 445 F. Supp. 3d 435, 450 (N.D. Cal. 2020 (claim stated where defendant's conduct prevented class printers "from operating, by impairing the condition of these printers, by reducing the value of these printers, and by depriving Plaintiff and Class members of the use of these printers and of their non-HP ink cartridges"); *San Miguel v. HP Inc.*, 317 F. Supp. 3d 1075, 1088 (N.D. Cal. 2018) (same harm as in *Parziale*); *Twitch Interactive, Inc. v. Does 1 Through 100*, No. 19-CV-03418-WHO, 2019 WL 3718582, at *1 (N.D. Cal. Aug. 7, 2019 (unauthorized video streamers injured plaintiff, who then had to suspend service, modify its systems, and expend resources in order to block unauthorized streamers).

No party cites caselaw that explains how significant the impact from non-temporary trespass – like the placement of the _fbp cookies at issue here – must be, other than recognizing that claims of "loss of use" must be significant following *Hamidi*. Plaintiffs have alleged measurable harm from the loss of available storage space on their devices. Compl. ¶ 495. An allegedly unconsented, surreptitious, non-temporary placement of software on devices that reduces storage has a measurable impact.

I will let the trespass to chattels claim based on the surreptitious placement of the _fbp cookie on plaintiffs' devices, resulting in a measurable decrease in the storage plaintiffs' have on their phone proceed. This is a close call involving thorny and evolving issues of state law. Discovery and expert testimony may establish that the placement of, operation of, or impact of the _fbp cookie cannot rise to a sufficient level of harm under *Hamidi*, but the impacts are better explored after discovery.

Meta's motion to dismiss is DENIED.

IV. MOTION TO STRIKE

Meta separately moves to strike Paragraph 357 of the FAC, where plaintiffs exclude from their class "health information that was obtained by Meta from Hey Favor, Inc." Meta wants, in connection with its pending motion to sever the claims asserted against in it the *Doe v. Hey Favor* case, Case No. 23-cv-0059-WHO, to have those claims wrapped into this case. The claims against Meta in the *Hey Favor* action will stay in the *Hey Favor* action and proceed along with the claims against the other defendants in that case. *See* Case No. 23-cv-0059, Dkt. No. 117.

The motion to strike is DENIED. As I reminded counsel during the hearing on this motion, the shape this consolidated class action will ultimately have – with respect to any class or classes certified or otherwise – will be determined by me at the appropriate time. Plaintiffs have defined the scope of the class in the pending FAC to their liking, but I will be the ultimate arbiter of what makes sense from a case management and litigation perspective.[6]

CONCLUSION

Meta's motion to dismiss is DENIED, except for the CLRA claim that plaintiffs voluntarily abandon.

IT IS SO ORDERED.

Dated: January 29, 2024

William H. Orrick
United States District Judge

[6] Meta should not, however, take this statement as a reason to attempt to circumscribe or refuse discovery. Defendants have not challenged the scope of the FAC – in terms of covered entities or technologies involved – and therefore this Order places no express or implied limit on discovery other than those required by Civil Rule of Civil Procedure 26(b).