Orin Snyder (*pro hac vice*)
osnyder@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
200 Park Avenue
New York, NY 10166-0193
Telephone: 212.351.4000
Facsimile: 212.351.4035

Joshua S. Lipshutz (SBN 242557)
jlipshutz@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306
Telephone: 202.955.8500
Facsimile: 202.467.0539

Kristin A. Linsley (SBN 154148)
klinsley@gibsondunn.com
Brian M. Lutz (SBN 255976)
blutz@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
555 Mission Street, Suite 3000
San Francisco, CA 94105-0921
Telephone: 415.393.8200
Facsimile: 415.393.8306

Attorneys for Defendant Facebook, Inc. and Non-Prioritized Defendants Mark Zuckerberg and Sheryl Sandberg

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

IN RE: FACEBOOK, INC. CONSUMER PRIVACY USER PROFILE LITIGATION,

This document relates to:

ALL ACTIONS

CASE NO. 3:18-MD-02843-VC

MEMORANDUM OF LAW IN SUPPORT OF MOTION OF DEFENDANT FACEBOOK, INC. TO DISMISS PLAINTIFFS' CONSOLIDATED COMPLAINT

Judge: Hon. Vince Chhabria
Courtroom 4, 17th Floor
Hearing Date: January 23, 2019
Hearing Time: 10:30 a.m.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutional Provisions, Statutes & Rules

Other Authorities

I. INTRODUCTION

Ever since the March 2018 news reports about Cambridge Analytica's misuse of Facebook users' data, Plaintiffs have been trying to find a viable cause of action against Facebook. In these seven months, Plaintiffs have had the benefit of 38 different complaints, the collective wisdom of dozens of law firms, extensive public reporting, and discovery from Facebook consisting of nearly 10,000 pages. They even recruited new named plaintiffs. But Plaintiffs' 255-page complaint is little more than a broadside against Facebook's business model: a lengthy description of how Facebook works, followed by a kitchen sink-like lobbing of 50 claims—all in the hopes that something, anything, sticks.

The Cambridge Analytica events drew public attention to the policy implications of sharing data on the Internet, sparking an important and ongoing discussion about the ways in which people's data can be used (and misused). Facebook has acknowledged that it must do better to regain people's trust, and it has already taken a number of steps to do so, including product changes, additional disclosures to users, and significant investments around privacy, security, and integrity. But Facebook's role in these events does not give rise to a viable cause of action. No court has ever accepted the far-fetched legal theories invented by Plaintiffs in this case, and this Court should dismiss the Complaint in its entirety.

Plaintiffs *lack standing* because they have not suffered any Article III injury. Despite repeated colloquies with the Court about the challenge of proving standing and whether users suffered any concrete or particularized harm, the Complaint still fails to articulate *any* cognizable harm suffered by *any* Facebook user—let alone the named Plaintiffs themselves. In the initial wave of complaints, Plaintiffs alleged diverse and bizarre theories of harm, ranging from drained cell phone batteries to the election of President Trump. Recognizing that those allegations did not come close to establishing Article III standing, the consolidated Complaint takes a different approach, this time alleging that the sharing of data is, by itself, enough to satisfy the standing requirements. But Plaintiffs do not describe *any* specific content they shared on Facebook, much less allege that third parties obtained such content as a result of any of the allegedly improper practices discussed in the Complaint. Plaintiffs do not

claim that *any* app developer (other than Dr. Aleksandr Kogan) or electronic device maker (like Microsoft or Apple) obtained their data, and they identify only a single instance in which Dr. Kogan's app obtained their data—without specifying whether their privacy settings were set to allow such sharing. Nor do Plaintiffs explain how the Cambridge Analytica events or the alleged sharing of data with any third-party apps or device makers led them, personally, to suffer any cognizable injury. Indeed, they do not explain how the alleged conduct described in the Complaint caused injury to *any* Facebook users—only that it supposedly led to some users being served more tailored ads and enabled some users to use Facebook on their mobile devices, neither of which is "harm" at all.

Facebook users *consent* to sharing their data with third-party apps and device manufacturers. The documents incorporated into the Complaint by reference demonstrate that Facebook users consent to their data being shared with third-party apps and have the option to limit such sharing or turn it off entirely. Facebook's Terms of Service and Data Use Policy make this clear. Plaintiffs admit, for example, that "Facebook provided 'Privacy Settings' to users, and made them prominent and accessible." Compl. ¶ 9. They allege that Facebook "allowed external developers to reach out to Facebook users and request access [to] a large chunk of their personal data," *id*. ¶ 118, but admit that apps could obtain user data only "[a]s long as the request complies with the user's and/or friends' privacy settings," *id*. ¶¶ 121, 122. They even provide page after page, screenshot after screenshot, depicting the privacy settings that Facebook account holders can use to specify precisely which types of information should be shared with whom—friends, apps, the public—and even to "turn off Platform" altogether. *Id*. ¶¶ 185–201. The problem with Cambridge Analytica—the only entity named by Plaintiffs as allegedly obtaining their data—was that the app developer, Dr. Kogan, obtained the user data (with consent) but then sold it to Cambridge Analytica in violation of Facebook's policies. And even that risk was fully disclosed. As Plaintiffs acknowledge (*e.g.*, *id.* ¶¶ 560–561), Facebook's Data Use Policy told users that "games, applications and websites are created and maintained by other businesses and developers who are not part of, or controlled by, Facebook," *e.g.*, Duffey Decl. ("D.D."), Ex. 45 at 8, and the Statement of Rights and Responsibilities clearly and unambiguously waived claims based on third-party conduct, *e.g.*, D.D., Ex. 21 at 3.

The Complaint also attempts to construct a cause of action out of Facebook's sharing of data

with electronic device manufacturers, such as Microsoft and Apple. But in binding admissions, Plaintiffs plead themselves out of court by acknowledging that such sharing was necessary to allow users to experience Facebook on their mobile phones and other devices. *See* Compl. ¶ 171. Again, Facebook's Data Use Policy made this common sense reality crystal clear, stating: "We give your information to the people and companies that help us provide, understand, and improve the services we offer. For example, we may use outside vendors to help host our website, serve photos and videos, process payments," etc. D.D., Ex. 45 at 15 (Dec. 11, 2012 Data Use Policy); Compl. ¶¶ 281–283.

Facebook users *consent* to targeted advertising. Advertising-supported services are a common and well-known feature on the Internet and people know that Facebook uses the data it collects to show relevant ads to them. Plaintiffs themselves admit "[t]here is nothing wrong with targeted advertising." Compl. ¶ 110. Facebook's Data Use Policy stated that Facebook "get[s] data from [its] advertising partners, customers, and other third parties that helps [it] (or them) deliver ads," that Facebook "may also put together data about you to serve you ads that might be more relevant to you," and that "[w]hen an advertiser creates an ad [on Facebook], they are given the opportunity to choose their audience by location, demographics, likes, keywords, and any other information we receive or can tell about you and other users." D.D., Ex. 45 at 2, 3, 11 (Dec. 11, 2012 Data Use Policy). As Plaintiffs acknowledge, targeted advertising works by connecting advertisers with users who have certain interests—not by disclosing such data to advertisers. And, to the extent Plaintiffs complain about political ads resulting from Cambridge Analytica's activities, no plaintiff alleges to have viewed any such ad, and Cambridge Analytica did not obtain user data directly from Facebook—only from Kogan, in violation of Facebook's policies.

* * *

Dismissing this case does not mean Plaintiffs are left without recourse. The very kind of policy and social issues raised in the Complaint—how to ensure consumers understand and utilize privacy settings (Compl. ¶¶ 9, 10, 182), how many clicks it should take to opt out of data sharing (*id.* ¶¶ 200–201), how to know when advertising is *too* targeted (*id.* ¶ 367)—are the subject of Congressional hearings, regulatory inquiries, and robust public discourse. That is where those discussions

belong, *see* U.S. Const. arts. I & II, not on a piecemeal basis in courts charged with enforcing existing statutory and common laws that do not give rise to any viable legal claim against Facebook.

II. STATEMENT OF ISSUES TO BE DECIDED

1. Whether the complaint should be dismissed under Rule 12(b)(1) because Plaintiffs lack Article III standing.

2. Whether the complaint should be dismissed under Rule 12(b)(6) as to Facebook for failure to state a claim.

III. BACKGROUND

The lawsuits comprising this MDL were first filed in March 2018,[1] after *The Guardian* and *The New York Times* each reported that Cambridge Analytica—a data analytics company that had worked with the Trump campaign (and previously worked with the Ted Cruz campaign)—had improperly obtained data regarding millions of Facebook users.[2] The articles explained that Cambridge Analytica obtained this information from a developer named Aleksandr Kogan who, along with his company GSR, created an application called "thisisyourdigitallife" in 2013. Compl. ¶ 132. As with other developers that offer apps integrated with Facebook's platform, Kogan obtained data from users who authorized the app, and some limited data about those users' friends—*if* those friends "had their privacy settings set to allow it." *Id.* ¶ 138. Then, in contravention of Facebook's policies and the terms of use to which he agreed, Kogan sold this data to Cambridge Analytica. *Id.* ¶ 142. Cambridge Analytica then allegedly used the information to develop a targeted ad campaign through which it served political ads to Facebook users. *Id.* ¶¶ 5, 21–88, 135, 144, 386, 538.

None of this was news when the articles were published in 2018; like the rest of the public, "Facebook became aware that Kogan and GSR had misused data after the *Guardian* published an article about it on December 11, 2015" and immediately "conducted an investigation." Compl. ¶ 311. In

[1] *See Price v. Facebook, Inc.*, No. 18-cv-0732 (N.D. Cal.) (filed Mar. 20, 2018).

[2] M. Rosenberg, N. Confessore & C. Cadwalladr, *How Trump "Consultants" Exploited the Facebook Data of Millions*, N.Y. Times (Mar. 17, 2018), https://nyti.ms/2HH74vA; C. Cadwalladr & E. Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, The Guardian (Mar. 17, 2018), https://bit.ly/2yMUmK2.

that 2015 article, the *Guardian* reported the same essential allegations as the 2018 *Guardian* article, with Cambridge Analytica allegedly misusing the data to serve ads in furtherance of the Cruz campaign.[3] Subsequent articles reported on many of the same allegations.[4] What was news in the 2018 articles was the claim that Cambridge Analytica may not have deleted the data in the years since the 2015 article was published, as it had certified to Facebook it had done.

A. Plaintiffs' Flawed Theories of Wrongdoing

Plaintiffs' allegations appear to focus on six issues: (1) data sharing with third-party apps; (2) failure to prevent third parties from misusing data; (3) targeted advertising; (4) device manufacturers; (5) accessibility of Facebook's policies; and (6) accessibility of Facebook's user controls. We address each below.

1. Data sharing with third-party apps. Facebook allowed third-party app developers "to access not only the content and information of the user who had installed the application, but also the content and information that the user's *friends* had shared with her." Compl. ¶ 7. As Plaintiffs acknowledge, this data was provided only if it "complie[d] with the user's and/or friends' privacy settings." *Id.* ¶¶ 121–122. According to Plaintiffs, Kogan's app accessed from the downloading users' friends, *at most*, only their "*Public* Facebook Profile, including their name and gender; Birth date; Current city if the friends had chosen to add this information to their profile; Photographs in which the friends were tagged; and Pages that the friends had liked." *Id.* ¶ 147 (emphasis added). None of the Plaintiffs describes any specific information that he or she shared on Facebook that Cambridge Analytica could have obtained—such as that they were tagged in any photographs, that they shared their current city, or that they liked any specific pages. Rather, Plaintiffs make only vague and generic allegations that they "shared content and information with Facebook," "'liked' videos on Facebook,"

---

[3] H. Davies, *Ted Cruz using firm that harvested data on millions of unwitting Facebook users*, The Guardian (Dec. 11, 2015), https://bit.ly/2lHR0Ac.

[4] *E.g.*, M. Schwartz, *Facebook Failed to Protect 30 Million Users From Having Their Data Harvested By Trump Campaign Affiliate*, The Intercept (Mar. 30, 2017), https://bit.ly/2oduMK7; S. Kirchgaessner, *Cambridge Analytica used data from Facebook and Politico to help Trump*, The Guardian (Oct. 26, 2017), https://bit.ly/2iDmKsG; S. Halpern, *How He Used Facebook to Win*, The New York Review of Books (June 8, 2017), https://bit.ly/2QkmzP7; H. Grassegger & M. Krogerus, *The Data That Turned the World Upside Down*, Vice Motherboard (Jan. 28, 2017), https://bit.ly/2ujkgUS.

"'liked' pages on Facebook that contain videos," and "use[d] Facebook messenger and/or instant messaging through Facebook." *E.g., id.* ¶ 55. Plaintiffs say, based on these rote allegations, that the effect of such data sharing was that individuals were served more specific and politically targeted ads than otherwise would have been the case. *Id.*, ¶¶ 5, 21–88, 135, 144, 386, 538. Plaintiffs do not identify any specific targeted ads they viewed or explain how any such ads caused them harm.

2. Failure to prevent third parties from misusing data. Plaintiffs allege that Facebook is responsible for any misuses of data obtained by third parties because it allegedly did not do enough to monitor the millions of apps users can download on Facebook. Specifically, Plaintiffs opine that Facebook had an obligation to "audit[] … the app developers to whom it gave access" and to tell users that app developers might "sell or disperse user content and information." Compl. ¶¶ 8, 486. But, other than Cambridge Analytica, Plaintiffs do not identify any app or company they interacted with personally. And they do not identify any harm they allegedly suffered from the so-called failure to audit Cambridge Analytica or any other third-party app.

3. Targeted advertising. Plaintiffs admit that "[t]here is nothing wrong with targeted advertising." Compl. ¶ 110. They complain only that advertising on Facebook is *too targeted* because Facebook "build[s] digital profiles of" its users, *id.* ¶ 366–367, and allows advertisers to target audiences based in part on demographic and other details that Facebook collects. *Id.* ¶¶ 377–379. Plaintiffs allege that this somehow "violates Facebook's promise not to give advertisers the content and information of users," *id.* ¶ 382, even though there is no allegation that Facebook actually shares *any* of this user data with advertisers. Plaintiffs identify no harm that supposedly befell them as a result of too-targeted advertising.

4. Device manufacturers. Plaintiffs allege it was wrong for Facebook to provide information to manufacturers of electronic devices "to make Facebook available not only on desktop computers, but also on users' mobile phones, smart TVs, game consoles, and other devices." Compl. ¶ 170. These "partnerships" with device makers allowed users "access to their Facebook network and messages" on various devices. *Id.* ¶ 171. For example, Facebook "allowed Microsoft-powered devices to add contacts and friends and receive notifications." *Id.* And it allowed Apple devices to "enable[] users to post photos to the social network without opening the Facebook

application." *Id.* Plaintiffs do not allege that they used devices manufactured by Microsoft or Apple, or any other specific manufacturer listed in the Complaint. Nor do they allege that any of the companies that facilitated access to Facebook on electronic devices obtained their data. As a result of this alleged data sharing with device manufacturers, Plaintiffs allege only that people with Facebook accounts could experience Facebook functionality on their mobile devices. *Id.* ¶¶ 170–171. The Complaint articulates no actionable theory under which this increased functionality caused harm to any Facebook user.

5. Accessibility of Facebook's policies. Plaintiffs acknowledge that Facebook's policies informed users how their data might be used by Facebook or shared with third parties, and that Facebook users could control how third parties accessed their data by adjusting their "App Settings." But they complain that these policies and the App Settings were too "difficult to access on Facebook's website." Compl. ¶¶ 9–10. Several of Plaintiffs' allegations attack the layout and user experience of Facebook's website. They acknowledge that, for most of the putative class period, the Data Use Policy was accessible on a single screen. *Id.* ¶¶ 248, 255. But they allege that, at other times, the Data Use Policy was divided into subheadings and that "to read the actual contents of the Data Use Policy, the user would have to read several subheadings" and "click on the subheadings or click '*expand all*.'" *Id.* ¶¶ 250, 252. The Complaint does not allege that any named plaintiff ever attempted to view the Data Use Policy, much less was thwarted in their attempt to read the Data Use Policy due to its layout.

6. Accessibility of Facebook's user controls. Plaintiffs admit that "Facebook provided 'Privacy Settings' to users," and that these settings were "prominent and accessible." Compl. ¶ 9. But they complain that the settings were too "confusing" because they were divided into separate "App Settings" and "Privacy Settings." *Id.* ¶ 182. Plaintiffs also assert that the App Settings were, in effect, *too* detailed and granular; they complain that Facebook offered them so many choices about what information to share that a user would have to click "twenty separate" times to turn them all off. *Id.* ¶ 198. And Plaintiffs complain that it "would have taken five affirmative clicks" to turn off any sharing with apps. *Id.* ¶¶ 200, 201. Plaintiffs do not allege that they tried to change their application settings, or what their privacy or application settings actually were. Nor do they allege any harm whatsoever that befell them as a result of the supposedly confusing Facebook user interface.

B. Plaintiffs' Purported Harm

Plaintiffs assert three general types of injury: (1) diminished value of their data; (2) increased risk of identity theft and emotional distress; and (3) invasion of privacy. We address each below.

1. Diminished value of their data. Plaintiffs allege generally, though no plaintiff alleges individually, that they "suffered diminished loss of use of their own data." Compl. ¶ 409. They try to quantify this inventive theory of harm by alleging "that an individual's online identity, including hacked financial accounts, can be sold for $1200 on the dark web" and that "Facebook logins can be sold for approximately $5.20 each." *Id.* But even under Plaintiffs' fanciful theory, there is no allegation that any Facebook user's "financial accounts" or "Facebook logins" were compromised, and any such allegation would be inconsistent with what Plaintiffs acknowledge actually happened here—Cambridge Analytica is alleged to have used Facebook user data only to inform the targeted ad campaigns it ran on Facebook (*id.*, ¶¶ 5, 21–88, 135, 144, 386, 538), not to sell anyone's data on the "dark web" or anywhere else. Not surprisingly, Plaintiffs do not allege that they ever tried to sell their own data on the "dark web," on any other "illegal marketplace," or elsewhere. Compl. ¶ 409. Plaintiffs' far-fetched theory of injury fails to establish standing.

2. Increased risk of identity theft and emotional distress. Plaintiffs allege that they "are at increased risk of identity theft due to Facebook's practices concerning sharing users' content and information with third parties" and that they "*may be* subjected to voter fraud, identity theft, medical fraud, and other harms." Compl. ¶ 574 (emphasis added). As a result of this perceived risk of identity theft, several plaintiffs allege to have purchased credit monitoring services, *id.* ¶ 412, and others allege that they suffered emotional distress and anxiety, *see, e.g.*, *id.* ¶ 32. But Plaintiffs do not claim that they or any putative class member was the victim of identity theft in the several years since Cambridge Analytica allegedly obtained their data. And Plaintiffs admit that there was no "theft of social security numbers or credit card numbers," *id.* ¶ 12, and do not describe any specific data they shared on Facebook or explain how that data might be used to steal someone's identity, *see, e.g.*, *id.* ¶ 29. Again, the only use of the data that is identified anywhere in the Complaint is to inform targeted ad campaigns run on Facebook. *Id.* ¶¶ 5, 21–88, 135, 144, 386, 538. No court has ever accepted Plaintiffs' theory of Article III standing based on such a speculative and implausible risk of identity theft.

3. Invasion of privacy. Plaintiffs contend that they "suffered egregious invasions of privacy" because "they were directly targeted by advertisements that would be highly offensive to a reasonable person." Compl. ¶ 415. But Plaintiffs do not allege what advertisements they viewed or what they depicted; they say only that "during the 2016 U.S. Presidential election," Plaintiffs "frequently received political advertisements while using Facebook." *See, e.g.*, *id.* ¶¶ 22, 24. It is unclear whether Plaintiffs viewed the content of the advertisements as offensive, or contend that targeted advertising is itself an invasion of privacy. *See id.* ¶ 397 ("Cambridge Analytica target[ed] people in the privacy of their homes."). They also assert that the disclosure of content and information to apps and device manufacturers is an invasion of privacy. *See, e.g.*, *id.* ¶ 24. But Plaintiffs point to only a single app—Kogan's app—that ever allegedly obtained any of their information. They do not allege any specific content Kogan's app (or any other app) obtained from them, however, and acknowledge that much of the information available to Kogan's app was *publicly available* in any event. They do not allege anything about their privacy settings or whether those settings allowed their information to be shared with Kogan's app. And they do not allege any *use* of the data provided by Kogan other than Cambridge Analytica's alleged use of certain Facebook user data to inform ad campaigns it ran on Facebook. *Id.* ¶¶ 5, 21–88, 135, 144, 386, 538.

C. The Relevant Agreements

Plaintiffs' Complaint acknowledges that sharing information—with both friends and apps—is a central purpose of Facebook and numerous other social media platforms, such as Spotify, Twitter, and Snapchat. Facebook "enable[s] users to connect, share, and communicate with each other through text, photographs, and videos, as well as to interact with third party apps such as games and quizzes on mobile devices and personal computers." Compl. ¶ 89. Not surprisingly, and as Plaintiffs also acknowledge, sharing on Facebook is governed by agreements between Facebook and its users. Plaintiffs admit that "[a]t all relevant times, Facebook and Plaintiffs mutually assented to, and therefore were bound by the version of Facebook's Statement of Rights and Responsibilities or later, the Terms of Service, (collectively, the 'Contracts') that was [sic] operative at the time each of the Plaintiff and Class Member [sic] joined Facebook." Compl. ¶ 527.

The use and sharing of data by Facebook and its users is governed by two primary documents: Facebook's Statement of Rights and Responsibilities ("SRR") and its Data Use Policy (previously referred to as the "Privacy Policy"). *See* Compl. ¶ 246 (Facebook's Data Policy governs "how [Facebook] collect[s] and can use your content and information"). The SRR and the Data Use Policy cover all of the policies and conduct Plaintiffs' Complaint characterizes as wrongful, including how Facebook shares data with third-party apps, provides advertising on its platform, and shares data with service providers such as device manufacturers. These policies also show users how to control data sharing and caution them about sharing data with third parties.

1. Sharing data with third-party apps. Facebook's Data Use Policy informs users of the information third-party apps may access if users choose to use (or "authorize") apps to do so. For example, the version of Facebook's Data Use Policy in effect in 2013 and 2014 told users that apps they accessed would receive their User ID—a string of numbers associated with a particular user (not to be confused with the Facebook ID)—and any information that users shared publicly. Compl. ¶ 275. Apps could also access users' friends' User IDs, also called a "friend list." *Id*. As the Data Use Policy explained, providing this information to apps allowed users to obtain the social benefits of connecting the apps to Facebook. *Id.* Providing a friend list allows an app to "know[] which of her friends is also using it," which allows for a "more personalized and social" experience. *Id.*

Facebook also allowed users to share additional information about their friends. For example, "one of your friends might want to use a music application that allows them to see what their friends are listening to." Compl. ¶ 275. In using the app, "[y]our friend might … want to share the music you 'like' on Facebook." *Id*. "If you have made that information public, then the application can access it just like anyone else. But **if you've shared your likes with just your friends, the application could ask your friend for permission to share them**." *Id*. (emphasis added). Thus, a user's friend could re-share the user's likes with an app that the friend had downloaded, so long as the original user (whose likes were at issue) had consented to such sharing. If a user had chosen to turn off all Platform apps, that user's friends could not share the user's information.

The Data Use Policy told users that the information they shared with friends could be disclosed to the apps their friends use: "Just like when you share information by email or elsewhere on the web,

information you share on Facebook can be re-shared. This means that if you share something on Facebook, anyone who can see it can share it with others, including the games, applications, and websites they use." *Id.* ¶ 275. Elsewhere, users were reminded that, even if they deleted their apps, "apps may still be able to access your information when the people you share with use them." *Id.*[5]

2. Advertising. Facebook also told users that it obtained information from them and described how it used that information in connection with advertising. The first full sentence of the Data Use Policy in effect in 2013 and 2014 (and in prior iterations back to 2011) stated that Facebook "receive[s] a number of different types of information about you," including "the information you choose to share on Facebook, such as when you post a status update, upload a photo, or comment on a friend's story." D.D., Ex. 45 at 2 (Dec. 11, 2012 Data Use Policy). The policy then explained that "sometimes we get data from our … advertising partners, customers and other third parties that helps us (or them) deliver ads, understand online activity, and generally make Facebook better," and that Facebook "may also put together data about you to serve you ads that might be more relevant to you." *Id.* at 2. Facebook also disclosed that advertisers could target users by characteristics gleaned from user data: "When an advertiser creates an ad [on Facebook], they are given the opportunity to choose their audience by location, demographics, likes, keywords, and any other information we receive or can tell about you and other users. … Sometimes we allow advertisers to target a category of user, like a 'moviegoer' or a 'sci-fi fan.' We do this by bundling characteristics that we believe are related to a category." *Id.* at 11-12.[6]

3. Device manufacturers. Facebook's policies also explained how Facebook might share data with companies who "recreate Facebook-like experiences for their individual devices or operating

[5] Prior iterations of the Data Use Policy, then called the Privacy Policy, contained similar terms. For example, the May 24, 2007 Privacy Policy (*see* Compl. ¶ 277) informed users that "If you, your friends, or member of your network use any third-party applications … those Platform Applications may access and share certain information about you with others in accordance with your privacy settings. You may opt-out of any sharing of certain or all information through Platform Applications on the Privacy Settings page." D.D., Ex. 34 at 5 (May. 24, 2007 Privacy Policy).

[6] Earlier policies, such as the May 24, 2007 Privacy Policy, similarly told users that "Facebook may use information in your profile without identifying you as an individual to third parties. We do this for purposes such as … personalizing advertisements and promotions." D.D., Ex. 34 at 4.

system." Compl. ¶ 170. The 2012 Data Use Policy, for example, explained that Facebook would "give your information to the people and companies that help us provide the services we offer. For example, we may use outside vendors to help host our website, serve photos and videos." *Id.* ¶ 281.[7] But Facebook made clear that "[i]n all of these cases our partners must agree to only use your information consistent with the agreement we enter into with them, as well as this Data Use Policy." *Id.*

4. User control of privacy settings. In keeping with the Data Use Policy, Facebook allowed users to control the information they shared with other Facebook users, and also with apps. The SRR informed users that "you can control how [content and information you post on Facebook] is shared through your privacy [hyperlinked] and application [hyperlinked] settings." Compl. ¶ 219. The hyperlinked "application settings" (labeled "Apps" in the control panel) included a series of controls regarding "Apps others use." *Id.* ¶ 194. It informed users that "People who can see your info can bring it with them when they use apps. Use this setting to control the categories of information people can bring with them." *Id.* Following that prompt sent users to a screen identifying categories of data, if any, that app developers could access, *id.* ¶ 197, and allowed users to check off which categories of data they wished to allow their friends to share with apps, *id.* ¶ 196.

[7] Earlier policies, such as the May 24, 2007 Privacy Policy, also informed users that Facebook "may provide information to service providers to help us bring you the services we offer." Compl. ¶ 277.

The same screen also informed users that "if you don't want apps and websites to access other categories of information (like your friend list, gender or info you've made public) you can turn off all platform apps." *Id.* ¶ 196; *id.* ¶ 200 (image depicting "App Settings" page where users could turn off all apps).

5. Disclosures about third parties. The Data Use Policy told users that "games, applications and websites are created and maintained by other businesses and developers who are not part of, or controlled by, Facebook," D.D., Ex. 45 at 8 (Dec. 11, 2012 Data Use Policy), and the SRR stated that a user's "agreement with [an] application will control how the application can use, store, and transfer … content and information," *id.*, Ex. 21 at 1 (Oct. 4, 2010 SRR); Compl. ¶¶ 221–222. Consistent with these controls and disclosures, the SRR clearly and unambiguously waived claims based on third-party conduct. It stated:

> FACEBOOK IS NOT RESPONSIBLE FOR THE ACTIONS, CONTENT, INFORMATION, OR DATA OF THIRD PARTIES, AND YOU RELEASE US, OUR DIRECTORS, OFFICERS, EMPLOYEES, AND AGENTS FROM ANY CLAIMS AND DAMAGES, KNOWN AND UNKNOWN, ARISING OUT OF OR IN ANY WAY CONNECTED WITH ANY CLAIM YOU HAVE AGAINST ANY SUCH THIRD PARTIES.

Id. at 3 (Oct. 4, 2010 SRR). This provision also expressly waived California Civil Code § 1542. *Id.*

IV. LEGAL STANDARD

A complaint must be dismissed under Rule 12(b)(6) unless it "contain[s] sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). Although the court accepts factual allegations as true, this rule is "inapplicable to legal conclusions." *Id.* The Court is not "required to accept as true allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences." *In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008). The factual allegations must "rise above the speculative level" and do more than "create[] a suspicion of a legally cognizable right of action." *Twombly*, 550 U.S. at 555, 561 (citation and quotation marks omitted); *Dahlia v. Rodriguez*, 735 F.3d 1060, 1076 (9th Cir. 2013). In making this determination, a court must "draw on its judicial experience and common sense." *Iqbal*, 556 U.S. at 679. This analysis provides a critical gatekeeping function, because claims must be sufficiently plausible "that it is not

unfair to require the opposing party to be subjected to the expense of discovery and continued litigation." *Eclectic Prop. E., LLC v. Marcus & Millichap Co.*, 751 F.3d 990, 996 (9th Cir. 2014).

When a complaint contains allegations that sound in fraud, "a party must state with particularity the circumstances constituting [the] fraud...." Fed. R. Civ. P. 9(b). "Rule 9(b) demands that … the circumstances constituting the alleged fraud 'be specific enough to give defendants notice of the particular misconduct … so that they can defend against the charge and not just deny that they have done anything wrong.'" *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1106 (9th Cir. 2003) (quoting *Bly–Magee v. California*, 236 F.3d 1014, 1019 (9th Cir. 2001)). "Averments of fraud must be accompanied by 'the who, what, when, where, and how' of the misconduct charged." *Id.* (quoting *Cooper v. Pickett*, 137 F.3d 616, 627 (9th Cir. 1997)). "A party alleging fraud must set forth more than the neutral facts necessary to identify the transaction." *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1124 (9th Cir. 2009) (quotation marks omitted). "Any averments which do not meet that standard should be 'disregarded,' or 'stripped' from the claim for failure to satisfy Rule 9(b)." *Id.* (quoting *Vess*, 317 F.3d at 1105–06).

V. ARGUMENT

Plaintiffs have tried hard to cast this case as some kind of data breach, where sensitive private information was made public, placing individuals at risk of financial fraud or identity theft. But that is not what this case is about, by Plaintiffs' own admissions. Rather, it involves users who consented to provide certain data (1) to a social media company—the very purpose of which is to facilitate information sharing, and whose primary source of revenue is serving advertisements—and (2) to certain third parties who use Facebook's platform and help users access Facebook on whatever device they choose. Plaintiffs' claims are based on the conduct of one such third party, Aleksandr Kogan, who obtained data as a developer that he was entitled to receive consistent with users' privacy settings, and then violated Facebook's policies by selling it to Cambridge Analytica. Plaintiffs allege that Cambridge Analytica, in turn, used the data to inform political ad campaigns it ran on Facebook—not to steal their identities. None of these events has anything in common with the limited number of data breach cases where courts have upheld complaints based on serious allegations of identity theft and similar concrete, unconsented-to harms. In this case, Plaintiffs can articulate no theory of actual or cognizable harm that would give them Article III standing to pursue their claims in federal court, and

in any event, the Complaint fails to state any viable legal cause of action.

A. Plaintiffs Lack Article III Standing

All of Plaintiffs' claims fail because they have not alleged, and cannot allege, that they suffered any concrete and particularized injury. To satisfy the "irreducible constitutional minimum of standing," Plaintiffs must establish an injury that is: (1) concrete and particularized, and actual or imminent, not conjectural or hypothetical; (2) causally connected to the defendant's alleged wrongdoing; and (3) redressable. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992). "A 'concrete' injury must be '*de facto*'; that is, it must actually exist," and cannot be "abstract." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016). It is insufficient to plead a mere statutory violation; "'a bare procedural violation … , divorced from any concrete harm' will not constitute an injury-in-fact." *Dutta v. State Farm Mut. Auto. Ins. Co.*, 895 F.3d 1166, 1173 (9th Cir. 2018) (quoting *Spokeo*, 136 S. Ct. at 1549).

1. Plaintiffs lack standing because they consented to the alleged conduct

As an initial matter, Plaintiffs lack Article III standing because they consented to Facebook's conduct. The law has long recognized *volenti non fit injura*, or as California codified: "He who consents to an act is not wronged by it." Cal. Civ. Code § 3515; *Hamud v. Hawthorne*, 52 Cal. 2d 78, 86 (1959) (en banc). Consent is discussed in more detail below. *See infra* Argument B.

2. The vast majority of the allegations in the Complaint are irrelevant for standing purposes because they have no connection to the named plaintiffs

Plaintiffs' claims also fail at the threshold because they have not alleged any *individual* facts that could support an assertion of Article III injury. The law is clear that "named plaintiffs who [seek to] represent a class 'must allege and show that they *personally* have been injured, not that injury has been suffered by other, unidentified members of the [putative] class ….'" *Lewis v. Casey*, 518 U.S. 343, 357 (1996) (emphasis added) (quoting *Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26, 40 n.20 (1976)). Only injuries that "affect the plaintiff in a personal and individual way" are cognizable. *Lujan*, 504 U.S. at 561 n.1. "[T]he plaintiff … must allege a distinct and palpable injury to himself, even if it is an injury shared by a large class of other possible litigants." *Warth v. Seldin*, 422 U.S. 490, 501 (1975). "[I]f none of the named plaintiffs purporting to represent a class establishes the requisite of a case or controversy with the defendants, none may seek relief on behalf of himself or any other member

of the class." *Lierboe v. State Farm Mut. Auto. Ins. Co.*, 350 F.3d 1018, 1022 (9th Cir. 2003); *see also Birdsong v. Apple, Inc.*, 590 F.3d 955, 961 (9th Cir. 2009) (plaintiffs must show "injury to *themselves*" to establish Article III standing (emphasis added)). Yet, "[d]espite a lengthy … Complaint, Plaintiffs do not allege injury in fact to themselves. This failure alone is sufficient reason to dismiss the … Complaint." *In re iPhone Application Litig.*, 2011 WL 4403963, at *4 (N.D. Cal. Sept. 20, 2011) (Koh, J.).

Although the Complaint spans over a thousand paragraphs, only a handful of the allegations relate to any of the individual plaintiffs. Plaintiffs allege that they have "watched and 'liked' videos and … pages on Facebook that contain videos" (Compl. ¶¶ 21, 23, 25, 27)—but not a single plaintiff identifies any video or page he or she liked. Plaintiffs allege that they "accessed [their] Facebook account[s]" via a variety of devices, but do not specify any particular device manufacturer. *See, e.g.*, *id*. And they allege that they "shared content and information with Facebook," but do not identify *any* specific content they shared—not a single photograph, message, news article, or video—and do not even say whether any of the content was set to be private. Indeed, despite the Complaint's central focus on users' privacy settings, the Complaint contains not a single allegation regarding any named plaintiff's *actual* privacy settings, let alone that they had set their privacy settings to anything more restrictive than "Public." Critically, Plaintiffs identify only a single instance of purported wrongdoing that affected them personally: the thisisyourdigitallife app's possible acquisition of a limited amount of their information, which they admit could have occurred only if their privacy settings allowed it. *See id.* ¶¶ 121–122, 138.

The remaining allegations in the Complaint have no discernible connection to individual Plaintiffs. For example, the Complaint alleges that additional apps may have accessed Facebook users' data, *e.g.*, *id.* ¶ 164–167, but none of the named plaintiffs identifies any additional apps that he or she, or his or her Facebook friends, used—nor does any of them assert that any specific apps accessed his or her data. Although the Complaint contains numerous allegations regarding Facebook's alleged agreements with device manufacturers such as Microsoft, Blackberry, Apple and others, *id.* ¶ 169, no plaintiff alleges that he or she ever used devices or services from these companies, or how any alleged sharing

with such companies harmed them. Finally, Plaintiffs do not allege that they saw any particular advertisement, let alone that the advertisement was shown to them because of the data that Cambridge Analytica accessed, nor how the content of any such advertisement invaded their privacy or otherwise affected them in any way.

3. Plaintiffs have not alleged facts supporting a claim of identity theft, or even an increased risk of identity theft

Plaintiffs assert that they "are at increased risk of identity theft due to Facebook's practices concerning sharing users' content and information with third parties," that they "*may be* subjected to voter fraud, identity theft, medical fraud, and other harms," Compl. ¶ 574, and that they have accordingly "suffered emotional distress," *see, e.g.*, *id.* ¶ 88. But this theory simply does not hold water when viewed in the context of cases addressing similar claims. Not a single Plaintiff identifies any specific "content and information" that they shared on Facebook, much less how they were placed at risk of having their identity stolen through use of the unidentified information,[8] and even Plaintiffs' more generalized allegations fail to articulate any cognizable theory of identity theft or similar harm.

For one thing, the data allegedly shared with third parties here—such as users' name, gender, and pages they have "liked"—bears no resemblance to the kinds of data courts have held may give rise to an actionable risk of identity theft. The common thread in *bona fide* identity theft cases is that the information stolen was likely to cause imminent economic harm by facilitating access to financial accounts or funds. Thus, the Ninth Circuit held that the plaintiffs in *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1140 (9th Cir. 2010), had standing where a thief obtained "unencrypted names, addresses, and social security numbers." As the Court later explained in *In re Zappos.com, Inc.*, 888 F.3d 1020, 1026 (9th Cir. 2018), there was a legitimate risk of identity theft in *Krottner* because the "thief had all the information he needed to open accounts or spend money in the plaintiffs' names." And in *Zappos*, the Court found actionable identify theft where hackers obtained "names, account numbers, passwords,

[8] Where, as here, a plaintiff claims that he or she is at risk of a future injury, the plaintiff must demonstrate that "the threatened injury is 'certainly impending,' or there is a 'substantial risk' that the harm will occur." *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014) (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013)). To plead a "substantial risk" that identity theft will occur, Plaintiffs must, at minimum, specify what data was taken from them and explain how it could be used to steal their identity—which the Plaintiffs here have not done.

email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information." 888 F.3d at 1023. This information "gave hackers the means to commit fraud or identity theft." Indeed, some "plaintiffs … alleged that the hackers had already commandeered their accounts or identities using information taken from Zappos." *Id*. at 1027.

The other common thread in actionable identity theft cases is that the data was stolen for the *purpose* of committing identity theft—creating a reasonable likelihood that it would be used for that purpose. As the Third Circuit noted, "[w]hy else would hackers break into a ... database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Attias v. Carefirst, Inc.*, 865 F.3d 620, 628–29 (D.C. Cir. 2017); *see Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015).

Here, by contrast, neither the type of information at issue, nor the use to which it allegedly was put by the third party who misused it, supports Plaintiffs' "identity theft" theory. The information that allegedly was shared—user name, likes, gender, and similar information—is not akin to the credit card information, passwords, and social security numbers that were at issue in *Krottner* and *Zappos*, and Plaintiffs offer no explanation for how the kind of information actually at issue here could facilitate identify theft. This, alone, is sufficient to defeat this theory of injury because, as numerous courts have held, a plaintiff does not allege injury in fact based on a risk of identity theft where that plaintiff fails to allege disclosure of data such as social security numbers or credit card information. *See In re SuperValu, Inc.*, 870 F.3d 763, 769–71 (8th Cir. 2017); *Dugas v. Starwood Hot. & Res. Worldwide, Inc.*, 2016 WL 6523428, at *5 (S.D. Cal. Nov. 3, 2016) (Curiel, J.); *see also Antman v. Uber Techs., Inc.*, 2015 WL 6123054, at *11 (N.D. Cal. Oct. 19, 2015) (Beeler, M.J.) ("theft of names and driver's licenses" insufficient; "[w]ithout a hack of information such as social security numbers, account numbers, or credit card numbers, there is no obvious, credible risk of identity theft that risks real, immediate injury").

Nor do Plaintiffs allege that the limited data at issue here would enable theft of someone's identity. On the contrary, the admitted purpose of using the information was to inform targeted ad campaigns on Facebook. Compl. ¶¶ 5, 21–88, 135, 144, 386, 538. That bears no resemblance to situations, such as in *Attias*, where a thief undertook to use the information to steal money or property from

the plaintiffs. Rather, this case falls squarely into the line of precedents in which courts have dismissed complaints where the allegedly stolen data *could not* plausibly enable identity theft.[9] As the Complaint alleges, for friends of users who downloaded the thisisyourdigitallife app, the app obtained their "*Public* Facebook Profile, including their name and gender; Birth date; Current city if the friends had chosen to add this information to their profile; Photographs in which the friends were tagged; and Pages that the friends had liked." *Id.* ¶ 147 (emphasis added). Much of this information, including name and gender, birth date, and city of residence (if it was shared, and Plaintiffs do not so allege), would have been publicly available, through either Plaintiffs' public Facebook profile or online records. Such basic "[d]emographic information is constantly collected on all consumers by marketers, mail-order catalogues and retailers." *Goodman v. HTC Am., Inc.*, 2012 WL 2412070, at *7 (W.D. Wash. June 26, 2012) (citation omitted). And the information, by definition, was shared by Plaintiffs with others on Facebook, including their friends who may have shared it with the app. Plaintiffs neither allege that identity thieves obtained any of this information nor offer any cogent explanation of how they might steal one's identity with this information if they had it.

Notably, the events of which Plaintiffs complain occurred years ago, yet they point to not a *single* instance of identity theft to them or any putative class member. That omission underscores the absence of any actual or "impending" harm. "[A]s the [events] fade further into the past, the Plaintiffs' threatened injuries become more and more speculative." *Beck v. McDonald*, 848 F.3d 262, 275 (4th Cir. 2017) (citation omitted), *cert. denied sub nom. Beck v. Shulkin*, 137 S. Ct. 2307.

Plaintiffs have also attempted to bootstrap standing by claiming that they have paid money for identity theft monitoring or have spent time monitoring their credit. "But this allegation is merely a

[9] *See, e.g.*, *In re SuperValu, Inc.*, 870 F.3d at 769 ("the allegedly stolen Card Information d[id] not include any personally identifying information, such as social security numbers, birth dates, or driver's license numbers"); *Dugas*, 2016 WL 6523428, at *5 (no standing where "because the PII stolen was limited only to Plaintiff's name, address, and credit card information, and because the credit card has since been cancelled"); *Low v. LinkedIn Corp.*, 2011 WL 5509848, at *6 (N.D. Cal. Nov. 11, 2011) (distinguishing *Krottner* in that the plaintiff had not alleged that his highly personal information had been stolen and then exposed to the public); *see also Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011) (affirming dismissal when hypothetical allegations of harm speculated that the hacker read, copied, and understood their personal information; that they intended to use the information to commit future criminal acts; and that they had the capacity to make unauthorized future transactions).

repackaged version of [Plaintiffs'] first failed [identity theft] theory of standing." *Beck*, 848 F.3d at 276 (citation and quotation marks omitted). As the Supreme Court explained, Plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm." *Clapper*, 568 U.S. at 416; *see also Reilly v. Ceridian Corp.*, 664 F.3d 38, 46 (3d Cir. 2011). Thus, "[m]itigation expenses do not qualify as actual injuries where the harm is not imminent." *Remijas*, 794 F.3d at 694; *accord Beck*, 848 F.3d at 272.

Plaintiffs' claims of emotional distress stem from the same purported source—the risk of identity theft—and fail for the same reason. *See, e.g.*, Compl. ¶ 44. As with the identity-theft allegations, Plaintiffs' allegations lack basic details such as "what information was actually disclosed to third parties that would lead Plaintiff[s] to suffer emotional harm." *Low v. LinkedIn Corp.*, 2011 WL 5509848, at *3 (N.D. Cal. Nov. 11, 2011) (Koh, J.); *compare Reilly*, 664 F.3d at 44–45 (plaintiff lacked standing for emotional distress claim because there was no alleged data misuse), *with Krottner*, 628 F.3d at 1141–42 (plaintiff had standing for emotional distress claim where thief stole laptop containing Plaintiff's unencrypted social security number).

4. Plaintiffs have not plausibly alleged that the market value of their personal information was diminished

Plaintiffs claim that they "have suffered injury in fact and lost money or property due to [Facebook's] business acts or practices" because their "content and information has tangible value." Compl. ¶ 573. But "injury-in-fact in this context requires more than an allegation that a defendant"—or a third party—"profited from a plaintiff's personal identification information." *In re Google, Inc. Privacy Policy Litig.*, 2013 WL 6248499, at *5 (N.D. Cal. Dec. 3, 2013) (Grewal, M.J.); *see also Silha v. ACT, Inc.*, 807 F.3d 169, 174–75 (7th Cir. 2015) ("[A] plaintiff's claim of injury in fact cannot be based solely on a defendant's gain; it must be based on a plaintiff's loss."). "'Demographic information is constantly collected on all consumers by marketers, mail-order catalogues and retailers,' but courts have not held that 'the value of this collected information constitutes damage to consumers or unjust enrichment to collectors.'" *Goodman*, 2012 WL 2412070, at *7. Rather, "a plaintiff must allege how the defendant[] … deprived the plaintiff of the information's economic value," *In re Google*, 2013 WL 6248499, at *5, by, for example, "identify[ing] a[n] … individual who was foreclosed from entering

into a 'value-for-value exchange' as a result of [Defendant's] alleged conduct," *Low*, 2011 WL 5509848, at *4; *see also In re iPhone Application Litig.*, 2011 WL 4403963, at *4; *LaCourt v. Specific Media, Inc.*, 2011 WL 1661532, at *4 (C.D. Cal. Apr. 28, 2011) (Wu, J.).

Plaintiffs have not made (and cannot make) such a showing, particularly as to the very limited and largely public types of "content and information" they allege was available to the thisisyourdigitallife app. Plaintiffs claim that "Facebook has undermined the market value of users' data" by making it "ubiquitously available." Compl. ¶ 409. As an initial matter, there is nothing in the Complaint to support the assertion that any of this data was made "available" in any relevant sense, given that the only use that allegedly was made of the data was to inform ad campaigns run on Facebook. *Id.* ¶¶ 5, 21–88, 135, 144, 386, 538. But in any event, Plaintiffs "do not allege they attempted to sell their personal information, that they would do so in the future, or that they were foreclosed from entering into a value for value transaction relating to their PII, as a result of [Facebook's] conduct." *In re Google Android Consumer Privacy Litig.*, 2013 WL 1283236, at *4 (N.D. Cal. Mar. 26, 2013) (White, J.). Further, without specifying whether *any* of the generic "content and information" that was obtained from them was private, they have not alleged that its limited disclosure somehow diminished its value. Nor have they plausibly alleged that a market existed for the limited content and information they allege was obtained by the thisisyourdigitallife app. They allege only "that an individual's online identity, *including hacked financial accounts*, can be sold for $1200 on the dark web" and that "*Facebook logins* can be sold for approximately $5.20 each." Compl. ¶ 409 (emphases added). The implication that Plaintiffs were deprived of the opportunity to sell their own financial data and Facebook logins on an "illegal marketplace" is absurd. In any event, Plaintiffs' "financial accounts" and "Facebook logins" are not at issue, as there is no allegation that any third parties obtained such information from them or from any Facebook account holder.

5. Plaintiffs have not alleged any cognizable privacy injury

Plaintiffs claim to have "suffered egregious invasions of privacy" because they were subjected to unidentified targeted ads and because Facebook released data that they assert was private. Compl. ¶¶ 402(iii), 404, 405, 415. These allegations are insufficient to establish injury in fact for Article III

purposes. Plaintiffs do not explain how the mere targeting of ads—a core feature of Facebook's platform to which Plaintiffs consented—could constitute a "privacy" injury, even if, as alleged, such ads were delivered with particular frequency or were focused with particular precision on Plaintiffs' interests. And Plaintiffs provide no detail as to how any of the alleged sharing of their data with third parties led to any "concrete" injury or "appreciable risk of harm" relating to any such ads. *Spokeo*, 136 S. Ct. at 1549; *Lujan*, 504 U.S. at 560. Courts have made clear that the sharing of allegedly personal information "without any concrete consequences" does not give rise to Article III injury. *Hancock v. Urban Outfitters, Inc.*, 830 F.3d 511 (D.C. Cir. 2016). Here, Plaintiffs nowhere identify any concrete way in which their privacy interests were harmed by the alleged voluntary sharing of limited categories of their Facebook information.

6. Plaintiffs have not articulated a sufficient contract injury amounting to injury in fact

Plaintiffs assert a breach of contract claim, alleging that Facebook's sharing of data with third-party apps violated the SRR. Compl. ¶¶ 526–544. But "under California law, a breach of contract claim requires a showing of appreciable and actual damage." *Aguilera v. Pirelli Armstrong Tire Corp.*, 223 F.3d 1010, 1015 (9th Cir. 2000). "[N]ominal damages, like speculative harm or fear of future harm, [do] not suffice to show legally cognizable damage . …" *Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908, 917 (N.D. Cal. 2009) (Conti, J.), *aff'd*, 380 F. App'x 689 (9th Cir. 2010); *see also Frangipani v. Boecker*, 64 Cal. App. 4th 860, 865 (1998) (contract damages "not recoverable for mental suffering or injury to reputation"). For this reason, "a contract breach by itself [does not] constitute[] an injury in fact" for purposes of standing. *In re Google*, 2013 WL 6248499, at *6; *accord Meneses v. U–Haul Int'l, Inc.*, 2012 WL 669518, at *5 (N.D. Cal. Feb. 29, 2012) (Ryu, M.J.). Thus, the standing analysis for Plaintiffs' breach of contract claim is the same as above—Plaintiffs have not plausibly alleged any existing or threatened harm from the alleged sharing of their information with third-party apps, and therefore lack standing.

B. Plaintiffs' Claims Are Foreclosed Because They Consented To The Alleged Conduct

"He who consents to an act is not wronged by it." Cal. Civ. Code § 3515; *see also Kent v. Microsoft Corp.*, 2013 WL 3353875, at *6 (C.D. Cal. July 1, 2013) (Carter, J.) ("[P]laintiffs generally

may not assert a wrong arising out of an action which they consented to."). That well-established maxim encapsulates another common flaw in all of Plaintiffs' claims: Plaintiffs consented to the very policies and practices they attack, and the absence of consent is a necessary component of each of their claims. Courts routinely dismiss similar claims against Facebook and other companies where users consented to conduct disclosed in the defendant's terms of service. *See Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 953 (N.D. Cal. 2017) (Davila, J.); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1028–32 (N.D. Cal. 2014) (Koh, J.); *Mortensen v. Bresnan Commc'n, L.L.C.*, 2010 WL 5140454, at *4 (D. Mont. Dec. 13, 2010) (Cebull, J.); *Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1214 (N.D. Cal. 2014) (Koh, J.).

1. Plaintiffs' consent is plain on the face of the relevant documents.

Plaintiffs consented, through the SRR and Data Use Policy, to each practice alleged in the Complaint. *See supra* pp. 10–12 (quoting specific disclosures covering advertising practices, sharing of data with third-party apps and device manufacturers). Many of Plaintiffs' claims fail for this reason alone.

Stored Communications Act (Claim I): An electronic service provider may disclose customer communications "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service." 18 U.S.C. § 2702(b)(3); *see also Perkins*, 53 F. Supp. 3d at 1214 (LinkedIn's policies made reasonable user aware that LinkedIn would be accessing emails from user's accounts); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1028–29.

Deceit by Concealment (Claim III): Facebook's disclosures defeat any claim that Facebook concealed a material fact because Plaintiffs were "already in possession of knowledge" they allege Facebook "attempted to conceal." *Sills v. Siller*, 218 Cal. App. 2d 735, 741 (1963).

Tort Claims (Claims IV, V, VII, IX, X): "Plaintiffs' consent also bars their common-law tort claims and their claim[s] for invasion of privacy …." *Smith*, 262 F. Supp. 3d at 955. "One who effectively consents to conduct of another intended to invade his interests cannot recover." Restatement (Second) of Torts § 892A (1979); Cal. Civ. Code § 3515; *see also Kent*, 2013 WL 3353875, at *6. In

particular, "the plaintiff in an invasion of privacy case … must not have manifested by his or her conduct a voluntary consent to the invasive actions of defendant." *Hill v. NCAA*, 7 Cal. 4th 1, 26 (1994); *see also Cross v. Facebook, Inc.*, 14 Cal. App. 5th 190, 208 (2017) ("lack of consent" is an element of common law right of publicity claim).

Breach of Contract (Claim VI) and Breach of Implied Covenant of Good Faith and Fair Dealing (Claim XI): A breach of contract action will not lie where the alleged breach is, on its face, consistent with the terms of the contract, or where the plaintiff consented to the conduct allegedly constituting the breach. *See Young v. Facebook, Inc.*, 790 F. Supp. 2d 1110, 1117 (N.D. Cal. 2011). The same applies to an alleged breach of the implied covenant of good faith and fair dealing. *Id.*; *see also Stewart v. Screen Gems-EMI Music, Inc.*, 81 F. Supp. 3d 938, 965 (N.D. Cal. 2015) ("[A] party cannot breach the implied covenant by engaging in acts or conduct consistent with the express provisions of a contract.") (citing *Carma Developers (Cal.), Inc. v. Marathon Dev. Cal., Inc.*, 2 Cal. 4th 342, 374 (1992)).

2. Plaintiffs' attempts to avoid the relevant documents fail as a matter of law.

Plaintiffs attempt to avoid the plain consent language contained in Facebook's contracts in two ways, both of which fail as a matter of law.

First, although Plaintiffs concede they are bound by Facebook's SRR (Compl. ¶ 527), they assert they are *not* bound by Facebook's Data Use Policy (*id.* ¶ 531). But Plaintiffs cannot have it both ways; the SRR expressly incorporated the Data Use Policy. "Under California law, parties may validly incorporate by reference into their contract the terms of another document." *Slaught v. Bencomo Roofing Co.*, 25 Cal. App. 4th 744, 748 (1994). The incorporated document does not itself need to be a contract. 1 Witkin, Summary (11th) of Contracts § 770 (2018); *Cadigan v. Am. Trust Co.*, 131 Cal. App. 2d 780, 787 (1955). Indeed, "[t]he contract need not recite that it 'incorporates' another document, so long as it 'guide[s] the reader to the incorporated document.'" *Shaw v. Regents of Univ. of Cal.*, 58 Cal. App. 4th 44, 54 (1997) (quoting *Baker v. Aubry*, 216 Cal. App. 3d 1259, 1264 (1989)). The plaintiff need not even know about the relevant provisions of the incorporated document, so long as it "was easily available to him." *Wolschlager v. Fid. Nat'l Title Ins. Co.*, 111 Cal. App. 4th 784,

791 (2003). If the contract "identifie[s] the [document] by name and direct[s] the plaintiff to where he could inspect it[, n]othing further [is] needed to bind the plaintiff." *Id.*

There can be no doubt that the SRR incorporated the Data Use Policy (and, earlier, the Privacy Policy). Plaintiffs allege that, "[a]t all relevant times until June 8, 2012," the second paragraph of the SRR stated:

> Your privacy is very important to us. We designed our Privacy Policy [hyperlinked] to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Privacy Policy, and to use it to help make informed decisions.

Compl. ¶ 243. Plaintiffs allege that, after June 8, 2012, the second paragraph of the SRR was revised to substitute the word "Data Use Policy" for "Privacy Policy," but otherwise remained identical. *Id*. ¶ 244. This language in the SRR was designed to call the terms of the Data Use Policy to users' attention. *Shaw*, 58 Cal. App. 4th at 54. It "encourage[d] [users] to read" the policy, so that they could "make informed decisions." *See Wolschlager*, 111 Cal. App. 4th at 787, 791 (insurance policy incorporated into title report where the report named the policy and stated that "copies of the policy forms should be read"). It stated that the Data Use Policy made "important disclosures" about Facebook's use of data. And the Data Use Policy's terms were "easily available." *Wolschlager*, 111 Cal. App. 4th at 791. Plaintiffs allege, for example, that "[p]rior to September 2011, if a curious user clicked on th[e] hyperlink [to the Privacy Policy in the SRR], she would be routed to one webpage that contained the entire Policy." Compl. ¶ 248. Moreover, the 2015 version of the SRR provided that users "agree[d] that [Facebook] can collect and use [your] content and information in accordance with the Data Policy." D.D., Ex. 26 at 6.

Even if the Data Use Policy were not expressly incorporated into the contract, Plaintiffs' allegations still would show that they consented to it. "If words or conduct are reasonably understood by another to be intended as consent, they constitute apparent consent and are as effective as consent in fact." Restatement (Second) of Torts § 892; *see also Griggs-Ryan v. Smith*, 904 F.2d 112, 116 (1st Cir. 1990) ("[C]onsent inheres where a person's behavior manifests acquiescence or a comparable voluntary diminution of his or her otherwise protected rights."). Plaintiffs admit that, as early as May 2007, any new user who signed up for Facebook was told that clicking "Sign Up" constituted the user's

"agree[ment]" that he or she had "read and agree to the … Privacy Policy," or "have read our Data Use Policy," depending on when the user signed up. Compl. ¶¶ 259–269. And because Plaintiffs concede they were bound by the SRR, which clearly and unmistakably referenced the Data Use Policy, they cannot reasonably deny they were aware that the policy governed Facebook's use of their data. In California, courts presume a plaintiff has read the relevant contract, *see Constantian v. Mercedes-Benz Co.*, 5 Cal. 2d 631, 634 (1936), and therefore is "chargeable with knowledge of its contents," *Taussig v. Bode & Haslett*, 134 Cal. 260, 266 (1901). Because the "contents" of the contracts informed users that the Data Use Policy contained "important disclosures about … how [Facebook] collect[s] and can use your content and information," the only reasonable inference from Plaintiffs' undisputed assent to the SRR was that they consented to the Data Use Policy.

That is why nearly every complaint filed in this case—up until the Consolidated Amended Complaint—acknowledged that the Data Use Policy was one of the contracts binding the plaintiffs. *See, e.g.*, Beiner Compl. ¶ 38, No. 18-cv-1953 (describing the "Privacy Policy" as one of "the documents that form the agreement between Facebook and its users"); Burk Compl. ¶ 85, No. 18-cv-2504 ("Plaintiffs and Class members had agreements with Facebook, including Facebook's Data Use Policy"); Comforte Compl. ¶ 188, No. 18-cv-3394 ("In order to register as a user of Facebook, Plaintiffs and the Class affirmatively assent to its Terms and Conditions and Privacy Policy"). Plaintiffs cannot negate this irrefutable fact by alleging the contrary in their amended complaint. *See Airs Aromatics, LLC v. Opinion Victoria's Secret Stores Brand Mgmt., Inc.*, 744 F.3d 595, 600 (9th Cir. 2014) ("A party cannot amend pleadings to 'directly contradic[t] an earlier assertion made in the same proceeding.'" (quoting *Russell v. Rolfs*, 893 F.2d 1033, 1037 (9th Cir. 1990)); *Kabir v. Flagstar Bank, FSB*, 2017 WL 8220425, at *4 (C.D. Cal. May 12, 2017) (granting motion to dismiss based on inconsistencies with prior allegations); *Elofson v. Bivens*, 2017 WL 566323, at *7 (N.D. Cal. Feb. 13, 2017) (same).

Second, Plaintiffs catalogue minute changes in the terms of Facebook's agreements, in an attempt to argue that they did not consent to policies Facebook adopted after they joined and (to this day) continue to use Facebook. But Plaintiffs' concession that they are "bound by" the agreement that existed when they registered (Compl. ¶ 527) forecloses any argument that they were not bound by later

iterations of the agreement. That is because each of the contracts contained clauses authorizing Facebook to update the agreements without securing any additional manifestation of assent from Plaintiffs. For example, the first paragraph of the Terms of Service in effect prior to May 2009 stated

> We reserve the right, at our sole discretion, to change, modify, add, or delete portions of these Terms of Use at any time without further notice. If we do this, we will post the changes to these Terms of Use on this page and will indicate at the top of this page the date these terms were last revised. Your continued use of the Service or the Site after any such changes constitutes your acceptance of the new Terms of Use. If you do not agree to abide by these or any future Terms of Use, do not use or access (or continue to use or access) the Service or the Site. It is your responsibility to regularly check the Site to determine if there have been changes to these Terms of Use and to review such changes.

E.g., D.D., Ex. 8 at 1. Facebook subsequently clarified in the SRR that notice to users would be provided "by posting the change on the Facebook Site Governance Page [hyperlink]." Compl. ¶ 237. And Plaintiffs concede that Facebook did, in fact, publish any proposed changes "on the Facebook Site Governance Page," as it said it would do in the SRR. *Id.* ¶ 291. *See In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155, 1167 (N.D. Cal. 2016) (holding that Facebook's provision of notice to users of changes to its policies "in combination with a user's continued use [of Facebook] is enough for notice and assent" to the new terms).

Thus, regardless of when Plaintiffs joined Facebook, their continued use of Facebook binds them to updated versions of the terms. *See Tompkins v. 23andMe, Inc.*, 840 F.3d 1016, 1032–33 (9th Cir. 2016) (unilateral modification clauses are enforceable when, as in California, they are limited by the implied covenant of good faith and fair dealing); *Ali v. J.P. Morgan Chase Bank, N.A.*, 647 F. App'x 783, 786 (9th Cir. 2016) (unilateral modification clause enforceable). And, in any event, the app-related terms and disclosures did not change in any material way during the putative class period at issue here, as Plaintiffs' Complaint makes clear. *See, e.g.*, Compl. ¶¶ 274–285.

C. Many of Plaintiffs' Claims Are Barred By the Statute of Limitations

The events underlying Plaintiffs' claims were widely reported more than two years before the first lawsuit was filed on March 20, 2018, when the *Guardian* published an article on December 11, 2015, describing in detail the underlying facts concerning Cambridge Analytica's misuse of Facebook user data. Because this public disclosure put Plaintiffs on notice of a potential claim, all of their

claims with a statute of limitations period of two years or shorter are barred. These include Plaintiffs' federal claims under the Stored Communications Act[10] and the Video Privacy Protection Act[11]; their claims for invasion of privacy, negligence, and gross negligence[12]; and their claim for breach of the implied covenant of good faith and fair dealing.[13]

For the federal claims, "the general federal rule is that a limitations period begins to run when the plaintiff knows or has reason to know of the injury which is the basis of the action." *Mangum v. Action Collection Serv., Inc.*, 575 F.3d 935, 940 (9th Cir. 2009). Similarly, under California law, "a cause of action accrues at the time when the cause of action is complete with all of its elements." *Fox v. Ethicon Endo-Surgery, Inc.*, 35 Cal. 4th 797, 806 (2005). The discovery rule, an exception to the general rule, "postpones accrual of a cause of action until the plaintiff discovers, or has reason to discover, the cause of action." *Id.* at 807. "A plaintiff has reason to discover a cause of action when he or she has a reason at least to suspect a factual basis for its elements." *Id.*

The 2015 *Guardian* article put Plaintiffs on notice of all of the facts surrounding the Cambridge Analytica issues alleged in the Complaint. Lipshutz Decl., Ex. 1. The article reported that Cambridge Analytica had obtained data from "tens of millions of Facebook users, harvested largely without their permission." The article stated that "names, locations, birthdays, genders—as well as … Facebook 'likes'" had been collected. And a chart set out explicitly how the process purportedly worked. It said that "[u]sers agreed for the survey to access their Facebook account and download data including:

[10] "A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation." 18 U.S.C. § 2707(f).

[11] "No action may be brought under this subsection unless such action is begun within 2 years from the date of the act complained of or the date of discovery." 18 U.S.C. § 2710(c)(3).

[12] California Code of Civil Procedure Section 335.1 provides that "[a]n action for assault, battery, or injury to, or for the death of, an individual caused by the wrongful act or neglect of another" must be brought "[w]ithin two years."

[13] California Code of Civil Procedure Section 339 provides that "[a]n action upon a contract, obligation or liability not founded upon an instrument of writing" must be brought "[w]ithin two years." *See also Eisenberg v. Ins. Co.*, 815 F.2d 1285, 1292 (9th Cir. 1987) ("California courts would apply Section 339(1)'s two year period to a breach of the covenant of good faith and fair dealing claim.").

name, age, location, and Likes" and that "the same information was captured for each of the [downloading users'] friends." The article reported that Cambridge Analytica used that data "to build sophisticated models of users' personalities." The article further explained that this Facebook data was being paired "with existing voter datasets" to improve political advertising.

Plaintiffs nonetheless assert that "users did not know until March of 2018" about the practices alleged in the Complaint, Compl. ¶ 3, referencing the pair of March 17, 2018 articles published in *The New York Times* and *The Guardian*. But even those 2018 articles explicitly referenced and built off the 2015 *Guardian* article, reporting the same basic information. The only new fact alleged in the 2018 articles was that Cambridge Analytica had not deleted the Facebook user data as it had previously promised it did—a factual allegation that forms no part of Plaintiffs' core allegations against Facebook here. By December 2015, Plaintiffs therefore "ha[d] a reason at least to suspect a factual basis for [the] elements" of their claims, and all of their claims with a two-year statute of limitations are barred.

D. Plaintiffs' Federal Statutory Claims Fail For Additional Reasons

1. Stored Communications Act

Section 2701(a) does not apply. Plaintiffs cannot state a claim against Facebook under Section 2701(a) for "accessing [their data] without" or "exceeding" Facebook's "authorization" because the statute does not apply "with respect to conduct authorized by the person or entity providing a wire or electronic communications service." 18 U.S.C. § 2701(c)(1). Plaintiffs allege that Facebook is a provider of an electronic communications service, Compl. ¶ 459, and that the electronic communications at issue were sent "from their computers or mobile devices to Facebook's servers," *id.* ¶ 452. Because Facebook itself provided the service at issue and is alleged to have authorized access to users' data, Section 2701(c)(1) bars Plaintiffs' claim under this provision. *See In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1026–27.

Plaintiffs have not adequately alleged a violation of § 2702(a). Section 2702(a)(1) provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." Section 2702(a)(2) provides that "a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which

is carried or maintained on that service—on behalf of, and received by means of electronic transmission from … a subscriber or customer of such service." Plaintiffs assert that Facebook violated these provisions by disclosing their "Facebook content"—"all posts, private messages, and similar communication[s]"—"to unauthorized third parties." Compl. ¶¶ 452, 467–468. These claims fail.

First, as explained above, Plaintiffs consented to the data sharing at issue, a complete defense to an alleged violation of Section 2702. *See* 18 U.S.C. § 2702(b)(3).

Second, Plaintiffs do not adequately allege that any communications protected by the SCA were shared with the thisisyourdigitallife app or by any other means. The California Supreme Court recently held that publicly available information is not protected under Section 2702. *Facebook, Inc. v. Superior Court*, 4 Cal. 5th 1245, 1268 (2018). That court looked to users' privacy settings to determine whether particular data was restricted in some fashion. *See id.* at 1272 (remanding to trial court for determination of whether requested information was public or private); *cf. Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 2d 659, 669 (D.N.J. 2013) (Martini, J.) (users' wall posts were covered by SCA because plaintiff "chose privacy settings"). Here, Plaintiffs have not alleged that any of their Facebook information was set to anything other than "public."

In addition, the only potentially non-public information that Plaintiffs allege the thisisyourdigitallife app *ever* obtained from users was "[p]hotographs in which [the downloading users]were tagged," "Pages that the friends had liked," and, for a handful of Facebook users, messages they sent to those who downloaded the app. Compl. ¶¶ 139, 146–147. But Plaintiffs have failed to allege any SCA violation with regard to these categories of information. Not a single individual Plaintiff alleges that he or she was tagged in any photos or sent any specific messages, and that any such content was disclosed to Kogan's app. As to Facebook messages, the Complaint establishes that Facebook was authorized to disclose these communications. The SCA permits disclosure with "the lawful consent of the originator *or an addressee or intended recipient* of [the] communication, or the subscriber." 18 U.S.C. § 2702(b)(3) (emphasis added); *see also Facebook*, 4 Cal. 5th at 746; *In re Facebook, Inc.*, 923 F. Supp. 2d 1204, 1206 (N.D. Cal. 2012). Plaintiffs admit that Kogan's app obtained messages only from users who authorized the app. *See* Compl. ¶¶ 139, 146. By definition, those users were

either an "originator," "addressee," or "intended recipient" of the message, whose consent was sufficient to allow sharing with Kogan's app. In any event, Plaintiffs do not allege that any of *their* specific messages were actually disclosed to Kogan's app—not surprising since, as Plaintiffs concede, message information was acquired from fewer than 1,500 of the more than 300,000 users of the App. *Id.* ¶ 139.

2. Video Privacy Protection Act

Plaintiffs contend that Facebook violated the VPPA—a 1988 statute that explicitly regulates "video tape service provider[s]"—because it allegedly allowed access to "posts in a user's timeline" that may have included "videos uploaded by the user as well as videos or video hyperlinks shared with a user by the user's friends." Compl. ¶ 479. These claims fail for several reasons.

Facebook is not a Video Tape Service Provider. The VPPA prohibits "video tape service provider[s]" from "knowingly disclos[ing], to any person, personally identifiable information concerning any consumer of such provider." 18 U.S.C. § 2710(b)(1). "The term 'video tape service provider' means any person, engaged in the business … of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials...." 18 U.S.C. § 2710(a)(4). Facebook is not in the "business … of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials." 18 U.S.C. § 2710(a)(4). In *Lane v. Facebook, Inc.*, 696 F.3d 811, 823 (9th Cir. 2012), the Ninth Circuit analyzed the fairness of a class settlement including a VPPA claim and noted that Facebook is likely not a Video Tape Service Provider—as opposed to a company like Blockbuster, which the court noted was "one of the only defendants that might qualify" as a Video Tape Service Provider. *See also id.* at 833 (Kleinfeld, J., dissenting) ("Facebook had a good argument that it was not itself a 'video tape service provider'"). This Court should arrive at the same conclusion and find that Facebook is not a video tape service provider. *See In re Vizio, Inc. Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1221–22 (C.D. Cal. 2017) ("peripheral[] or passive[] involve[ment] in video content delivery" not covered by VPPA).

The information regarding user "likes" of videos on Facebook is not "personally identifiable information" under the VPPA. The VPPA states that "[t]he term 'personally identifiable information' includes information that identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3). The VPPA was

enacted after a video store gave a newspaper "a list of the videos that Circuit Judge Robert Bork had rented"; that fact pattern is the "paradigmatic case" for VPPA liability. *In re Hulu Privacy Litig.*, 86 F. Supp. 3d 1090, 1096 (N.D. Cal. 2015) (Beeler, M.J.). The definition of personally identifiable information "is intended to be transaction-oriented," and limited to "information that identifies a particular person as having engaged in a specific transaction." S. Rep. 100-599 at 12. Thus "the statute protects personally identifiable information that identifies a specific person and ties that person to particular videos *that the person watched*." *In re Hulu Privacy Litig.*, 2014 WL 1724344, at *8 (N.D. Cal. Apr. 28, 2014) (Beeler, M.J.) (emphasis added); *see also Gonzalez v. Central Elec. Co-op, Inc.*, 2009 WL 3415235, at *11 (D. Or. Oct. 15, 2009) (Hogan, J.). Here, Plaintiffs have not alleged that Facebook maintains, or disclosed, any personally identifiable information, as understood by the VPPA. That a plaintiff has "liked" a page containing a video—or even "liked" the video itself—does not mean he or she has ever viewed that video, let alone engaged in any transaction to procure access to that content.

E. Plaintiffs' California State-Law Claims Fail For Additional Reasons

1. Facebook's disclaimer of liability bars all claims based on the conduct of third parties

Several of Plaintiffs' claims rely on the actions of third parties—advertisers who allegedly showed "offensive" advertisements and third parties, such as Kogan, who mishandled user data. But Plaintiffs cannot maintain actions on those theories because the SRR—which Plaintiffs admit was binding—expressly waived claims based on third-party conduct. *See supra* p. 13.[14]

Plaintiffs assert that "any purported waiver of liability" is contrary to public policy and unconscionable. Compl. ¶¶ 560–561. Both contentions lack merit. A contractual liability waiver may be invalid under California public policy when "[i]t concerns a business of a type generally thought suitable for public regulation," "[t]he party seeking exculpation is engaged in performing a service of great importance to the public, which is often a matter of practical necessity for some members of the public," and "[a]s a result of the essential nature of the service, in the economic setting of the transaction, the

[14] In addition, to the extent Plaintiffs seek to hold Facebook responsible for alleged injuries related to the content of the third-party ads they saw on Facebook, such claims would be barred by the Communications Decency Act, 47 U.S.C. § 230. *See Bennett v. Google, LLC*, 882 F.3d 1163, 1167–68 (D.C. Cir. 2018) (Google not liable for blog posts by third parties); *Goddard v. Google, Inc.*, 640 F. Supp. 2d 1193, 1201 (N.D. Cal. 2009) (Google not liable for allegedly fraudulent third-party ads).

party invoking exculpation possesses a decisive advantage of bargaining strength against any member of the public who seeks his services." *Tunkl v. Regents of Univ. of Cal.*, 60 Cal. 2d 92, 98–99, 101 (1963) (release in hospital-patient contract unenforceable). Courts often point to the "essential" nature of the services being provided as the reason for striking down a release of liability provision. *See, e.g.*, *Henrioulle v. Marin Ventures, Inc.*, 20 Cal. 3d 512, 517–520 (1978) (negligence by residential landlord); *Gavin W. v. YMCA of Metropolitan L.A.*, 106 Cal. App. 4th 662, 676 (2003) (negligence by provider of child care services); *Gardner v. Downtown Porsche Audi*, 180 Cal. App. 3d 713, 718 (1986) (negligence by auto repair shop). But Facebook's services do not qualify as "essential" for these purposes. Rather, as Plaintiffs allege, using Facebook enables users "to coordinate daily activities, network, engage in political and cultural discourse, and pursue interests and hobbies," all by "shar[ing] their personal information with their friends." Compl. ¶ 560. Facebook's service is akin to the type of services for which courts repeatedly uphold releases of liability. *See City of Santa Barbara v. Superior Court*, 41 Cal. 4th 747, 757–58 (2007) (citing cases upholding releases of liability in the context of recreation); *YMCA of Metropolitan L.A. v. Superior Court*, 55 Cal. App. 4th 22, 27 (1997) ("simple recreational offerings of games, socializing, shopping, … [are] not so essential as to rob [P]laintiff[s] of [their] free will in deciding" whether to consent to the contracts).

Plaintiffs' remaining theories for avoiding the waiver fare no better. Plaintiffs allege that Facebook is a business "suitable for public regulation"; that Facebook "possesses a decisive advantage of bargaining strength"; that the liability waiver "occurs in a standardized adhesion contract"; and that Facebook is in "total control of its platform and services." Compl. ¶ 560. Those allegations ignore that Facebook users *have control over the content they share and with whom they share it*. Indeed, if a Facebook account holder does not want apps to obtain his data, that user can opt out of apps altogether or stop using Facebook. *Id.* ¶ 199; *see, e.g.*, *YMCA of Metropolitan L.A.*, 55 Cal. App. 4th at 28 (upholding senior club's release because plaintiff could "find[] another senior center or club").

Next, Plaintiffs vaguely assert that "any purported waiver of liability is unconscionable." Compl. ¶ 561. But Plaintiffs' allegations do not come close to pleading unconscionability under California law. "A finding of unconscionability requires a procedural and a substantive element, the former focusing on oppression or surprise due to unequal bargaining power, the latter on overly harsh or one-

sided results." *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333, 340 (2011) (quotation marks omitted). The procedural element "focuses on two factors: oppression and surprise." *Aron v. U–Haul Co. of Cal.*, 143 Cal. App. 4th 796 (2006). "Oppression arises from an inequality of bargaining power which results in no real negotiation and … absence of meaningful choice." *A & M Produce Co. v. FMC Corp.*, 135 Cal. App. 3d 473, 486 (1982). "'Surprise' involves the extent to which the supposedly agreed-upon terms of the bargain are hidden in a prolix printed form drafted by the party seeking to enforce the disputed terms." *Id.* Plaintiffs' Complaint includes no allegations about the individual circumstances under which Plaintiffs formed their contracts, let alone allegations concerning oppression or surprise. *See Lancaster v. Alphabet Inc.*, 2016 WL 3648608, at *3 (N.D. Cal. July 8, 2016) (plaintiff failed to allege non-conclusory facts to support contention that YouTube's Terms of Service are unconscionable or otherwise void because they prohibit punitive damages).

"Substantive unconscionability focuses on the actual terms of the agreement and evaluates whether they create 'overly harsh' or 'one-sided results.'" *Wayne v. Staples, Inc.*, 135 Cal. App. 4th 466, 480 (2006). "To be substantively unconscionable, a contractual provision must shock the conscience." *Id.* Plaintiffs do not allege that the terms of Facebook's specific limitation of liability create overly harsh or one-sided results so as to shock the conscience. Nor could they, as such liability releases are routinely enforced in California, and are consistent with a person's expectations that a contracting party should not be held liable for the actions of a third party.

2. Deceit by concealment or omission

Plaintiffs' concealment claim fails because Plaintiffs cannot point to any fact that Facebook was obligated, and failed, to disclose. And they have not come close to pleading fraudulent concealment with the stringent particularity that Rule 9(b) requires.

> [A]n action for fraud and deceit based on concealment has five elements: (1) the defendant must have concealed or suppressed a material fact, (2) the defendant must have been under a duty to disclose the fact to the plaintiff, (3) the defendant must have intentionally concealed or suppressed the fact with the intent to defraud the plaintiff, (4) the plaintiff must have been unaware of the fact and would not have acted as he did if he had known of the concealed or suppressed fact, and (5) as a result of the concealment or suppression of the fact, the plaintiff must have sustained damage.

Tenant Healthsystem Desert, Inc. v. Blue Cross of Cal., 245 Cal. App. 4th 821, 844 (2016) (quotation

marks and brackets omitted); *Copart, Inc. v. Sparta Consulting, Inc.*, 277 F. Supp. 3d 1127, 1148 (E.D. Cal. 2017) (Mueller, J.). "[T]he elements of fraud and deceit based on concealment are the same as intentional fraud, with the additional requirement that the plaintiff allege that the defendant concealed or suppressed a material fact in a situation in which the defendant was under a duty to disclose [it]." *Tenant Healthsystem*, 245 Cal. App. 4th at 844.

Plaintiffs contend that Facebook failed to "disclose known risks that third party app developers would sell or disperse user content and information." Compl. ¶ 486. This theory is barred by the parties' waiver of liability for third-party actions. *See supra* p. 38. But in any event, there is no duty to disclose a risk of third-party wrongdoing. Just as "one owes no duty to control the conduct of another," there is no duty "to warn those endangered by such conduct," *Davidson v. City of Westminster*, 32 Cal. 3d 197, 203 (1982), and even if there were such a duty, Facebook satisfied it by telling users that it did not exercise ultimate control over how app developers treated users' data. Its Data Use Policy told users that "games, applications and websites are created and maintained by other businesses and developers who are not part of, or controlled by, Facebook, so you should always make sure to read their terms of service and privacy policies to understand how they treat your data." D.D., Ex. 45 at 8 (Dec. 11, 2012 Data Use Policy). That disclosure was more than sufficient to alert users to the possibility that an app developer could conceivably misuse their information. And this disclosure went hand in hand with the waiver, which confirmed that users themselves were responsible for controlling their disclosures to and dealings with third parties.

Plaintiffs also contend that Facebook was required to "disclose … how Facebook allows other third parties—including but not limited to app developers, device makers, mobile carriers, software makers, and others—to obtain their personal information notwithstanding their privacy settings." Compl. ¶ 496. As an initial matter, the Complaint does not allege that the privacy settings of any named plaintiff was anything other than "public." And no named plaintiff alleges that any "device makers, mobile carriers, software makers, [or] others … obtain[ed] [that person's] personal information." *Id.* They allege only that the thisisyourdigitallife app obtained their information. As to that app, none of the named plaintiffs alleges that it obtained any "personal information" not already publicly available, or that any such acquisition exceeded that person's privacy permissions. Thus, they have not alleged

any injury, much less a link between their injury and Facebook's purported nondisclosure. In any event, Facebook's SRR and Data Use Policy disclosed how Plaintiffs' information could be used.

Plaintiffs next assert that Facebook failed to "disclose … how [its] content and information was being collected, shared and aggregated to develop digital dossiers of each user," Compl. ¶ 503, and that it "had a duty to disclose the full extent to which it allowed Plaintiffs … to be targeted by advertisers and marketers," *id*. ¶ 504. But Facebook fully disclosed that it earns revenue through targeted advertising, and Plaintiffs consented to those very activities. *See supra* pp. 11, 22-27.

Plaintiffs identify no cognizable harm they allegedly suffered as a result of targeted advertising they viewed, or how knowing more about Facebook's advertising practices would have helped them to avoid that harm. They say only that they (collectively) "would have not shared their information and content on Facebook to the extent that they did, if at all." Compl. ¶ 509. Again, Plaintiffs do not even specify what they shared on Facebook, much less explain how doing so harmed them. Without *any* specific allegations of harm here, Plaintiffs cannot plausibly allege that they "have sustained damage" "as a result of [any] concealment." *Tenant Healthsystem Desert*, 245 Cal. App. 4th at 844.[15]

3. Privacy claims under California Constitution and Invasion of privacy—intrusion into private affairs

Article I, Section 1 of the California Constitution "sets a high bar for establishing an invasion of privacy claim." *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1038. "First, the complaining party must … demonstrate (1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy." *Lewis v. Superior Court*, 3 Cal. 5th 561, 571 (2017) (citations omitted). "Second, if a claimant satisfies the threshold inquiry, [a] defendant may prevail" if "the invasion of privacy is justified because it substantively furthers one or more countervailing interests." *Id*. at 572.

Plaintiffs' common-law intrusion claim are governed by similar standards. *Hernandez*

[15] To the extent the Complaint alleges that Facebook violated the terms of the 2012 FTC consent decree, *see* Compl. ¶¶ 487, 614, Plaintiffs lack standing to assert such claims. *Dahl, Inc. v. Roy Cooper Co.*, 448 F.2d 17, 20 (9th Cir. 1971) ("Only the Government can seek enforcement of its consent decrees."); *Gajo v. Chicago Brand*, 2017 WL 2473142, at *1 (N.D. Cal. June 8, 2017) ("Courts have held that consumers and members of the public at large may not maintain a private action to enforce the FTCA.").

v. Hillsides, Inc., 47 Cal. 4th 272, 287 (2009). "'[T]he action for intrusion has two elements: (1) [intentional] intrusion into a private place, conversation or matter, (2) in a manner highly offensive to a reasonable person.'" *Taus v. Loftus*, 40 Cal. 4th 683, 734 n.18 (2007) (quoting *Shulman v. Grp. W. Prods., Inc.*, 18 Cal. 4th 200, 231 (1998)). "The tort is proven only if the plaintiff had an objectively reasonable expectation of seclusion or solitude in the place, conversation or data source." *Id*. at 232

Plaintiffs have not demonstrated a legally protected privacy interest. "The California Constitution protects only the 'dissemination or misuse of *sensitive* and *confidential* information.'" *In re Yahoo*, 7 F. Supp. 3d at 1041 (quoting *Hill*, 7 Cal. 4th at 35). Courts have dismissed similar claims where plaintiffs failed to specify exactly what *protected* information was disseminated. *See id.*; *Zbitnoff v. Nationstar Mortg., LLC*, 2014 WL 1101161, at *4 (N.D. Cal. Mar. 18, 2014) (Alsup, J.); *Scott-Codiga v. Cty. of Monterey*, 2011 WL 4434812, at *7 (N.D. Cal. Sept. 23, 2011) (Koh, J.); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1041. Here, Plaintiffs do not allege any specifics regarding the data they shared on Facebook that was allegedly disclosed, let alone that the data is "sensitive."

Plaintiffs have not alleged, and cannot allege, a reasonable expectation of privacy because they consented to the disclosure of the information. *See supra* pp. 22-27.

Plaintiffs have not alleged a *serious* invasion of privacy. "Actionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right." *Hill*, 7 Cal. 4th at 37. "[R]outine commercial behavior" does not constitute an "egregious breach of . . . social norms," *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (2011), and "[e]ven disclosure of very personal information has not been deemed an 'egregious breach of social norms' sufficient to establish a constitutional right to privacy," *In re Yahoo*, 7 F. Supp. 3d at 1038. The social norm undergirding Facebook from the day it was founded until now is, explicitly, sharing. The Court should not hold that Facebook violated a social norm when Plaintiffs do not allege what norm was violated.

Indeed, courts consistently have found a lack of "egregious breach of social norms" in the context of dissemination or failure to secure consumers' sensitive personal information. *See Razuki v. Caliber Home Loans, Inc.*, 2018 WL 2761818, at *2 (S.D. Cal. June 8, 2018) (Burns, J.) ("insufficient security" is not "an egregious breach of social norms"); *In re iPhone Application Litig.*, 844 F. Supp.

2d 1040, 1063 (N.D. Cal. 2012) (no egregious breach even if information were "transmitted without Plaintiffs' knowledge and consent"); *In re Google*, 2013 WL 1283236, at *11 (N.D. Cal. Mar. 26, 2013) (White, J.) (allowing third parties to obtain plaintiffs' PII, transmit it without encryption, and track PII); *Gonzales v. Uber Techs., Inc.*, 2018 WL 1863148, at *10 (N.D. Cal Apr. 18, 2018) (Uber obtained Plaintiff's name and home address); *Yunker v. Pandora Media, Inc.*, 2013 WL 1282980, at *15 (N.D. Cal. Mar. 26, 2013) (White, J.) (Pandora obtained personal information "and provided that information to advertising libraries for marketing purposes" in violation of its privacy policy); *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (Koh, J.) (LinkedIn disclosed to third parties users' numeric LinkedIn ID and LinkedIn browsing histories); *Ruiz*, 540 F. Supp. 2d at 1127–28 (theft of retailer's laptop containing personal information, including the social security numbers, of job applicants). Here, Plaintiffs have not alleged any specific content they shared on Facebook, and therefore have not come close to alleging that disclosing this information was an "egregious breach." And given the nature of the specific information at issue here, all of which was shared with others on Facebook, Plaintiffs fail to allege how it could have been the kind of highly sensitive and confidential information necessary to support their privacy claims.

4. Invasion of privacy – public disclosure of private facts

Plaintiffs have not alleged any actionable invasion of privacy as a result of the public disclosure of private facts. "The elements of this tort are: (1) public disclosure (2) of a private fact (3) which would be offensive and objectionable to the reasonable person and (4) which is not of legitimate public concern." *Moreno v. Hanford Sentinel, Inc.*, 172 Cal. App. 4th 1125, 1129–30 (2009).

Plaintiffs fail to allege any "public" disclosure. A disclosure to a single private entity does not constitute "public" disclosure. *See Del Llano v. Vivint Solar Inc.*, 2018 WL 656094, at *5 (S.D. Cal. Feb. 1, 2018) (Battaglia, J.). Here, the tort "'must be accompanied by publicity in the sense of communication to the public in general or to a large number of persons as distinguished from one individual or a few.'" *Id*. (quoting *Kinsey v. Macur*, 107 Cal. App. 3d 265, 270 (1980)); *see also* Prosser, Law of Torts (4th ed. 1971) § 117, p. 810.

Plaintiffs have failed to allege a "private" fact. "A matter that is already public or that has previously become part of the public domain is not private." *Moreno*, 172 Cal. App. 4th at 1130.

Plaintiffs do not specify whether their privacy settings were anything other than "public" or any specific content or information they allege was disclosed, much less allege that it was private.

Finally, any alleged disclosure does not rise to the level of an egregious breach of social norms, which is governed by the same standard as under the California Constitution. *White v. Social Sec. Admin.*, 111 F. Supp. 3d 1041, 1053 (N.D. Cal. 2015) (Tigar, J.) (quoting *Low*, 900 F. Supp. 2d at 1024–25).

5. Common law right of publicity

Plaintiffs allege that Facebook violated their common law right of publicity by allegedly providing "access" to their "names, like history, photographs, and video." Compl. ¶ 591. That theory bears no resemblance to the common law right of publicity. A violation of publication rights requires, among other things, an "appropriation of [the] plaintiff's name or likeness to defendant's advantage." *Cross*, 14 Cal. App. 5th at 208. Plaintiffs fail to allege any such appropriation. "What the right of publicity holder possesses is ... a right to prevent others from misappropriating the economic value generated ... through the merchandising of the 'name, voice, signature, photograph, or likeness' of the [holder]." *Timed Out, LLC v. Youabian, Inc.*, 229 Cal. App. 4th 1001, 1006 (2014) (quoting *Comedy III Prods., Inc. v. Gary Saderup, Inc.*, 25 Cal. 4th 387, 394 (2001)). The plaintiff must show that the defendant used the plaintiff's identity in a manner related to the plaintiff's "notoriety." *Newton v. Thomason*, 22 F.3d 1455, 1461 (9th Cir. 1994) ("[A]ny commercial advantage that Appellees gained … was totally unrelated to Newton's notoriety as a country/western music performer."). Here, Plaintiffs allege only that Facebook allowed others "*access*" to their "likeness," not that it capitalized on Plaintiffs' publicity. They fail to allege any "notoriety" that could form the basis of a right of publicity claim.

6. Negligence

Plaintiffs' negligence claims fail for multiple reasons.

First, Plaintiffs fail plausibly to allege facts establishing the elements of the claim: (1) a legal duty to use due care; (2) a breach of that legal duty; and (3) injury proximately or legally caused by the breach. *Pirozzi v. Apple Inc.*, 913 F. Supp. 2d 840, 852 (N.D. Cal. 2012) (Rogers, J.).

Plaintiffs cannot establish the core element of duty. They assert that Facebook had a "duty [to]

… ensur[e] that no app developers, device makers or third parties, including Kogan, GSR and Cambridge Analytica, were improperly collecting, storing, obtaining and/or selling Plaintiffs' and Class members' content and information. " Compl. ¶ 547. But that theory is expressly barred by the SRR's specific limitation of liability. *See supra* pp. 32-24.

Nor would there be a duty even absent this contractual waiver. "As a general rule, one owes no duty to control the conduct of another, nor to warn those endangered by such conduct." *Davidson*, 32 Cal. 3d at 203; *see also* Restatement (Second) of Torts §§ 314, 315. Courts in this District have rejected the notion that companies have an affirmative duty to prevent third-party app developers from committing torts. *Pirozzi*, 913 F. Supp. 2d at 852; *In re iPhone Application Litig.*, 2011 WL 4403963, at *9; *In re Google*, 2013 WL 1283236, at *13.

Nor can Plaintiffs ground any tort duty in the applicable contracts because California law does not permit a plaintiff to recover in tort solely on a theory that a contract was negligently performed, absent some independent tort duty. *Applied Equip. Corp. v. Litton Saudi Arabia Ltd.*, 7 Cal. 4th 503, 514–15 (1994); *Stoops v. Abbassi*, 100 Cal. App. 4th 644, 657 n.10 (2002) (plaintiff "may not convert his contract cause of action into a tort").

Plaintiffs' claims also are barred by the economic loss rule. "In the absence of (1) personal injury, (2) physical damage to property, (3) a 'special relationship' existing between the parties, or (4) some other common law exception to the rule, recovery of purely economic loss is foreclosed." *Kalitta Air, L.L.C. v. Cent. Tex. Airborne Sys., Inc.*, 315 F. App'x 603, 605 (9th Cir. 2008) (citations omitted). Numerous courts have held that the rule bars claims that closely resemble those at issue here. In *In re iPhone Application Litigation*, for example, the court dismissed the plaintiffs' negligence claim when they alleged only that they were harmed "as a result of Apple's breach of its duties, which damage is separate and apart from any damage to their iPhones themselves." 844 F. Supp. 2d at 1064; *see also, e.g.*, *In re Lenovo Adware Litig.*, 2016 WL 6277245, at *9 (N.D. Cal. Oct. 27, 2016) (Whyte, J.); *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1055 (N.D. Cal. 2014) (Tigar, J.); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 973 (S.D. Cal. 2014) (Battaglia, J.); *In re Google*, 2013 WL 1283236, at *12–13. So too here.

Plaintiffs have not alleged personal injury or physical damage to property, and they cannot

allege that they were in a "special relationship" with Facebook. "[A] critical foundational requirement for finding a special relationship is whether the third-party transaction was intended to affect the plaintiff in a particular way." *Platte Anchor Bolt, Inc. v. IHI, Inc.*, 352 F. Supp. 2d 1048, 1054 (N.D. Cal. 2004) (Walker, J.). California courts consistently have interpreted this factor to require that a defendant's conduct be unique to the plaintiff, as opposed to generally applicable to all customers. *See Greystone Homes, Inc. v. Midtec, Inc.*, 168 Cal. App. 4th 1194, 1230–31 (2008) (no duty where conduct was "no different from any other purchaser of the *same product*"); *Ott v. Alfa-Laval Agri, Inc.*, 31 Cal. App. 4th 1439, 1455 (1995) ("[N]either the pleadings nor the evidence suggests the [allegedly defective product] was 'intended to affect' the plaintiffs in any way particular to the plaintiffs, as opposed to all potential purchasers of the equipment."). Here, "Plaintiffs have failed to allege a 'special relationship' with [Facebook] beyond those envisioned in everyday consumer transactions, and therefore, negligence is the wrong legal theory on which to pursue recovery for Plaintiffs' economic losses." *In re Sony*, 996 F. Supp. 2d at 969; *see also Stewart v. Electrolux Home Prods., Inc.*, 2018 WL 339059, at *4 (E.D. Cal. Jan. 9, 2018) (O'Neil, C.J.).

Plaintiffs also cannot allege an "appreciable, nonspeculative present harm," which "is an essential element of a negligence cause of action." *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 962 (S.D. Cal. 2012) (Battaglia, J.); *see also Aas v. Superior Court*, 24 Cal. 4th 627, 646 (2000). Courts addressing data-access allegations consistently have found a failure to sufficiently allege harm. *See Razuki*, 2018 WL 2761818, at *2; *In re iPhone I*, 2011 WL 4403963, at *9; *In re iPhone II*, 844 F. Supp. 2d at 1064; *In re LinkedIn User Privacy Litig.*, 932 F. Supp. 2d 1089, 1094 (N.D. Cal. 2013) (Davila, J.); *Low*, 900 F. Supp. 2d at 1032.

7. Breach of contract

"Under California law, to state a claim for breach of contract a plaintiff must plead the contract, plaintiffs' performance (or excuse for nonperformance), defendant's breach, and damage to plaintiff therefrom." *Low*, 900 F. Supp. 2d at 1028. Here, Plaintiffs have not alleged a breach of contract, or that they suffered any damages.

Plaintiffs have not pled a breach. Plaintiffs allege that Facebook breached its promise that it would "not share your content and information with ***advertisers*** without your consent," when it shared

user data with its "business partners" and when it shared friends' data with third-party applications, Compl. ¶¶ 528–530 (emphasis added). But that is not the same thing as sharing user data "with advertisers." *See supra* pp. 10-12. Regarding other third parties like third-party apps and device manufacturers, Plaintiff consented to such sharing. *See* supra pp. 10-12, 22-27. Plaintiffs argue that they are not bound by the Data Use Policy because "Facebook made it unreasonably difficult for users to access the provisions of the … Data Use Polic[y]." Compl. ¶ 533. But, again, as explained *supra* pp. 12-13, 24-26, the Complaint itself shows that the Data Use Policy was readily accessible.

Plaintiffs have not pled contract damages. "Under California law, a breach of contract claim requires a showing of appreciable and actual damage." *Aguilera v. Pirelli Armstrong Tire Corp.*, 223 F.3d 1010, 1015 (9th Cir. 2000). As discussed above, Plaintiffs cannot show that disclosure of their information caused them any economic harm. *See Folgelstrom*, 195 Cal. App. 4th at 994.

8. Breach of the implied covenant of good faith and fair dealing

Because breach of the implied covenant is just a species of breach of contract, *see Carson v. Mercury Ins. Co.*, 210 Cal. App. 4th 409, 429 (2012), this claim fails because Plaintiffs have not alleged viable contract damages. *See supra* p 22. Plaintiffs' implied covenant theory also fails because the actions that they say violated the implied covenant—sharing "content and information" with advertisers, providing data to app developers, device makers and other third parties, and allowing its users "to be targeted by advertisements"—were expressly covered by the Data Use Policy, which was itself part of Facebook's contract with users. Compl. ¶¶ 605–607. "'There can be no implied covenant where the subject is completely covered by the contract.'" *Third Story Music, Inc. v. Waits*, 41 Cal. App. 4th 798, 804 (1995) (quoting *Lippman v. Sears Roebuck & Co.*, 44 Cal. 2d 136, 140 (1955)).

9. Quantum meruit and unjust enrichment

Plaintiffs' quasi-contractual quantum meruit claim is not viable because Plaintiffs concede that they "agreed on express terms" governing their claims. *Hedging Concepts, Inc. v. First All. Mortg. Co.*, 41 Cal. App. 4th 1410, 1419 (1996); *see also* Compl. ¶¶ 526–544. "[A]s a matter of law, a quasi-contract action for unjust enrichment does not lie where ... express binding agreements exist and define the parties' rights." *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 718 (N.D. Cal. 2011) (Ware,

J.). Plaintiffs cannot rely on a quantum meruit theory to "supply 'missing' terms that are not missing." *Hedging Concepts*, 41 Cal. App. 4th at 1419.

10. Unfair Competition

To have statutory standing under the UCL, an individual must "ha[ve] suffered injury in fact and ha[ve] lost money or property as a result of the unfair competition." Cal. Bus. & Prof. Code § 17204; *see Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310 (2011). This requirement is "more stringent than the federal standing requirements." *Troyk v. Farmers Grp., Inc.*, 171 Cal. App. 4th 1305, 1348 n.31 (2009). "Whereas a federal plaintiff's 'injury in fact' may be intangible and need not involve lost money or property, Proposition 64, in effect, added a requirement that a UCL plaintiff's 'injury in fact' specifically involve 'lost money or property.'" *Id*.

Plaintiffs cannot allege economic injury under a "benefit of the bargain" theory because they did not pay for Facebook's services. *See In re Sony*, 903 F. Supp. 2d at 966; *In re Facebook Privacy Litig.*, 791 F. Supp. 2d at 714–15; *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2018 WL 1243332, at *9 (N.D. Cal. Mar. 9, 2018).

Nor can Plaintiffs allege UCL standing based on the purported diminution in value of their personal information. "[A] plaintiff's 'personal information' does not constitute money or property under the UCL." *In re iPhone Application Litig.*, 2011 WL 4403963, at *14; *see, e.g.*, *Sony*, 903 F. Supp. 2d at 966 (the loss of "property value in one's information, do[es] not suffice as injury under the UCL"); *Yunker*, 2013 WL 1282980, at *4 (plaintiff failed to demonstrate Article III "injury-in-fact" "based on the purported diminution in value of his PII"); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d at 714–15 (personal information does not "constitut[e] property for purposes of a UCL claim").

Because Plaintiffs cannot allege a credible risk of identity theft, they also cannot claim injury based on their alleged purchase of identity theft monitoring services. Courts have made clear that such self-inflicted monetary injury is not cognizable where, as here, the underlying risk of identity theft has not been established. *Compare Sony*, 903 F. Supp. 2d at 966 (no injury), *with Corona v. Sony Pictures Entm't, Inc.*, 2015 WL 3916744, *4 (C.D. Cal. June 15, 2015) (Klausner, J.) (injury where plaintiffs purchased monitoring services after the public disclosure of "Social Security numbers, employment files, salary and bank account information, health insurance and other medical information, names,

home and email addresses, visa and passport numbers, and retirement plan data").

Even if Plaintiffs could adequately plead that they lost money or property, they cannot plausibly allege that Facebook's conduct was unfair, unlawful, or fraudulent. As an initial matter, claims for "unfair" conduct under the UCL are available only for competition claims. *See Cel-Tech Commc'n, Inc. v. L.A. Cellular Tel. Co.*, 20 Cal. 4th 163, 187 (1999); *Durell v. Sharp Healthcare*, 183 Cal. App. 4th 1350, 1366 (2010); *Byars v. SCME Mortg. Bankers, Inc.*, 109 Cal. App. 4th 1134, 1147 (2003). Rather, Plaintiffs allege that Facebook's conduct was "unlawful" because it violated the VPPA, SCA, Cal. Civ. Code §§ 1709–1710, and the California Constitution. Compl. ¶¶ 570–571. But Facebook has explained above why those claims must be dismissed. *See supra* pp. 29-32, 34-38. Finally, as to the "fraudulent" prong, Plaintiffs allege that Facebook misled users about the use of their content. Compl. ¶ 572. But as demonstrated above, Facebook disclosed its use of Plaintiffs' data, Plaintiffs consented to that use, and Facebook had no legal duty to disclose additional information. *See supra* pp. 22-27, 34-36.

Finally, Plaintiffs have no right to restitution—a required part of their UCL claim—because Facebook has not taken "money or property" from them "by means of unfair competition." *Kraus v. Trinity Mgmt. Servs., Inc.*, 23 Cal. 4th 116, 126 (2000). And damages are not permitted under the UCL. *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1138 (2003).

F. Plaintiffs' Non-California Claims Should Be Dismissed

Plaintiffs' Complaint also lists 31 causes of action under 23 different states' laws. Yet Plaintiffs concede that California law applies here. Thus, all of the non-California claims must be dismissed.[16]

As the Complaint correctly asserts, "[t]he relevant terms of Plaintiffs' contracts with Facebook … provide[] that all claims that might arise between the user and Facebook would be governed by the laws of California, without regard to conflict-of-law provisions." Compl. ¶ 19. Therefore, as Plaintiffs concede, this "choice-of-law provision establishes that California law applies to Plaintiffs' and all Class Members' claims." *Id.* ¶ 20; *see also id.* ¶ 527 ("Plaintiffs mutually assented to, and therefore were

[16] Facebook reserves its right to address additional grounds for dismissal of these (and any other) non-prioritized claims at a later date, if necessary, pursuant to Plaintiffs' prioritization motion. *See* Dkt. 156, 170.

bound by" the contracts containing the choice-of-law provision); *Nedlloyd Lines B.V. v. Superior Court*, 3 Cal. 4th 459, 464–65 (1992) (en banc) (contractual choice-of-law provisions are enforceable).

Because the parties agree that California law applies, this Court should dismiss any non-California state-law claims. Courts frequently dismiss claims arising from other states' laws when the parties agree that their disputes will be governed by a particular state's law. *See C.M.D. v. Facebook, Inc.*, 2014 WL 1266291, at *5 (N.D. Cal. Mar. 26, 2014) (Seeborg, J.) ("Plaintiffs effectively concede that their claims under Illinois law are dependent on a conclusion that the SRRs—which contain a California choice of law provision—are invalid. Accordingly, … the claims under Illinois law must also be dismissed."); *Song fi Inc. v. Google, Inc.*, 108 F. Supp. 3d 876, 888 (N.D. Cal. 2015) (Conti, J.) (dismissing claims under District of Columbia law when the contract "provides that California law governs"); *see also Cannon v. Wells Fargo Bank, N.A.*, 917 F. Supp. 2d 1025, 1055 (N.D. Cal. 2013) (Chen, J.) (dismissing a California UCL claim because contract chose Florida law); *Armstrong v. Accrediting Council for Continuing Educ. & Training*, 980 F. Supp. 53, 59–60 (D.D.C. 1997) (dismissing a claim under District of Columbia law where contract selected California law).

VI. CONCLUSION

For the foregoing reasons, Facebook respectfully requests that this Court dismiss Plaintiffs' Consolidated Complaint without leave to amend.

DATE: November 2, 2018

Respectfully submitted,

GIBSON, DUNN & CRUTCHER, LLP

By: */s/ Orin Snyder*

Orin Snyder (*pro hac vice pending*)
osnyder@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
200 Park Avenue
New York, NY 10166-0193
Telephone: 212.351.4000
Facsimile: 212.351.4035

Joshua S. Lipshutz (SBN 242557)
jlipshutz@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306
Telephone: 202.955.8500
Facsimile: 202.467.0539

Kristin A. Linsley (SBN 154148)
klinsley@gibsondunn.com
Brian M. Lutz (SBN 255976)
blutz@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
555 Mission Street, Suite 3000
San Francisco, CA 94105-0921
Telephone: 415.393.8200
Facsimile: 415.393.8306

Attorneys for Defendant Facebook, Inc.