

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

MIKHAIL GERSHZON,
Plaintiff, on behalf of himself
and all others similarly situated,
v.
META PLATFORMS, INC.,
Defendant.

Case No. [23-cv-00083-SI](#)

**ORDER DENYING DEFENDANT’S
MOTION TO DISMISS AND DENYING
REQUESTS FOR JUDICIAL NOTICE**

Re: Dkt. No. 31

On June 23, 2023, the Court held a hearing on defendant’s motion to dismiss the complaint. For the reasons set forth below, the Court concludes that the complaint states a claim and therefore the motion to dismiss is DENIED.

BACKGROUND

On January 6, 2023, plaintiff Mikhail Gershzon filed this class action lawsuit against Meta Platforms, Inc. (“Meta”). Gershzon alleges that Meta violated his privacy rights under federal and state law by knowingly obtaining statutorily protected personal information and communications, including names, disability information, and e-mail addresses, through the use of a “hidden tracking code” created by Meta and installed on the website of the California Department of Motor Vehicles (“DMV”). Gershzon alleges that this software code, known as the “Meta Pixel,” “sends to Meta time-stamped, personally-identifiable records of Plaintiff and Class members’ personal information, activities and communications on the [California] DMV website.” Compl. ¶ 2. Gershzon brings claims under the federal Driver’s Privacy Protection Act, 18 U.S.C. §§ 2721-2725 (“DPPA”) and the California Invasion of Privacy Act, Cal. Pen. Code § 631 (“CIPA”),

1 The following facts are taken from the complaint and assumed as true for purposes of the
2 present motion. The DMV operates the website www.dmv.ca.gov, “where users can access and
3 manage their data on file with the DMV, book virtual or in-person appointments, and prepare
4 applications for DMV services such as driver’s licenses and disabled parking placards.” Compl.
5 ¶ 27. The DMV “strongly encourages Californians to use its ‘virtual’ agents and offices, and usage
6 of DMV services online has climbed steadily in recent years.” *Id.* ¶ 28. The DMV reported 23
7 million online transactions in 2020, and that figure grew during the COVID-19 pandemic, “during
8 which time the DMV created and promoted new online options for users, allowing, for example,
9 online driver’s testing and license renewals that typically required an office visit.” *Id.*

10 Meta is “an advertising company which sells advertising space on the social media platform
11 it operates,” and “Meta’s advertising is based on sophisticated user-categorizing and targeting
12 capabilities that are fueled by the personal data or users of the social media platform and other
13 Internet users.” *Id.* ¶ 15. Meta “surveils users’ online activities both on and off Meta’s own websites
14 and apps,” which allows Meta to “make highly personal inferences about users, such as about their
15 ‘interests,’ ‘behavior,’ and ‘connections.’” *Id.* Meta “compiles information it obtains and infers
16 about Internet users and uses it to identify personalized ‘audiences’ likely to respond to particular
17 advertisers’ messaging.” *Id.* In 2021, Meta generated approximately \$114.93 billion, nearly 98%
18 of its revenue, through advertising. *Id.*

19 The Meta Pixel, originally called the Facebook Pixel, was first introduced in 2015. *Id.* ¶ 16.
20 “It is now the primary means through which Meta acquires personal information to create
21 customized audiences for its advertising business, although Meta’s public-facing descriptions of the
22 Pixel obscure and minimize this fundamental purpose of the tracking code.” *Id.* Meta characterizes
23 the Pixel as a simple “snippet of JavaScript code” that helps website owners keep track of user
24 activity on their websites, and Meta emphasizes that website managers can easily install Pixel on a
25 website. *Id.*

26 The Meta Pixel is “configured to capture a substantial amount of information by default,”
27 and since 2015 the Pixel has transmitted “HTTP header information, including the URL of each
28 page visited on a website.” *Id.* ¶ 17. In 2017 and 2018, Meta modified the Pixel code to transmit

1 more information:

2 In 2017, Meta quietly modified the Pixel code to transmit additional information
3 automatically, including “microdata” (details about the website and substance of
4 what it offers), other “contextual information” (including details about the structure
5 of a particular webpage), and “SubscribeButtonClick” information (details about
6 buttons available to click on each page including the text), which fires each time a
7 user clicks on a hyperlink or button on the webpage. Meta made these changes to
8 learn more about website users for advertising purposes. Since 2017, the Pixel has
9 been configured to gather all such data indiscriminately and by default without
10 intervention from the website owner requesting the information be tracked.

11 In 2018, Meta again modified the default operation of the Pixel to maximize the
12 private information it transmits. Meta introduced a “first-party cookie option” for
13 the Pixel, to circumvent improvements in how web browsers block third-party
14 cookies (a primary means by which Facebook historically tracked people across the
15 web). Being embedded in websites as a first-party cookie, rather than as a third-party
16 cookie, causes users’ browsers to treat that Pixel as though it is offered by the website
17 they are visiting, rather than by Meta, a third party. When the Pixel is embedded in
18 a website as a first-party cookie, the third-party cookie blocking functions of modern
19 web browsers do not inhibit the Meta Pixel’s collection of data. Operating similarly
20 to, and with the same privacy exemptions applicable to, a first party cookie became
21 another default Pixel setting in or around October 2018.

22 *Id.* ¶¶ 17-18.

23 The Meta Pixel operates in the following manner:

24 In all websites where the Pixel operates, when a user exchanges information with the
25 host of that site, Meta’s software script surreptitiously directs the user’s browser to
26 send a separate message to Meta’s servers. This second, secret transmission contains
27 the original request sent to the host website, (“GET request”), along with additional
28 data that the Pixel is configured to collect (“POST request). GET and POST requests
are communications that contain contents from both the user and from servers
associated with the website they are visiting. These transmissions are initiated by
Meta code and concurrent with the communications to and from the host website.

Meta associates the information it obtains via the Meta Pixel with other information
regarding the user, using personal identifiers that are transmitted concurrently with
other personal information the Pixel is configured to collect. For Facebook account-
holders, these identifiers include the “c user” IDs, which allow Meta to link data to
a particular Facebook account, and “xs” cookies associated with a browsing session.
For both Facebook accountholders and users who do not have a Facebook account,
these identifiers also include cookies that Meta ties to their browser, such as “datr”
and “fr” cookies.

29 *Id.* ¶¶ 20-21 (internal footnotes omitted). Meta then “feeds the vast quantities of information
30 obtained from Meta Pixels into its advertising systems, using it to identify users and their personal
31 characteristics, categorize them for Meta’s business purposes, and target them with marketing
32 messages from its advertising clients.” *Id.* ¶ 22.

33 The Meta Pixel is “embedded on and throughout the DMV website, and transmits extensive

1 information from the DMV to Meta in accordance with the Meta Pixel’s default configuration.” *Id.*
2 ¶ 29. This information includes the first name of each person who accesses their online account, *id.*
3 ¶¶ 32-35; information that a person has applied for or sought to renew a disabled person parking
4 placard or a disabled person license plate, *id.* ¶¶ 36-43; e-mail addresses, *id.* ¶¶ 45-50; and other
5 identifying information “concerning users’ interests, phone and address status, health and disability
6 status, immigration status, and concerns, all of which are personally identifying in themselves and
7 in combination . . .” *Id.* ¶ 51.

8 Meta learns, for example, when someone takes the DMV’s self-assessment for
9 driving with impaired vision, or researches the DMV’s procedures for licensing
10 people suffering from dementia. Meta also learns when someone accesses MyDMV
to update their physical address or phone number, transfer a title, or renew their
vehicle registration.

11 To illustrate one of innumerable examples in detail, if a user asks the DMV to show
12 the page for updating a phone number on the DMV site, Meta intercepts a time-
13 stamped record of the request while it is in transit to the DMV, including unique
14 identifiers for the user, and intercepts the URL transmitted back to the user by the
15 DMV. When a user logs into their MyDMV account, as they must to update their
16 phone number, Meta intercepts a record that the user logs in and successfully
17 completes two-factor authentication, then is presented with hyperlinks or buttons
18 including one to “Change Phone Number.” When a user tells the DMV what they
19 would like to do by clicking that hyperlink, Meta learns that the link “Change Phone
Number” is clicked, and obtains the descriptive URL that the DMV presents next,
namely <https://www.dmv.ca.gov/portal/update-your-phone-number/>. This page
explains the process for updating one’s phone number with the DMV, and a presents
button to “Start” the process. When a user clicks the “Start” button, Meta learns that
the button “Start” was clicked on that page, and obtains the URL that the DMV
presents next, for account verification, and so on. In short, Meta secretly watches
every step of the process, and intercepts any and all communications between users
and the DMV for its own purposes and its own use.

20 *Id.* ¶¶ 51-52. The Pixel also transmits communications MyDMV users send the DMV through the
21 search bar on the DMV website as part of the URL returning search results and answers. *Id.* ¶ 53.
22 For example, a “user who asks the DMV ‘How do I renew a disabled parking placard?’ has their
23 disability information transmitted to Meta within the URL ‘[https://www.dmv.ca.gov/portal/?s=
24 how+do+I+renew+disabled+parking+placard,](https://www.dmv.ca.gov/portal/?s=how+do+I+renew+disabled+parking+placard)’ in addition to the transmission that occurs upon
25 starting the renewal application.” *Id.*

26 Meta “assigns a unique numerical identifier to each Meta Pixel and maintains records
27 associating each Pixel with the data it transmits and the website where it is embedded.” *Id.* ¶ 30.
28 Meta has assigned numerical identifiers to the two Meta Pixels that currently operate on the DMV

1 website, and thus “Meta knows that the Meta Pixel operates on the DMV site and knows that
2 information and communication exchanged between users and the DMV are transmitted to Meta by
3 the Pixel.” *Id.*

4 Gershzon is a California resident who has had an online account with the DMV since 2019.
5 *Id.* ¶ 61. Gershzon provided his full name, e-mail address, and telephone number to the DMV in
6 order to open the account. *Id.* Gershzon has used the DMV website approximately twice a year
7 since 2019, including to apply for a disabled parking placard in 2020. *Id.* ¶ 62. Gershzon also has
8 a Facebook and/or Meta account since 2010. *Id.* ¶ 61. Gershzon alleges that the Meta Pixel tracked
9 his activities on the DMV website and the Pixel transmitted his personal information, including his
10 first name, e-mail address, and disability information, from the DMV to Meta without his consent.
11 *Id.* ¶ 63. Gershzon claims that he did not authorize Meta to obtain his personal information from
12 the DMV for any purpose, and that the DMV website explicitly states that the DMV does not collect
13 personal information for marketing, advertising or similar purposes. *Id.* ¶¶ 54-55. Gershzon brings
14 this lawsuit on behalf of “all persons who accessed their MyDMV account on the California DMV
15 website or viewed the status of a pending application to the California DMV by clicking on the
16 ‘status checker’ link in electronic correspondence from the California DMV.” *Id.* ¶ 64.

17
18 **LEGAL STANDARD**

19 A complaint must contain “a short and plain statement of the claim showing that the pleader
20 is entitled to relief,” and a complaint that fails to do so is subject to dismissal pursuant to Rule
21 12(b)(6). Fed. R. Civ. P. 8(a)(2). To survive a Rule 12(b)(6) motion to dismiss, the plaintiff must
22 allege “enough facts to state a claim to relief that is plausible on its face.” *Bell Atl. Corp. v. Twombly*,
23 550 U.S. 544, 570 (2007). This “facial plausibility” standard requires the plaintiff to allege facts
24 that add up to “more than a sheer possibility that a defendant has acted unlawfully.” *Ashcroft v.*
25 *Iqbal*, 556 U.S. 662, 678 (2009). While courts do not require “heightened fact pleading of
26 specifics,” a plaintiff must allege facts sufficient to “raise a right to relief above the speculative
27 level.” *Twombly*, 550 U.S. at 555, 570. Although “a well-pleaded complaint may proceed even if
28 it strikes a savvy judge that actual proof is improbable,” *id.* at 556, a plaintiff must include sufficient

1 “factual enhancement” to cross “the line between possibility and plausibility.” *Id.* at 557. “A
2 pleading that offers ‘labels and conclusions’ or ‘a formulaic recitation of the elements of a cause of
3 action will not do.” *Iqbal*, 556 U.S. at 678 (quoting *Twombly*, 550 U.S. at 555). “Nor does a
4 complaint suffice if it tenders ‘naked assertion[s]’ devoid of ‘further factual enhancement.’” *Id.*
5 (quoting *Twombly*, 550 U.S. at 557). “While legal conclusions can provide the framework of a
6 complaint, they must be supported by factual allegations.” *Id.* at 679.

7 8 DISCUSSION

9 I. DPPA

10 The first cause of action is brought under the Driver’s Privacy Protection Act. Compl. ¶¶
11 73-81. Gershzon alleges that Meta has violated the DPPA by obtaining personal information, such
12 as e-mail addresses and disability information, via the Meta Pixel on the DMV website, and that
13 Meta uses that information for prohibited purposes without the consent of the individuals to whom
14 the information pertains. *Id.*

15 “Congress enacted the DPPA in 1994, in response to a troubling phenomenon that occurred
16 throughout the 1980s and early 1990s—state DMVs’ practice of selling or freely disclosing drivers’
17 personal information, which led to unfortunate consequences ranging from the trivial (onslaughts of
18 random solicitations) to the tragic (the murders of several people by stalkers or ex-spouses).”
19 *Andrews v. Sirius XM Radio Inc.*, 932 F.3d 1253, 1257 (9th Cir. 2019). “At that time, ‘[u]nder the
20 law in over 30 States, it [was] permissible to give out to any person the name, telephone number,
21 and address of any other person if a drivers’ license or vehicle plate number [was] provided to a
22 State agency.’” *Id.* at 1258 (quoting 139 Cong. Rec. at S15,765 (statement of then-Sen. Biden)).
23 “Accordingly, ‘[c]oncerned that personal information collected by States in the licensing of motor
24 vehicle drivers was being released—even sold—with resulting loss of privacy for many persons,
25 Congress provided federal statutory protection’ through the DPPA.” *Id.* (quoting *Maracich v.*
26 *Spears*, 570 U.S. 48, 51-52 (2013)).

27 The first part of the DPPA focuses on a state’s own records and prohibits “[a] State
28 department of motor vehicles” from “knowingly disclos[ing] or otherwise mak[ing] available . . .

1 personal information . . . about any individual obtained by the department in connection with a
2 motor vehicle record.” 18 U.S.C. § 2721(a). The second part of the DPPA “concerns not DMVs
3 themselves, but instead those who illicitly seek information from motor vehicle records.” *Andrews*,
4 932 F.3d at 1258. Section 2722 makes it unlawful “for any person knowingly to obtain or disclose
5 personal information, from a motor vehicle record, for any use not permitted under section
6 2721(b),”¹ and “for any person to make false representation to obtain any personal information from
7 an individual’s motor vehicle record.” 18 U.S.C. § 2722. Section 2724 provides a private cause of
8 action for violations of the DPPA.

9 To state a claim against Meta under the DPPA, Gershzon must allege that Meta “(1)
10 knowingly obtained his personal information (2) from a motor vehicle record (3) for a
11 nonpermissible use.” *Andrews*, 932 F.3d at 1259.

12
13 **A. “Personal Information”**

14 The complaint alleges that Meta obtains “personal information” such as e-mail addresses,
15 names, disability information, and other personal information via the Meta Pixel. Compl. ¶ 77.

16 The DPPA defines “personal information” as “information that identifies an individual,
17 including an individual’s photograph, social security number, driver identification number, name,
18 address (but not the 5-digit zip code), telephone number, and medical or disability information, but
19 does not include information on vehicular accidents, driving violations, and driver’s status.” 18
20 U.S.C. § 2725(3). The statute further provides that “‘highly restricted personal information’ means
21 an individual’s photograph or image, social security number, medical or disability information.” *Id.*
22 § 2725(4).

23 Meta argues that Gershzon’s first name, e-mail address, and information that Gershzon
24

25 ¹ Permitted uses include “use in connection with matters of motor vehicle or driver safety
26 and theft, motor vehicle emissions, motor vehicle product alterations, recalls, or advisories,
27 performance monitoring of motor vehicles and dealers by motor vehicle manufacturers, and removal
28 of non-owner records from the original owner records of motor vehicle manufacturers.” 18 U.S.C.
§ 2721(b). The statute also allows disclosure of an individual’s personal information “[f]or use in
the normal course of business by a legitimate business,” but only “to verify the accuracy of personal
information submitted by the individual” and, “if such information as so submitted is not correct or
is no longer correct, to obtain the correct information” in limited circumstances. *Id.* § 2721(b)(3).

1 began an application for a disabled parking placard and later checked the status of that application
 2 do not “identify an individual” and therefore do not constitute “personal information” under the
 3 DPPA. Meta argues that a first name alone “sweeps in so many people that it is comparable to a ‘5-
 4 digit zip code,’” and that an e-mail address “does not always qualify as ‘personal information’—
 5 whether it does turns on the ‘content’ of the e-mail address.” Mtn. at 9 (Dkt. No. 31). Meta also
 6 argues that information that a person has applied for a disability parking placard is not “disability
 7 information” because, according to Meta, “disability information” means information about the
 8 specific nature of a person’s disability.

9 The Court is not persuaded by Meta’s arguments. As an initial matter, the statute expressly
 10 lists “name” and “medical or disability information” as types of “personal information” (and indeed
 11 specifies that “medical or disability information” is “highly restricted personal information”). A
 12 first name is a name, and information that someone has applied for a disability placard is “disability
 13 information” because it indicates that the applicant has a disability. Meta does not cite any authority
 14 for its assertion that “personal information” under the DPPA must be sufficient, on its own, to
 15 identify an individual, and courts have rejected that argument in favor of a broader reading of
 16 “personal information.” “The term ‘personal information’ should be read naturally to include facts
 17 that can identify an individual, as opposed to facts that in every instance must identify an
 18 individual.” *United States v. Hastie*, 854 F.3d 1298, 1304 (11th Cir. 2017). In *Hastie*, the Eleventh
 19 Circuit held that “[e]mail addresses fall within the ordinary meaning of ‘information that identifies
 20 an individual’” because “[t]hey can ‘prove’ or ‘establish the identity of’ an individual” and “[e]mail
 21 addresses often expressly include the account holder’s name, affiliated organization, or other
 22 identifying information.” *Id.* at 1303. The court explained,

23 This interpretation is strengthened by the material similarity between email addresses
 24 and the examples in the statute. Because “[a]ssociated words bear on one another’s
 25 meaning,” Scalia & Garner, *supra*, at 195, the examples give meaning to the term
 26 “personal information.” Email addresses are much like an online version of a
 27 physical address or a telephone number: they serve both as a way to find an individual
 28 in an online space and as a way to contact a person. . . . And the examples listed in
 the statute reveal that “information that identifies an individual” does not require that
 a single piece of information on its own be sufficient to locate a particular individual.
 An individual might have multiple phone numbers or one, and an address might be
 associated with one person or many—the ratio does not need to be 1:1.

1 *Id.* at 1303-04.

2 Similarly, in *Dahlstrom v. Sun-Times Media, LLC*, 777 F.3d 937, 940, 942 (7th Cir. 2015),
 3 the Seventh Circuit held that the definition of “personal information” under the DPPA included an
 4 individual’s approximate birth date (month and year), height, weight, hair color and eye color, even
 5 though that information does not uniquely identify an individual. The Seventh Circuit noted that
 6 “the term ‘including’—which introduces the itemized list of characteristics that constitute ‘personal
 7 information’ under the DPPA, *see* § 2725(3)—is typically ‘illustrative and not limitative.’” *Id.* at
 8 943 (quoting *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 577 (1994)). The court stated that
 9 an “expansive reading” of “personal information” was supported by the text of the statute, noting
 10 that “even though medical and disability information do not uniquely pertain to a single individual,
 11 they are included in a subcategory of ‘highly restricted personal information,’ which receives even
 12 greater protection under the DPPA.” *Id.* at 944 (citing 18 U.S.C. § 2724(4)). An expansive
 13 interpretation of “personal information” also served the public safety purpose of the DPPA because
 14 “[a]lthough a potential stalker would likely require information beyond hair and eye color to
 15 positively identify his victim, details regarding any pertinent physical feature would make such
 16 identification easier.” *Id.* In addition, the court found that “[m]uch of the information at issue here,
 17 particularly details regarding an individual’s age, height, and weight, could conceivably be of great
 18 interest to businesses . . . seeking to market their products or services to targeted audiences. While
 19 protection against commercial solicitation may not be as fundamental as the Act’s public safety
 20 objectives, excluding these categories of information from the DPPA’s definition of ‘personal
 21 information’ would likely contravene legislative intent.” *Id.* at 944-45.

22 Meta argues that *Dancel v. Groupon, Inc.*, 949 F.3d 999 (7th Cir. 2019), holds that an e-mail
 23 address does not always qualify as “personal information” and that whether it does or not depends
 24 on the content of the e-mail address. However, *Dancel* involved the Illinois Right of Privacy Act
 25 (“IRPA”), not the DPPA, and arose in the context of class certification. The IRPA prohibits the “(1)
 26 appropriation of one’s identity, (2) without consent, (3) for another’s commercial benefit.” *Id.* at
 27 1008. In *Dancel*, the Seventh Circuit affirmed the district court’s denial of class certification in a
 28 case alleging that the defendant’s commercial use of the plaintiff’s Instagram username violated the

1 IRPA, holding that the question of “whether any given username identifies that specific individual
2 who is behind that username” and thus is part of “an individual’s identity” under the IRPA could
3 not be established with common proof on a classwide basis. *Id.* at 1009. In reaching that holding,
4 the Seventh Circuit distinguished *Hastie* by stating that “the [*Hastie*] court did not hold that e-mail
5 addresses categorically identify an individual, only that they often did, and they often did so only
6 because of their content, not their inherent nature as e-mail addresses.” *Id.* at 1008. *Dancel* did not
7 hold that e-mail addresses are not “personal information” under the DPPA, and as discussed above,
8 courts have held that “personal information” under the DPPA need only be “facts that can identify
9 an individual, as opposed to facts that in every instance must identify an individual.” *Hastie*, 854
10 F.3d at 1304.

11 The reasoning of *Hastie* and *Dahlstrom* apply here. A first name, e-mail address, and
12 information that someone has applied for a disability parking placard are “facts that can identify an
13 individual,” *Hastie*, 854 F.3d at 1304, and as such the Court finds that Gershzon has alleged that
14 Meta obtained “personal information” within the meaning of the DPPA.²

15
16 **B. “From a Motor Vehicle Record”**

17 The complaint alleges that Meta obtains personal information from the DMV via the Meta
18 Pixel, and that the information comes “from a motor vehicle record” because the information
19 “derives from the DMV database.” Compl. ¶ 78.

20
21 ² To the extent Meta asserts that Gershzon does not have standing to challenge Meta’s
22 alleged improper acquisition of other types of “personal information” from the DMV website, the
23 Court disagrees. Gershzon brings this case as a class action and he alleges, *inter alia*, that “[a]ctive
24 at all times on nearly every page of the DMV website, the Meta Pixel also broadly transmits to Meta
25 other information from the DMV that identifies website users,” including “information concerning
26 users’ interests, phone and address status, health and disability status, immigration status, and
27 concerns, all of which are personally identifying in themselves” Compl. ¶ 51. Because
28 Gershzon has alleged that Meta has improperly obtained his “personal information” from the DMV
website via the Meta Pixel, he may pursue those claims. *Pichler v. UNITE*, 542 F.3d 380, 391-92
(3d Cir. 2008), cited by Meta, is inapposite. In *Pichler*, two women and their husbands alleged
DPPA violations based upon a union searching the husbands’ motor vehicle records; the search
revealed the couples’ shared addresses. The Third Circuit affirmed the dismissal of the wives’
claims, holding that “individuals . . . who are not specifically identified in a motor vehicle record,
have no legally protected privacy interest under the DPPA.” *Id.* at 391. Here, Gershzon has alleged
that Meta obtained his personal information from the DMV, and thus he has standing to assert a
claim about the improper acquisition of “personal information” from the DMV website.

1 Meta contends that Gershzon has not plausibly alleged that Meta obtained any of his
2 information “from a motor vehicle record.” The DPPA defines a “motor vehicle record” as a “record
3 that pertains to a motor vehicle operator’s permit, motor vehicle title, motor vehicle registration, or
4 identification card issued by a department of motor vehicles.” 18 U.S.C. § 2725(1). Meta argues
5 that a disabled person placard (or application for a placard) does not fit within this definition because
6 “[d]isabled person placards provide people with disabilities certain parking privileges” and “these
7 privileges are distinct from the person’s permit, the title or registration for that person’s car, and that
8 person’s ID card.” Mtn. at 10-11. As support, Meta relies on *Lake v. Neal*, 585 F.3d 1059 (7th Cir.
9 2009), in which the Seventh Circuit held that a voter registration form filled out at a state DMV was
10 not a “motor vehicle record” because a voter form does not pertain to any of the DMV documents
11 listed in § 2725(1) of the DPPA. *Id.* at 1061 (“Other than the fact that it is filled out simultaneously
12 with a driver’s license application, the voter form has nothing to do with, nor does it ‘pertain’ to, a
13 motor vehicle operator’s permit.”)

14 *Lake* does not aid Meta. Unlike a voter registration form, a disability parking placard (and
15 an application for such a placard) does pertain to a motor vehicle operator’s permit. If a person with
16 a disability is licensed to drive in California and requires an accommodation in the form of a disabled
17 parking placard, the person must apply for such a placard. Disability parking placards are only used
18 in connection with driving, unlike a voter registration form which has no connection to driving.
19 Thus, a disabled parking placard “pertains to a motor vehicle operator’s permit.”

20 Meta also argues that the information that Meta allegedly received cannot be described as
21 having come from a “record.” Meta argues that Gershzon has not alleged that Meta obtains
22 preexisting information maintained by the DMV, and instead that his only allegations are that the
23 DMV allegedly sends Meta information about Gershzon’s interactions with the DMV’s website
24 using GET and POST requests. Meta argues that GET and POST requests are not motor vehicle
25 “records” because they are HTTP requests generated when an online user clicks on a link or button,
26 and they exist completely independent from the DMV’s records. Meta argues that these GET and
27 POST requests are not “information about [plaintiff] that is maintained by [the DMV],” *Andrews*,
28 932 F.3d at 1260, and thus they are not a “record” under the DPPA. Similarly, Meta argues that

1 the pieces of code that the DMV allegedly sends Meta—i.e., “unique identifiers like the c_user ID,
2 datr, xs, and fr cookies,” Compl. ¶ 43—exist independently of any “motor vehicle records.” Finally,
3 Meta argues that Gershzon does not allege that Meta received information “from” a motor vehicle
4 record because “the information Meta allegedly received when plaintiff *began* a placard application
5 was received *before* the creation of a motor vehicle record, and all the information Meta allegedly
6 received (both when plaintiff began his application and later checked its status) was allegedly
7 derived from plaintiff’s *own online interactions* with the DMV website – not from any particular
8 *record.*” Mtn. at 11-12 (emphasis in original).

9 The Court is not persuaded by Meta’s arguments and finds that at most they raise factual
10 questions that are not amenable to resolution at the pleadings stage. *Andrews*, upon which Meta
11 relies, is factually distinguishable. In *Andrews*, the Ninth Circuit held that Sirius XM Radio did not
12 violate the DPPA by obtaining information from an individual’s driver’s license and a form provided
13 in connection with the purchase of vehicle because that information did not come from the DMV.
14 *Andrews*, 932 F.3d at 1260 (“[W]e conclude that where, as here, the initial source of personal
15 information is a record in the possession of an individual, rather than a state DMV, then use or
16 disclosure of that information does not violate the DPPA.”). The court held that this interpretation
17 was consistent with the purpose of the DPPA, which was “concern[ed] with the release of personal
18 information *by States.*” *Id.* (emphasis in original). Unlike *Andrews*, where the defendant obtained
19 personal information from sources other than a DMV, here Gershzon alleges that Meta obtained his
20 personal information from the DMV website and that the DMV maintained this information after
21 Gershzon provided it to the DMV through his “MyDMV” online account. These allegations are
22 sufficient to show that Meta obtained Gershzon’s information “from a motor vehicle record.”

23
24
25
26
27
28

C. Improper Purpose

The complaint alleges,

Meta obtains Plaintiff’s and Class members’ personal information from the DMV in a manner that is not consistent with any permissible purpose under 18 U.S.C. § 2721(b). On information and belief, Meta uses the personal information it obtains from the DMV for purposes that are prohibited, including for purposes of profiling, categorizing, and deriving “insights” about consumers, including through “Core

1 Audiences,” “Lookalike audiences,” and “Custom Audiences”; targeting and serving
2 advertisements to Meta platform users and non-users; improving Meta’s profiling
3 and categorizing algorithms; improving Meta platforms; and competing with other
4 advertising companies, without express consent of the individuals to whom the
5 information pertains.

6 Compl. ¶ 79.

7 Meta argues that Gershzon has failed to plausibly allege that Meta obtained his personal
8 information for an improper purpose, and that several of the DPPA’s exceptions for permissible
9 uses “plainly apply here.” Mtn. at 13. According to Meta, it is obvious from Gershzon’s allegations
10 that Meta used or obtained personal information for the permissible purpose of assisting the DMV
11 in carrying out its functions, such as market research activities. *See* 18 U.S.C. § 2721(b)(2) (personal
12 information may be disclosed “[f]or use in connection with . . . motor vehicle research activities,
13 including survey research . . .”). Meta also argues that Gershzon consented to the use of his
14 personal information by agreeing to Meta’s Privacy Policy, thus rendering Meta’s use of any data it
15 received about Gershzon permissible under 18 U.S.C. § 2721(b)(13).³

16 The Court is not persuaded by Meta’s arguments. The complaint expressly alleges that Meta
17 obtains individuals’ personal information via the Meta Pixel for the improper purpose of creating
18 customized audiences for its advertising business. Compl. ¶¶ 15-17, 21-26, 79. Whether Meta in
19 fact had a permissible purpose in obtaining and using personal information from the DMV website
20 raises factual questions to be resolved on summary judgment or at trial. The complaint also alleges
21 that Gershzon did not consent to Meta obtaining his information from the DMV website. *Id.* ¶ 62.
22 These allegations are plausible and sufficient at this stage of litigation.

23 ³ Meta seeks judicial notice of Meta’s Privacy Policy and Cookies Policy, and argues that a
24 reasonable person viewing these disclosures would understand that Meta collects information about
25 user activities on third-party websites and uses that information for advertising purposes. Meta also
26 seeks judicial notice of the DMV’s Conditions of Use, and argues that a reasonable person reading
27 these disclosures would understand that the DMV collects personal information and uses it for
28 “customer service” and “statistical analysis,” and thus would understand that his information would
29 be shared by the DMV with third parties for these purposes. Gershzon opposes Meta’s request for
30 judicial notice.

31 The Court DENIES Meta’s request for judicial notice. The Court will not consider
32 documents beyond the pleadings and draw inferences from those documents in Meta’s favor. *See*
33 *Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 999 (9th Cir. 2018) (“If defendants are
34 permitted to present their own version of the facts at the pleading stage—and district courts accept
35 those facts as uncontroverted and true—it becomes near impossible for even the most aggrieved
36 plaintiff to demonstrate a sufficiently ‘plausible’ claim for relief.”). Meta may renew its arguments
37 about consent and permissible purposes on a fuller factual record.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

D. “Knowingly”

Meta contends that Gershzon has failed to satisfy the “knowingly” requirement because the complaint does not allege that Meta knew the DMV was sending it “personal information” from a “motor vehicle record” for an improper purpose. Meta argues that “knowingly” “requires knowledge that the defendant’s conduct satisfied all elements of the offense,” and thus that Gershzon must allege that Meta essentially knew it was violating the DPPA by collecting and using personal information from the DMV website. Reply at 10.

The DPPA provides, “A person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains, who may bring a civil action in a United States district court.” 18 U.S.C. § 2724(a). District courts have held that as a matter of statutory construction, the “knowingly” requirement applies to the first element of a DPPA claim – “obtains, discloses or uses personal information.” *See Wilcox v. Swapp*, 330 F.R.D. 584, 594 (E.D. Wash. 2019) (“Because the rest of the statute is offset by commas, the ‘knowingly’ requirement in section 2724(a) only applies to the portion before the commas, which is the first element of the statute.”); *Wiles v. Worldwide Info., Inc.*, 809 F. Supp. 2d 1059, 1081 (W.D. Mo. 2011) (“The only reason to use commas to isolate the clause ‘from a motor vehicle record’ is to confine the adverb ‘knowingly’ to modifying the act of obtainment, disclosure, or use.”); *Rios v. Direct Mail Express*, 435 F. Supp. 2d 1199, 1205 (S.D. Fla. 2006) (“Thus, under the express language of the DPPA the term ‘knowingly’ only modifies the phrase ‘obtains, discloses, or uses personal information.’”). Further, although the Ninth Circuit has not expressly addressed the question, when the court has described the elements of a DPPA claim, it has applied “knowingly” to the first element. *See Andrews*, 932 F.3d at 1259 (“To prevail on his DPPA claim, Andrews must satisfy § 2722(a) and prove that (1) Sirius XM knowingly obtained his personal information (2) from a motor vehicle record (3) for a nonpermissible use.”); *Howard v. Criminal Info. Servs., Inc.*, 654 F.3d 887, 890 (9th Cir. 2011) (“Section 2724(a) sets forth the three elements giving rise to liability, i.e., that a defendant (1) knowingly obtained, disclosed or used personal information, (2) from a motor vehicle record, (3)

1 for a purpose not permitted.”) (internal citation and quotation marks omitted).

2 Meta does not cite any cases interpreting the DPPA which hold that “knowingly” applies to
3 all three elements of the statute. Meta cites *Enslin v. The Coca-Cola Co.*, 136 F. Supp. 3d 654 (E.D.
4 Pa. 2015), but that case does not support Meta’s position and actually undercuts it. In *Enslin*, a
5 former employee sued Coca-Cola under the DPPA, alleging that he provided Coca-Cola with
6 authorization to obtain his personal information from the DMV, and that this personal information
7 was stored on company laptops that were subsequently stolen, thus constituting a “knowing
8 disclosure” of personal information under the DPPA. The court dismissed the plaintiff’s DPPA
9 claim, holding that a “‘knowing disclosure’ of PDI requires the defendant to take some ‘voluntary
10 action’ to disclose the information,” and that “[t]he theft of Plaintiff’s PDI cannot be characterized
11 as a ‘voluntary action’ taken by the Coke Defendants to disclose that information.” *Id.* at 670-71.
12 In reaching that holding, the court stated that the “knowing” requirement “does not mean, however,
13 that the disclosing party knows that the disclosure is potentially illegal.” *Id.* at 670. The other cases
14 cited by Meta do not interpret the DPPA. In the absence of any contrary authority, the Court agrees
15 with the other courts which have held that “knowingly” applies to the first element of the DPPA.

16 Gershzon alleges that Meta “assigns a unique numerical identifier to each Meta Pixel and
17 maintains records associating each Pixel with the data it transmits and the website where it is
18 embedded,” that Meta has assigned numerical identifiers to the two Meta Pixels that currently
19 operate on the DMV website, and thus that “Meta knows that the Meta Pixel operates on the DMV
20 site and knows that information and communication exchanged between users and the DMV are
21 transmitted to Meta by the Pixel.” Compl. ¶¶ 30, 76. This is sufficient to show that Meta
22 “knowingly obtains, discloses or uses personal information” under the DPPA.

23
24 **II. CIPA**

25 The second cause of action is brought under the California Invasion of Privacy Act
26 (“CIPA”), Cal. Penal Code § 630 *et seq.* Penal Code Section 631(a) provides,

27 Any person who, by means of any machine, instrument, or contrivance, or in any
28 other manner, intentionally taps, or makes any unauthorized connection, whether
physically, electrically, acoustically, inductively, or otherwise, with any telegraph or

1 telephone wire, line, cable, or instrument, including the wire, line, cable, or
2 instrument of any internal telephonic communication system, or who willfully and
3 without the consent of all parties to the communication, or in any unauthorized
4 manner, reads, or attempts to read, or to learn the contents or meaning of any
5 message, report, or communication while the same is in transit or passing over any
6 wire, line, or cable, or is being sent from, or received at any place within this state;
7 or who uses, or attempts to use, in any manner, or for any purpose, or to communicate
8 in any way, any information so obtained, or who aids, agrees with, employs, or
9 conspires with any person or persons to unlawfully do, or permit, or cause to be done
10 any of the acts or things mentioned above in this section, is punishable by a fine not
11 exceeding two thousand five hundred dollars (\$2,500), . . .

12 “Subdivision (a) of section 631 prescribes . . . three distinct and mutually independent
13 patterns of conduct: intentional wiretapping, wilfully attempting to learn the contents or meaning of
14 a communication in transit over a wire, and attempting to use or communicate information obtained
15 as a result of engaging in either of the previous two activities.” *Tavernetti v. Superior Ct.*, 22 Cal.
16 3d 187, 192 (1978). “In enacting this statute, the Legislature declared in broad terms its intent ‘to
17 protect the right of privacy of the people of this state’ from what it perceived as ‘a serious threat to
18 the free exercise of personal liberties [that] cannot be tolerated in a free and civilized society.’”
19 *Ribas v. Clark*, 38 Cal. 3d 355, 359, 696 P.2d 637 (1985) (quoting (Cal. Penal Code § 630)).

20 The complaint alleges that Meta “tracked and intercepted Plaintiff’s and Class members’
21 internet communications exchanged with the DMV through the DMV website,” that Meta did so
22 without consent from all parties to the communications, that Meta “intended to learn, and did learn,
23 some meaning of the content in the communications including without limitation in the URLs,
24 search queries, and other content exchanged between Class members and the DMV on the DMV
25 website,” and that Meta used the Meta Pixel and other “machines, instruments and contrivances” to
26 track and intercept the communications. Compl. ¶¶ 82-92.

27
28 **A. Intent**

Meta argues that Gershzon does not allege that Meta intended to wiretap a conversation
without his consent. In addition, relying on documents outside the pleadings,⁴ Meta asserts that it
did not intentionally or willfully intercept Gershzon’s information because third parties decide

⁴ As stated earlier, the Court finds it inappropriate to consider these extrinsic documents on
this motion to dismiss.

1 whether to install the Meta Pixel, and Meta tells third parties not to send it any information unless
2 it has the legal right to do so.

3 Gershzon responds that Meta’s intent argument improperly focuses on the “wiretapping”
4 provision of CIPA (prong one of § 631(a)), while the complaint alleges violations of the second and
5 third prongs of CIPA – that Meta willfully read communications between Gershzon and the DMV
6 (second prong) and that Meta used the information it obtained (third prong). Gershzon also argues
7 that the complaint does allege that Meta read Gershzon’s communications by design, not
8 accidentally, and that willfulness and intent are fact questions.

9 Because Gershzon is not alleging a wiretapping claim, Meta’s arguments about what is
10 needed to plead such a claim are moot. Further, contrary to Meta’s assertions, the complaint alleges
11 far more than inadvertent receipt of information because Gershzon alleges that that Meta designed
12 the Meta Pixel “to maximize the private information it transmits,” that the Pixel is installed on the
13 DMV website, that personal information and communications are transmitted to Meta via the Pixel
14 on the DMV website, that Meta is aware that this information is being transmitted, and that “Meta
15 intended to learn, and did learn, some meaning of the content in the communications . . .” Compl.
16 ¶¶ 18, 88. These allegations, along with the other detailed allegations in the complaint, are sufficient
17 and non-conclusory, and whether Meta in fact acted willfully is a question of fact to be resolved on
18 a factual record.

19

20 **B. Consent**

21 Meta contends that Gershzon does not plausibly allege that he did not consent to Meta’s
22 receipt of his data from the DMV. For the reasons stated earlier, the Court finds that Gershzon’s
23 allegations are sufficient and that Meta’s arguments raise factual questions that cannot be resolved
24 on the pleadings.

25

26 **C. “Contents” of communications**

27 Section 631(a) prohibits “wilfully attempting to learn the contents or meaning of a
28 communication over a wire.” *Tavernetti*, 22 Cal. 3d at 192. The Ninth Circuit has held that “the

1 term ‘contents’ refers to the intended message conveyed by the communication, and does not include
 2 record information regarding the characteristics of the message that is generated in the course of the
 3 communication.” *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014).⁵ “Generally,
 4 customer information such as a person’s name, address, and subscriber number or identity is record
 5 information, but it may be contents when it is part of the substance of the message conveyed to the
 6 recipient.” *Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1093 (N.D. Cal. 2022) (citing *Zynga*,
 7 750 F.3d at 1104, 1108-09). “Similarly, URLs⁶ are record information when they only reveal a
 8 general webpage address and basic identification information, but when they reproduce a person’s
 9 personal search engine queries, they are contents.” *Id.*; see also *In re Google Inc. Cookie Placement*
 10 *Consumer Litig.*, 806 F.3d 125, 137 (3d Cir. 2015) (“In essence, addresses, phone numbers, and
 11 URLs may be dialing, routing, addressing, or signaling information, but only when they are
 12 performing such a function. If an address, phone number, or URL is instead part of the substantive
 13 information conveyed to the recipient, then by definition it is ‘content.’”).

14 “Courts employ a contextual ‘case-specific’ analysis hinging on ‘how much information
 15 would be revealed’ by the information’s tracking and disclosure.” *Id.* at 1092 (quoting *Google*
 16 *Cookie Placement*, 806 F.3d at 137-38). Thus, in *In re Facebook, Inc. Internet Tracking Litigation*,
 17 the Ninth Circuit held that URLs that could disclose a user’s search terms were “contents” because
 18 they could provide “significant information regarding the user’s browsing history” and divulge “a
 19 user’s personal interests, queries, and habits on third-party websites operating outside of Facebook’s
 20 platform.” 956 F.3d at 596, 605; see also *United States v. Forrester*, 512 F.3d 500, 510 n.6 (9th

21
 22
 23 ⁵ *Zynga* interpreted the federal Wiretap Act. “The analysis for a violation of CIPA is the
 24 same as that under the federal Wiretap Act.” *Cline v. Reetz-Laiolo*, 329 F. Supp. 3d 1000, 1051
 25 (N.D. Cal. 2018).

26 ⁶ A website’s “URL” is its Uniform Resource Locator. “URLs both identify an internet
 27 resource and describe its location or address.” *In re Facebook Inc., Internet Tracking Litig.*, 956
 28 F.3d 589, 596 (9th Cir. 2020). “[W]hen users enter URL addresses into their web browser using the
 ‘http’ web address format, or click on hyperlinks, they are actually telling their web browsers (the
 client) which resources to request and where to find them.” *In re Zynga Privacy Litig.*, 750 F.3d at
 1101. “Thus, the URL provides significant information regarding the user’s browsing history,
 including the identity of the individual internet user and the web server, as well as the name of the
 web page and the search terms that the user used to find it. In technical parlance, this collected URL
 is called a ‘referrer header’ or ‘referrer.’” *Facebook Tracking Litig.*, 956 F.3d at 956.

1 Cir. 2008) (stating that warrantless capture of URLs generally “might be more constitutionally
2 problematic” than warrantless capture of IP addresses because “[a] URL, unlike an IP address,
3 identifies the particular document within a website that a person views and thus reveals much more
4 information about the person’s [i]nternet activity.”). Similarly, in *Google Cookie Placement* the
5 Third Circuit held that the plaintiffs stated a claim under the federal Wiretap Act where they alleged
6 “a broad scheme in which the defendants generally acquired and tracked the plaintiffs’ internet
7 usage” because “at a minimum—some queried URLs qualify as content.” *Google Cookie*
8 *Placement*, 806 F.3d at 139; *see also Wesch v. Yodlee, Inc.*, Case No. 20-cv-05991-SK, 2021 WL
9 1399291, at *4 (N.D. Cal. Jul. 19, 2021) (holding individuals’ bank transaction histories constituted
10 “contents” because they “reveal personal details of Plaintiffs’ lives and their expenditures.”). By
11 contrast, in *Hammerling* Judge Breyer held that Google’s collection of “usage and engagement”
12 data – the average number of days that users were active on certain apps and the user’s total time
13 spent on non-Google apps – did not violate CIPA because “[w]hile Google might infer a user’s traits
14 and habits from the fact that this user uses non-Google apps designed for a specific purpose, the
15 extent of that inference is limited because Plaintiffs do not allege Google can read the specific
16 information (i.e., content) that a user inputs.” *Hammerling*, 615 F. Supp. 3d at 1093.

17 Meta argues that none of the information that Meta allegedly received from plaintiff
18 constitutes “contents” because it is “record information” about a user’s communication, not contents
19 of the communication.

20 The Court concludes that Gershzon has sufficiently alleged that the Meta Pixel transmits
21 “contents” of communications to Meta. The complaint alleges that the Meta Pixel is embedded on
22 and throughout the DMV website, that the Pixel transmits to Meta the URL of each page visited on
23 a website, and that, among other things, Meta obtained information showing that Gershzon
24 communicated with the DMV in order to apply for a disability parking placard and later to check on
25 the status of that application. This type of information is substantive and personal, as it shows that
26 Gershzon has a disability (or believes that he has a disability) and that he requires a disability parking
27 placard. Similar to the “broad scheme” in *Google Cookie Placement*, Gershzon alleges that the
28 Meta Pixel is “[a]ctive at all times on nearly every page of the DMV website,” and that it “broadly

1 transmits to Meta other information from the DMV that identifies website users,” including
2 “information concerning users’ interests, phone and address status, health and disability status,
3 immigration status and concerns.” Compl. ¶ 51. At least some of this information – such as
4 information someone is disabled – constitutes “contents” under CIPA, and thus the allegations are
5 sufficient at the pleadings stage.

6

7 **D. Statute of Limitations**

8 Meta contends that if the Court allows the CIPA claim to proceed, the claim should be
9 limited to conduct occurring within the one year statute of limitations. Gershzon responds that there
10 is no dispute that the complaint is timely, and that whether the statutes of limitation are tolled “as a
11 result of Meta’s knowing and active concealment of its conduct” as alleged in the complaint, *see*
12 Compl ¶¶ 56-60, is a factual question that requires discovery.

13 The Court agrees with plaintiff that the question of tolling cannot be decided on the
14 pleadings, and that Meta can renew its arguments on a fuller factual record.

15

16 **CONCLUSION**

17 For the foregoing reasons, the Court concludes that plaintiff has stated claims under the
18 DPPA and CIPA, and therefore Meta’s motion to dismiss is DENIED. The Court shall set a pretrial
19 schedule at the September 1, 2023 case management conference.

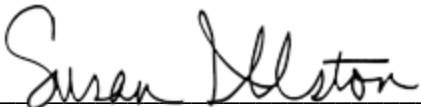
20

21 **IT IS SO ORDERED.**

22

23 Dated: August 22, 2023

24



SUSAN ILLSTON
United States District Judge

25

26

27

28