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.

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' FIRST AMENDED CONSOLIDATED COMPLAINT

Judge: Hon. Vince Chhabria
Courtroom 4, 17th Floor
Hearing Date: May 29, 2019
Hearing Time: 10:30 a.m.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutional Provisions, Statutes & Rules

Other Authorities

I. INTRODUCTION

A year after the March 2018 news reports about Cambridge Analytica surfaced, Plaintiffs still cannot articulate a viable legal theory. Their second amended complaint now spans 1,442 paragraphs and 413 pages. But the more ink they devote to explaining Facebook's business model and the events of the past 10 years, the more it becomes apparent that they have no case. This latest complaint does not move the needle: Plaintiffs' claims are barred not only by a lack of Article III standing, consent, and failure to meet the requisite statutory or common-law elements—all of which doomed their last complaint—but by the statutes of limitations as well. The Court should dismiss without leave to amend.

Plaintiffs lack Article III standing. At the last hearing, this Court intimated that Plaintiffs had not established standing on the basis of "increased risk of fraud/identity theft [or] 'economic harm.'" Pretrial Order No. 16, Dkt. 243 at ¶ 1 (Jan. 31, 2019); Tr. 156:3-5. Instead, the Court inquired whether Article III standing might be established based on alleged "privacy" violations alone—that is, whether Facebook's sharing of Plaintiffs' information with a third party is enough. It is not. The case law is clear that putative plaintiffs must do more than simply allege that their "privacy" was violated or their information shared: they must allege an actual or imminent real-world injury, whether tangible or intangible, arising from the sharing of information. That is why, for example, courts have spent so much time grappling with standing even in clear-cut data-breach cases, closely examining whether the type of information that was shared is sufficient to give rise to a credible risk of identity theft, as well as the likely intentions of the actor who obtained the information. *See, e.g.*, *Beck v. McDonald*, 848 F.3d 262, 275 (4th Cir. 2017); *Antman v. Uber Techs., Inc.*, 2015 WL 6123054, at *10-11 (N.D. Cal. Oct. 19, 2015); *Kamal v. J. Crew Grp., Inc.*, --- F.3d ----, 2019 WL 1087350, at *7 (3d Cir. Mar. 8, 2019). If the sharing of information alone were enough to establish standing, that inquiry would be unnecessary. It is also why all common-law privacy torts require proof of harm, *see* Restatement (Second) of Torts §§ 652A, 652H (1977), and why the Supreme Court held that the unauthorized sharing of ZIP codes, "without more," is not enough for Article III standing unless it "could work any concrete harm," *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1550 (2016). Again, it is the consequent harm or injury that matters, not the sharing alone.

The allegations in this case make clear that no harm resulted from the sharing of Plaintiffs' information with third-party apps—no actionable identity theft, emotional distress, or economic injury; just targeted advertising, which Plaintiffs have admitted is not a harm at all. Prior Compl. ¶ 110 ("There is nothing wrong with targeted advertising."). Moreover, the Complaint makes clear that the nature of the data being shared with third-party apps is not the type of highly offensive and sensitive information that could give rise to a common-law privacy violation, in part because, by definition, it is information the user has already shared with potentially hundreds or thousands of people—the very people who then re-shared the data with the apps.

The Court also inquired whether Plaintiffs' consent to the sharing of their information with third-party apps should be considered as part of the standing inquiry. The answer is clear—Yes. Again, hornbook law teaches that the very nature of a privacy-related injury turns on the absence of consent. Thus, where a plaintiff consents to the sharing of his private information, then by definition the plaintiff "has not suffered an 'invasion of privacy'" and lacks "Article III standing." *Larroque v. First Advantage LNS Screening Sols., Inc.*, 2016 WL 4577257, at *5 (N.D. Cal. Sept. 2, 2016). That is why the statutes on which Plaintiffs rely—the Stored Communications Act ("SCA") and Video Privacy Protection Act ("VPPA"), for example—all define the prohibited conduct as the *unconsented* sharing of certain information. *See* 18 U.S.C. § 2702(b)(3) (under SCA, providers allowed to disclose information with "consent"); *id.* § 2710(b)(2)(B) (under VPPA, disclosure allowed with "written consent"). The Ninth Circuit's decision in *Eichenberger v. ESPN, Inc.*, 876 F.3d 979 (9th Cir. 2017), which this Court asked about the last time around, confirms that consent is critical to the standing inquiry—the Ninth Circuit held that the plaintiff had standing, in part, because he "did not *consent* to Defendant's sharing his information with a third party." *Id.* at 981 (emphasis added).

Here, the opposite is true. Plaintiffs have admitted that third-party apps could obtain users' data only if "the request complie[d] with the user's and/or friends' privacy settings." Prior Compl. ¶¶ 121-22. They are still bound by that admission even though they deleted it from their latest complaint. And, in any event, they continue to admit that "[i]n order to gain access to nonpublic content and information, App Developers needed to request permission from the App User." Compl. ¶ 408; *see also id.* ¶ 414 ("App Developers sought all permissions, including the permissions that gave access to

Friends' content and information, from the App User when she downloaded or logged into the App."). These admissions regarding consent defeat Plaintiffs' standing.

Plaintiffs consented to the sharing of their information. On the merits, Plaintiffs' own allegations again defeat their claims. As this Court explained at the last hearing, "if you read the words [of the contracts], you come away knowing that even if you limit your settings so that you're sharing only with friends, these third-party apps can communicate with your friends and get all of the information that your friends have access to .... All of that seems to be disclosed." Tr. 135:3-11. Plaintiffs continue to admit that they are bound by Facebook's user terms (the "Statement of Rights and Responsibilities," or "SRR"). Compl. ¶ 937. They admit that "[a]t all relevant times, the SRR told users, 'You own all the content and information you post on Facebook, and you can control how it is shared through your privacy [hyperlinked] and application [hyperlinked] settings.'" *Id.* ¶ 593. They admit that, consistent with the SRR, "[t]he Data Policy … discussed in more detail how users could use their Privacy Settings and App Settings to control whether and how other users or other entities could access one's own content and information." *Id.* ¶ 594. And they admit that "Facebook told users that by using their App settings, they could prevent an App from accessing their data via a Friend that used the App. *This was true at all relevant times*." *Id.* ¶ 599 (emphasis added). Even beyond the two principal contracts, the Complaint is replete with screenshots showing exactly how users could control the sharing of their information with apps, along with disclosure after disclosure alerting users to the availability of such settings. *E.g., id.* ¶¶ 346-73. As a matter of law, these admissions are fatal. Users were told everything they needed to know, and therefore consented to the sharing of their information with third-party apps.

Plaintiffs' claims are time-barred. Plaintiffs' latest allegations plead them out of court for an additional reason: They now make clear that this entire case is barred by the various statutes of limitations that govern Plaintiffs' claims. As Plaintiffs admit, "an FTC complaint from 2011 ('FTC Complaint') filed against Facebook outlines many of the same issues" that form the basis of their claims—the sharing of friends' data with apps, the difference between the Privacy Settings page and the Apps Settings page, the manner in which users could "restrict the information that their Friends' Apps could

access," and how apps used data. Compl. ¶ 381. Plaintiffs' extensive reliance on the 2011 FTC complaint dooms their lawsuit because it demonstrates that the public was put on notice of these matters at least 8 years ago, too long ago to be actionable.

* * *

The issues Plaintiffs raise are better handled by the branches institutionally equipped to engage in sensitive policy making—Congress and executive-branch regulators—and not in one-off litigation where Plaintiffs ask courts to recognize new and ahistorical privacy rights. Plaintiffs have now, for the second time, failed to state any viable injury or claim against Facebook, and the Court should dismiss without leave to amend.

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 and because Plaintiffs' claims are time-barred.

III. BACKGROUND

As Plaintiffs now allege, this controversy began in 2009, when Facebook "changed its Privacy Policy to designate additional items of user information as public"—a change that resulted in a "public outcry" and "[p]rompt[ed] FTC Action." Compl. ¶¶ 385, 388, 673 & Heading IV.B.5; *see also* Complaint ¶ 33, *In re Facebook, Inc.* (F.T.C. Dec. 17, 2009) (Complaint filed by Electronic Privacy Information Center), https://bit.ly/2INKhDP. The FTC subsequently investigated and issued a complaint, which it resolved by entering into the 2012 Consent Order that Plaintiffs allege "bear[s] on what reasonable consumers expected from Facebook." Compl. ¶ 672. And the Consent Order expressly allowed the re-sharing of a user's data with third-party apps by the user's friends. *In re Facebook, Inc.*, No. C-4365, at 4 (F.T.C. Aug. 10, 2012), https://bit.ly/2J9YtXv.

Six years passed before the first of more than 30 class actions was filed against Facebook in connection with its app-sharing practices. After Plaintiffs filed a consolidated complaint in September 2018, *see* Dkt. 152-2 ("Prior Compl."), Facebook moved to dismiss for lack of standing and failure to

state a claim. Dkt. 184-1 ("Prior MTD"). On February 1, 2019, the Court heard argument on Facebook's motion, set forth some of the complaint's deficiencies, and invited Plaintiffs to try again, on the "assum[ption] that the amended complaint will, absent extraordinary circumstance, reflect the plaintiffs' best and final shot at alleging standing and stating a claim." Dkt. 247.

Plaintiffs' Amended Consolidated Complaint fares no better—and actually fares worse. The 150 pages that Plaintiffs added to the allegations do not solve the chronic problems the Court identified in February, but they do introduce new problems. Here are the primary changes Plaintiffs made:

- **Privacy settings.** Most of the named Plaintiffs now allege their privacy settings for various categories of the information that they shared on Facebook, asserting that certain categories of data were at various times set to "Friends" or "Friends of Friends." Only four Plaintiffs allege that they had any data set to "Only Me"—meaning that none of their Facebook Friends could view the relevant data—but these changes are alleged to have been made in 2018 or at an unknown time, and they do not allege that any app was able to access this "Only Me" data. *See* Compl. ¶¶ 51, 70, 162, 228. Plaintiffs do not allege how many friends or friends-of-friends they had, but studies show the median Facebook user has 200 friends and 31,170 friends-of-friends.[1]

- **Risk of economic injury.** Some named plaintiffs allege that they provided financial information to Facebook, though they do not allege that any of that information was given to any third party. Compl. ¶ 194. Certain plaintiffs also allege that they were subject to increased "phone solicitations," but do not explain how that would increase the risk of identity theft. *E.g.*, *id.* ¶ 159.

- **Advertising.** All Plaintiffs allege they have watched advertisements connected to the 2016 Presidential election, but they do not describe any advertisement or explain how they were harmful. *E.g.*, Compl. ¶¶ 42, 584.

- **Recollection of registration process.** Although Plaintiffs do not "recall being prompted to read or reading the Terms of Service or the Data Policy during the registration process," *e.g.*, Compl. ¶ 94, they acknowledge that they and Facebook "mutually assented to, and therefore were bound by," the Terms of Service. *Id.* ¶ 937.

- **Device manufacturers.** Plaintiffs again allege that Facebook violated their rights by sharing information with device manufacturers who created versions of Facebook on mobile devices (manufacturers that Plaintiffs refer to as "Business Partners"). Compl. ¶¶ 483-493. But Plaintiffs do not allege what user information was available to such manufacturers, or that any device manufacturer used any information improperly. And only two Plaintiffs allege that they or any of their friends used a device made by any of the identified device manufacturers, *id.* ¶¶ 226, 256 (iPhones), and

[1] A. Smith, *What People Like and Dislike About Facebook*, Pew Research Center (Feb. 3, 2014), https://pewrsr.ch/2Lmp7ZS; K.N. Hampton, et al., *Why Most Facebook Users Get More Than They Give* 5, Pew Research Center (Feb. 3, 2012), https://pewrsr.ch/1GTrJow. The Court may take judicial notice of news reports. *Heliotrope Gen., Inc. v. Ford Motor Co.*, 189 F.3d 971, 981 n.18 (9th Cir. 1999).

those two Plaintiffs do not allege that they shared on Facebook the "contact numbers and calendar entries" that the Complaint alleges Apple was able to obtain. *Id*. ¶¶ 226-233, 256-263, 563.

- **Facebook messenger.** Several Plaintiffs include new allegations describing the topics of some messages that they sent via Facebook Messenger, *e.g.*, Compl. ¶ 51, but they do not include any additional allegations to substantiate their belief that Cambridge Analytica obtained their messages, *id*. ¶¶ 424, 513, when only 1,500 of the 300,000 downloading users provided permissions to obtain messages.

- **"Whitelisted" apps.** Plaintiffs make several allegations regarding so-called "whitelisted apps" that, they claim, were allowed to access user data beyond that available to other apps. Compl. ¶¶ 494-517. But despite identifying these companies by name, *id*. ¶¶ 506, 508, 510, 516, Plaintiffs have not alleged that they or any of their friends used any of those apps.

IV. ARGUMENT

A. Plaintiffs Still Fail to Allege Any Cognizable Injury to Support Standing

Plaintiffs added more than 150 pages to their Complaint, but they still fail to allege any actual or imminent harm—either tangible or intangible. *Spokeo v. Robins*, 136 S. Ct. 1540, 1548 (2016); *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61 (1992). Mere invocation of an amorphous right to "privacy" is not enough. For Article III purposes, the alleged injury, whether tangible or intangible, must "actually exist" and cannot be "abstract." *Spokeo*, 136 S. Ct. at 1548 (quotation marks omitted). Where, as here, Plaintiffs' own factual allegations demonstrate that their privacy interests have not been injured (because of the nature of the data and the fact that they consented to the sharing of the data) and the sharing of their data did not result in any concrete, real-world harm (because it was used only for targeted advertising), there is no Article III standing.

1. Plaintiffs allege no tangible injury-in-fact

The Court already recognized that Plaintiffs did not "adequately allege[]" either "risk of fraud/identity theft" or any "economic harm" in the Prior Complaint. Dkt. 243 ¶ 1. Nothing in the Amended Complaint changes that conclusion. Plaintiffs' identity-theft allegations contain no new relevant information—they still fail to allege that Facebook released, or that any app obtained, any information such as "social security numbers," *Krottner v. Starbucks Corp*., 628 F.3d 1139, 1140 (9th Cir. 2010), that gives an identity thief "all the information he needed to open accounts or spend money in the plaintiffs' names," *In re Zappos.com, Inc*., 888 F.3d 1020, 1026 (9th Cir. 2018); *see* MTD at 17-18

(collecting cases); *see* Compl. ¶¶ 784-789.[2] Plaintiffs also have done nothing to support any theory of claimed economic harm. *See id*. ¶¶ 778-83, 790-801. Their claimed "out of pocket costs" are the very type of speculative injuries that the Supreme Court has found insufficient to establish standing. *See Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 157-58 (2014); *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013); Prior MTD at 20-21; *see also* Tr. 156:3-5.

Nor do Plaintiffs have standing to raise claims as to any apps or device manufacturers *other* than Kogan's app—including whitelisted apps. Plaintiffs list the names of these apps and device manufacturers, *e.g.*, Compl. ¶¶ 484, 930, but, other than Kogan's app, they do not identify any app or device manufacturer that allegedly obtained their data. No Plaintiff, for instance, alleges that he or she used Facebook through any Acer system or Huawei, *see id*. ¶ 484 (naming those companies as "Business Partners"), so no Plaintiff has standing to assert injuries arising from alleged data sharing with those companies. Although two Plaintiffs allege that they used a device running Apple's operating system, they state only that Apple obtained "contact numbers" and "calendar entries," which those plaintiffs do not allege they shared on Facebook. *Id*. ¶¶ 226-233, 256-263, 563. As to Facebook Messenger, some plaintiffs add new detail regarding messages they sent at some point during the class period, but no Plaintiff alleges facts suggesting that Kogan's app actually obtained their messages. *See* Tr. 28:22-29:2 ("But there's no reason to believe that ... the content of [Plaintiffs'] communications in Facebook Messenger were intercepted or disclosed."); *id.* at 36:7-16 ("I'm not sure that it's safe to assume that the contents of the plaintiffs' messages through the instant messaging system were acquired by Kogan or anyone else."); Comp. ¶¶ 424, 513 (alleging that App Developers *could* access Facebook Messenger content but failing to allege that any *did*, much less that Plaintiffs used any of the Apps that did).

[2] Plaintiffs allege they have "experienced additional security risks such as phishing attempts, increased phone solicitations, incidents of fraud or misuse, efforts by hackers trying to access or log in to their Facebook accounts, Friend requests from trolls or cloned or imposter accounts, and other interference with their Facebook accounts," Compl. ¶ 788, and, in one case, that a Plaintiff experienced "unauthorized access to his bank account." *Id.* ¶¶ 34, 59. But they fail to explain how the data allegedly shared—*e.g.*, "photographs with geolocation data and time stamps, ... Plaintiffs' religious and political beliefs, their relationships, posts, and the pages they had liked," *id*. ¶ 748—could have had anything to do with the alleged events underlying the Complaint. *See* Prior MTD at 17-19 & nn. 8, 9.

2. Plaintiffs fail to allege any cognizable privacy injury

Plaintiffs alternatively allege that Facebook injured their privacy interests by "disseminat[ing] or caus[ing] the dissemination of content and information that Plaintiffs reasonably believed was private." Compl. ¶ 748.[3] But Plaintiffs' own allegations refute any cognizable privacy injury. As an initial matter, Plaintiffs' allegations make clear that they authorized the sharing of their data with third-party apps. *See infra*, pp. 19-32. Privacy interests can be harmed only if disclosures are *unauthorized*, so consent—as determined by the facts alleged in the Complaint[4] —defeats standing at the pleading stage. And even if that were not the case, Plaintiffs still lack standing because the type of harm Plaintiffs allege is not recognized as a privacy injury at common law or under any applicable statute.

a. Consent Is A Standing Issue In Cases Involving Privacy

Consent goes to the heart of the jurisdictional standing analysis here. The absence of consent is the cornerstone of the very type of privacy injury being alleged. It is not merely an affirmative defense left for the merits.

Standing often "turns on the nature and source of the claim asserted." *Warth v. Seldin*, 422 U.S. 490, 500 (1975). The Supreme Court explained in *Spokeo* that merits questions—both the elements of a statute and the ways in which English and American courts have resolved such cases *on the merits*—are part of the jurisdictional question whether a plaintiff has standing to assert in federal court claims resting on intangible harm. 136 S. Ct. at 1549. Here, the core legal right at stake in Plaintiffs' claims is the right to keep certain private information to themselves. But if Plaintiffs consented to the sharing of data, they relinquished any privacy interest in that information and cannot be harmed—in the real-

[3] Plaintiffs' attempt to claim privacy injuries arising from alleged data sharing with Tinder, Brayola, Hot or Not, and Girls Around Me, Compl. ¶ 749, are irrelevant. Not a *single* Plaintiff alleges use of those apps, so they cannot claim any injuries arising from alleged data sharing with those apps.

[4] At the hearing, the Court asked whether the proper standard of analysis for the standing inquiry is to "assum[e] that the plaintiff would win on the merits," and then ask "were they injured?" Tr. 3:15-20. Facebook respectfully submits that this is not the correct analysis. As with any motion to dismiss, the question is whether Plaintiffs' allegations, if proven, would demonstrate standing. *See Leite v. Crane Co.*, 749 F.3d 1117, 1121 (9th Cir. 2014) (a "'facial' attack" to subject matter jurisdiction "accepts the truth of the plaintiff's allegations but asserts that they 'are insufficient on their face to invoke federal jurisdiction.'" (citation omitted)); *see also, e.g.*, *Warth*, 422 U.S. at 500 ("Although standing in no way depends on the merits of the plaintiff's contention that particular conduct is illegal, it often turns on the nature and source of the claim asserted." (citation omitted)).

world, concrete, Article III sense—if the information is shared in a way that is consistent with that consent. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 218 (1890) ("The right to privacy ceases upon the publication of the facts by the individual, or with his consent."). The nature of the alleged injury is what makes consent a standing issue.

That is why federal courts routinely dismiss similar privacy-related claims for lack of standing where the plaintiffs consented to the alleged conduct. If a plaintiff "consent[ed] to have her consumer report pulled, reviewed, and considered for purposes of employment"—and thus no "unauthorized disclosure" occurred—"Plaintiff has not suffered an 'invasion of privacy' or any other concrete harm. This is exactly the situation that the Supreme Court indicated cannot confer Article III standing." *Larroque v. First Advantage LNS Screening Sols., Inc.*, 2016 WL 4577257, at *5 (N.D. Cal. Sept. 2, 2016).[5] In that situation, "Plaintiff … agreed to the release of her private information, eliminating any argument that her privacy was somehow invaded." *Id.*; s*ee also, e.g.*, *Nokchan v. Lyft, Inc.*, 2016 WL 5815287, at *5-6 (N.D. Cal. Oct. 5, 2016) (finding no basis for Article III standing where plaintiff authorized defendant company to obtain his personal information and then claimed an "invasion of privacy"; theory of standing was defeated by plaintiff's consent); *In re Michaels Stores, Inc., Fair Credit Reporting Act (FCRA) Litig.*, 2017 WL 354023, at *9-10 (D.N.J. Jan. 24, 2017) ("the applicant's consent … vitiates any claim of a privacy violation" under FCRA); *Stacy v. Dollar Tree Stores, Inc.*, 274 F. Supp. 3d 1355, 1364 (S.D. Fla. 2017) ("[W]hen an employee consents to a background check …, her knowing consent vitiates any claim of a privacy injury" and "cannot satisfy Article III's requirement of a concrete injury in fact.").

Requiring the absence of consent as part of the standing inquiry makes sense. Private information not kept private is not a proper basis on which to support the injury requirement that is built into the standing analysis. If consensual sharing could give rise to standing, then anyone could claim

[5] *Larroque* involved FCRA claims. The FCRA was enacted out of concern that employers' ability to obtain consumer reports on job applicants without authorization "may create an improper invasion of privacy," S. Rep. No. 104-185, at 35 (1995), so its purpose is to "protect consumer privacy," *Safeco Ins. Co. of Am. v. Burr*, 551 U.S. 47, 52 (2007).

an "injury"—and therefore have standing to sue in federal court—every time an email provider transmits their emails to the intended recipients, on the theory that the email provider disclosed the data and information contained in the email. The provider would then be left to argue at the merits stage that the sender consented to the data transfer. That cannot be, and is not, the law.[6]

b. The Mere Sharing of Data, Without More, Is Not a Privacy Injury

Even if the Plaintiffs had plausibly alleged that they did not consent to the sharing of their data with third-party apps, they would still lack standing because the sharing they allege did not result in any concrete, real-world injury. An Article III injury must be "distinct and palpable, as opposed to merely abstract," *Whitmore v. Arkansas*, 495 U.S. 149, 155 (1990) (internal quotation, citation, and alteration omitted), in order to avoid "water[ing] down the fundamental requirements of Article III," *Clapper*, 568 U.S. at 416.

The mere fact that someone's information is shared with someone else does not give rise to a cognizable privacy injury. A "party that has brought statutory or common law claims based on nothing more than the unauthorized disclosure of personal information" has no "standing" on that basis alone. *In re Google, Inc. Privacy Policy Litig.*, 2012 WL 6738343, at *5 (N.D. Cal. Dec. 28, 2012); *see also id.*, at *4 (courts "must heed the constraints Article III imposes" even when Plaintiffs raised "questions regarding Google's respect for consumers' privacy"). Otherwise, every plaintiff who alleges that his or her data was compromised in a data breach would automatically have standing. But they do not. Courts routinely reject that theory of harm and dismiss such cases for lack of standing, where the sharing does not result in a credible risk of real-world harm. *See, e.g.*, *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, 2016 WL 6523428, at *5 (S.D. Cal. Nov. 3, 2016) (mere sharing of personal identifying information insufficient on its own to confer standing in data breach case); *Antman v. Uber Techs., Inc.*, 2015 WL 6123054, at *11 (N.D. Cal. Oct. 19, 2015) ("theft of names and driver's licenses" was insufficient to create standing where complaint lacked allegations of an "obvious, credible risk of identity theft that risks real, immediate injury"); *Low v. LinkedIn Corp.*, 2011 WL 5509848, at *6 (N.D.

[6] The Court asked whether, under Facebook's argument, a plaintiff would ever be able to satisfy Article III's requirement of standing but nevertheless lose on the merits because he consented to the challenged disclosure. Tr. 87:1-7, 88:7-10. Facebook submits that the standing inquiry will normally come out the same way as the merits question in most cases that turn on privacy claims and consent.

Cal. Nov. 11, 2011) (no standing where plaintiff had not alleged that his "sensitive" personal information had been exposed to the public). In these cases, the courts carefully consider, as part of the jurisdictional analysis, the nature of the data being shared and the intent of the party that obtained the data. If the data did not pose a sufficient risk of real-world harm, or the party obtaining the information did not have an intent to engage in identity theft or cause other injury using the data, there is no standing. *See Antman*, 2015 WL 6123054, at *11.

Plaintiffs' Complaint fails for the same reason. Plaintiffs concede that the reason Cambridge Analytica obtained their information was to engage in targeted advertising, which they admit is not wrongful. Prior Compl. ¶ 110; s*ee Cohen v. Facebook, Inc.*, 798 F. Supp. 2d 1090, 1097 (N.D. Cal. 2011) (dismissing under 12(b)(6) allegation that Facebook shared plaintiffs' names and likenesses without their knowledge or consent because, detached from any showing of additional injury, it did not "cause[] them any cognizable harm"); *id.*, 2011 WL 5117164, at *2-3 (N.D. Cal. Oct. 27, 2011) (dismissing amended complaint because plaintiffs failed to allege "they were somehow harmed"); *id.*, 2012 WL 13036789, at *2 (N.D. Cal. Apr. 10, 2012) (clarifying that second dismissal "was based on plaintiffs' lack of standing under Article III" "upon finding no injury-in-fact"). Moreover, the type of information allegedly shared with third-party apps (names, birthdays, hometown, education, activities, status updates, *see, e.g.*, Compl. ¶ 368) is not the kind of information that gives rise to a credible risk of concrete harm; it does not include, for example, social security numbers, account numbers, passwords, or credit card information that may pose an imminent and concrete threat of identity theft. *See Krottner*, 628 F.3d at 1140; *In re Zappos.com*, 888 F.3d at 1026. There is no allegation that Kogan, or any other app developer, used Facebook user data to inflict real-world harm on any of the Plaintiffs. Disclosure of information "without any concrete consequence" is insufficient to open the courthouse door. *Hancock v. Urban Outfitters, Inc.*, 830 F.3d 511, 514 (D.C. Cir. 2016) (no standing for consumer protection claim based solely on alleged disclosure of zip code); *see also Beck v. McDonald*, 848 F.3d 262, 275 (4th Cir. 2017) (disclosure of information on laptop and pathology reports, "without more, cannot confer Article III standing"); *Low*, 2011 WL 5509848, at *5-6.

This understanding of the requirements for privacy-related harms dates back to the common law, which recognzed that not every dissemination of allegedly private information is actionable. As

the Supreme Court has instructed, a plaintiff's alleged intangible harm is typically insufficient to establish Article III standing unless it bears a "close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." *Spokeo*, 136 S. Ct. at 1549. Courts look to four common-law privacy torts to determine whether intangible privacy harms qualify as concrete for Article III standing: unreasonable intrusion upon a person's seclusion, appropriation of a person's name or likeness, public disclosure of private facts, and false light. *E.g.*, *Rivera v. Google, Inc.*, -- F. Supp. 3d --, 2018 WL 6830332, at *9 (N.D. Ill. Dec. 29, 2018). Plaintiffs' alleged injuries bear no resemblance to any of these historically recognized torts.

1. Intrusion upon seclusion. This tort requires intentional intrusion "upon the solitude or seclusion of another or his private affairs or concerns … if the intrusion would be highly offensive to a reasonable person." Restatement (Second) of Torts § 652B. Plaintiffs have not alleged any intrusion into their private affairs; rather, the information at issue is all data they already shared with a broad circle of friends and even strangers (friends of friends). *See, e.g.*, *Felix v. State Comp. Ins. Fund*, 2007 WL 3034444, at *8 (C.D. Cal. Oct. 3, 2007) ("comings and goings from the office" were "not private affairs"); *Goldman v. Time, Inc.*, 336 F. Supp. 133, 138 (N.D. Cal. 1971) (no expectation of privacy where plaintiffs "made themselves readily available for both the text and photographs which eventually appeared in the Life Magazine article"). Nor could the disclosure of information such as page likes, which are designed to be communicated to other people, be "highly offensive to a reasonable person." Disclosure of far more private information, such as private medical records and the identity of undercover police, has been found insufficient. *See, e.g.*, *Fletcher v. Price Chopper Foods of Trumann, Inc.*, 220 F.3d 871, 875-79 (8th Cir. 2000) (medical information relating to workers' compensation claim obtained by subterfuge); *Ross v. Burns*, 612 F.2d 271, 272-74 (6th Cir. 1980) (photographs and name of undercover police officer not highly offensive, despite safety risk); *Bass v. Anoka Cty.*, 998 F. Supp. 2d 813, 824-25 (D. Minn. 2014) ("address, photograph, date of birth, weight, height, eye color and driver identification number … though personal, [are] not particularly sensitive or intimate in nature," and "individuals routinely turn over such information"). The "highly offensive standard … is reserved for truly exceptional cases of intrusion," *Med. Lab. Mgmt. Consultants v. Am. Broad. Cos.*, 30 F. Supp. 2d 1182, 1189 (D. Ariz. 1998) (quotation omitted), and this is not such as case. *See Low v. LinkedIn*

Corp., 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (holding disclosure of user ID and user's browsing history was not an egregious breach of social norms, and collecting similar cases).

2. Public disclosure of private facts. This tort requires publicity of private facts that are "of a kind that … would be highly offensive to a reasonable person." Restatement (Second) of Torts § 652D. The tort is inapplicable for several reasons.

First, Facebook never made a *public* disclosure. "[I]t is not an invasion of the right of privacy … to communicate a fact concerning the plaintiff's private life to a single person or even to a small group of persons." *Id.* cmt. a. According to the Complaint, Facebook disclosed information to Kogan, not to a large group. *E.g.,* Compl. ¶ 449. Courts routinely reject public disclosure claims, no matter how sensitive the information purportedly disclosed, where "[t]he facts were not made known to the general public, nor were they made known to so many people that the matter must be considered substantially certain to become one of public knowledge." *Dancy v. Fina Oil & Chem. Co.*, 3 F. Supp. 2d 737, 740 (E.D. Tex. 1997); *see also Yoder v. Ingersoll-Rand Co.*, 31 F. Supp. 2d 565, 570 (N.D. Ohio 1997) (disclosure of HIV status to "three people at most" does not amount to "publicity"); *Washburn v. Gymboree Retail Stores, Inc.*, 2012 WL 3818540, at *16 (W.D. Wash. Sept. 4, 2012) (publication to an individual and then to the State Human Rights Commission not "a communication to the public at large"); *Robins v. Conseco Fin. Loan Co.*, 656 N.W.2d 241, 246 (Minn. Ct. App. 2003) (disclosure of plaintiff's "credit information" to a third party "was not sufficient publicity").

Second, the facts disclosed were not strictly private. "There is no liability when the defendant merely gives further publicity to information about the plaintiff that is already public." Restatement (Second) of Torts § 652D cmt. b. Here, Plaintiffs already shared the information allegedly disclosed with large groups of friends or even strangers—even if they didn't make the information available to the public at large. *See, e.g.*, *Cottrell v. Smith*, 299 Ga. 517, 533 (2016) (extramarital affair already exposed on blogs and to Facebook friends was not a private fact); *Sipple v. Chronicle Publ'g Co.*, 154 Cal. App. 3d 1040, 1047 (1984) ("prior to the publication of the newspaper articles in question" the plaintiff's sexual orientation "had been known by hundreds of people in a variety of cities").

Third, even if (contrary to the facts) Plaintiffs had kept the information to themselves, and then

Facebook had disclosed it to the world, its disclosure would not have been "highly offensive to a reasonable person." Courts consistently have held disclosures of analogous—or even substantially more sensitive—information to be insufficiently offensive to support a claim of public disclosure of private facts. *See, e.g.*, *Johnson v. Sawyer*, 47 F.3d 716, 732 (5th Cir. 1995) (name, address, and job title); *Stern v. Great W. Bank*, 959 F. Supp. 478, 483 (N.D. Ill. 1997) (financial and employment information); *Matter of Med. Lab. Mgmt. Consultants*, 931 F. Supp. 1487, 1493 (D. Ariz. 1996) (place of work).[7] The information Facebook allegedly disclosed is nothing like the sorts of "highly offensive" facts recognized at common law. *See, e.g.*, *Reid v. Pierce Cty.*, 136 Wash. 2d 195, 198, 210-12 (1998) ("photographs of corpses of Plaintiffs' deceased relatives"); *Doe v. Mills*, 212 Mich. App. 73, 77, 82 (1995) (defendants carried signs outside abortion clinic bearing plaintiffs' names, stating that plaintiffs "were about to undergo abortions," and "implor[ing] them, inter alia, not to 'kill their babies'").

3. Appropriation of name or likeness. This tort only arises when a defendant uses a plaintiff's name or likeness "to advertise [its] business or product." Restatement (Second) of Torts § 625C cmts. a & b. Plaintiffs' theory of the case is inconsistent with appropriation. The animating thesis of the Complaint is not that Facebook used Plaintiffs' likenesses to advertise Facebook's products to other users, but that it allowed other information (such as Plaintiffs' page likes) to be used to serve Plaintiffs themselves with targeted ads. Plaintiffs have not, and "cannot, offer any evidence that Facebook used [their] name[s] or likeness[es] in any way." *Cross v. Facebook, Inc.*, 14 Cal. App. 5th 190, 210 (2017).

4. False light. Plaintiffs do not allege that anything disclosed by Facebook was false. *See* Restatement (Second) of Torts § 652E; *see, e.g.*, *Flowers v. Carville*, 310 F.3d 1118, 1132 (9th Cir. 2002) ("False light, like defamation, requires at least an implicit false statement of objective fact."); *Griley v. Nat'l City Mortg.*, 2010 WL 3633766, at *6 (E.D. Cal. Sept. 14, 2010) (dismissing false light claim because "plaintiff fails to identify any statements made by [defendant] that placed him in a false light"). To the extent Facebook disclosed any false information about Plaintiffs, it was only because Plaintiffs themselves supplied it. And even if Facebook had cast one or more Plaintiffs in a false light,

[7] *See also, e.g.*, *Morgan By & Through Chambon v. Celender*, 780 F. Supp. 307, 310 (W.D. Pa. 1992) (names and photos of abuse victims, even if obtained illegally); *Wells v. Thomas*, 569 F. Supp. 426, 437 (E.D. Pa. 1983) (details of separation agreement); *Fisher v. State ex rel. Dep't of Health*, 125 Wash. App. 869, 880 (2005) (prescribed medications).

there still would be no basis for a tort claim because, for reasons explained above, no disclosure made by Facebook was "highly offensive to a reasonable person." Restatement (Second) of Torts § 652E. Finally, torts analogous to false light are actionable only when a plaintiff "can demonstrate actual damages"—that is, "some actual, quantifiable pecuniary loss." *Doe v. Chao*, 540 U.S. 614, 625-26 (2004). Nothing in the Complaint suggests that Plaintiffs can do that here.

c. Plaintiffs' alleged statutory violations do not provide standing

Plaintiffs also cannot rely on the bare allegation that Facebook's conduct violates one or more statutes. "[T]he requirement of injury in fact is a hard floor of Article III jurisdiction that cannot be removed by statute." *Summers v. Earth Island Inst.*, 555 U.S. 488, 497 (2009); *see Raines v. Byrd*, 521 U.S. 811, 820 n.3 (1997) ("Congress cannot erase Article III's standing requirements by statutorily granting the right to sue to a plaintiff who would not otherwise have standing."). In *Spokeo*, the Court made clear that "Article III standing requires a concrete injury even in the context of a statutory violation." 136 S. Ct. at 1549. If an injury is intangible—like the Plaintiffs' alleged privacy harm—the Court looks to two factors: "history and the judgment of Congress." *Id.* As to history, "it is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." *Id.* Congress's "judgment" is "instructive and important" because "Congress is well positioned to identify intangible harms that meet minimum Article III requirements." *Id.* Here, neither history nor Congress's judgment supports a finding that the sharing of Plaintiffs' information with third-party apps gives them standing.

(i) Relationship to Historically Recognized Harm

For the reasons discussed above, Plaintiffs' allegations do not fit within any of the four common-law privacy-related claims, and cannot create Article III standing—irrespective of consent. In addition, Plaintiffs' theory that they suffered harm from disclosure *even with* their consent is inconsistent with the common law. Consent "creates an absolute privilege" with respect to "any publication, either of matter that is personally defamatory or of matter that invades privacy." Restatement (Second) of Torts § 652F; *see also Shoots v. iQor Holdings US Inc.*, 2016 WL 6090723, at *5 (D. Minn. Oct. 18, 2016) ("American courts have long recognized that … consent to an invasion of privacy is a complete defense to that act."). The right of privacy simply "does not exist where the person has published

the matter complained of, or consented thereto." *Melvin v. Reid*, 112 Cal. App. 285, 290 (1931); *see also* Warren & Brandeis, *supra*, at 218 ("The right to privacy ceases upon the publication of the facts by the individual, or with his consent."). As the Third Circuit recently held, privacy-based common law torts "protect[] against *unauthorized* disclosure[] of information," meaning the "harm underlying" these torts "transpires when a third party gains *unauthorized* access to a plaintiff's personal information." *Kamal*, 2019 WL 1087350, at *7 (emphases added) (alleged violation of Fair and Accurate Credit Transactions Act did not confer standing). That common law privacy torts are tethered to consent further underscores that *the harm itself*—and thus injury-in-fact for standing purposes—requires the absence of consent.

(ii) Congress's Judgment

As for Plaintiffs' SCA and VPPA claims, they do not track back to the common law for reasons already discussed, and the legislature has not elevated statutory violations of these federal statutes into previously unrecognized harms. Just as *Spokeo* held that the FCRA does not make all inaccuracies an injury-in-fact because "not all inaccuracies cause harm or present any material risk of harm," 136 S. Ct. at 1550, the SCA cannot be read to make *all* disclosures the basis of an injury-in-fact. Congress has not conveyed any express judgment that someone in Plaintiffs' position has Article III standing to sue. The SCA targets only *unconsented* disclosures—and consent can come from either the originator (here, Plaintiffs) or the recipients (here, Plaintiffs' Facebook friends who had access to Plaintiffs' data). 18 U.S.C. § 2702(b)(3) ("A provider … may divulge the contents of a communication … with the lawful consent of the originator or an addressee or intended recipient of such communication"); *accord Facebook, Inc. v. Superior Court*, 4 Cal. 5th 1245, 1276-77 (2018); *In re Facebook, Inc.*, 923 F. Supp. 2d 1204, 1206 (N.D. Cal. 2012). Thus, even if Plaintiffs had plausibly alleged that *they* did not consent to their friends sharing their data with apps, they concede that their friends (the recipients of their communications) *did* consent to such sharing. Compl. ¶ 408 ("In order to gain access to nonpublic content and information, App Developers needed to request permission from the App User."); *id.* ¶ 414 ("App Developers sought all permissions, including the permissions that gave access to Friends' content and information, from the App User when she downloaded or logged into the App.").

The SCA also does not exhibit congressional judgment about *who* may bring suit. The SCA

provides only that a "person aggrieved" by a knowing violation of the statute may sue, 18 U.S.C. § 2707(a), but this language does not elevate an intangible injury to one cognizable under Article III. As the Court has explained, Congress could signal its judgment that a statutory violation constitutes an injury in fact by defining a class of persons deemed to be injured by a statutory violation, as in *Spokeo*, where the statute provided that a person who commits a knowing violation "with respect to any consumer is liable to *that consumer*." 15 U.S.C. § 1681n(a) (emphasis added). In contrast, a statutory reference to a "person aggrieved" reflects at most an intent to create a cause of action for those who *already* have Article III standing. *See Thompson v. N. Am. Stainless, LP*, 562 U.S. 170, 177-78 (2011) (under the APA, "person aggrieved" refers to a smaller subset of people than those who have Article III standing, even "excluding plaintiffs who might technically be injured in an Article III sense"). It says nothing about which particular injuries are sufficiently concrete under Article III.

Similarly, the VPPA does not confer standing whenever a disclosure occurs. Like the SCA, the VPPA targets only *unauthorized* disclosures. 18 U.S.C. § 2710(b)(2)(B) ("A video tape service provider may disclose personally identifiable information concerning any consumer to any person with the informed, written consent … of the consumer …."). Like the SCA, the text of the VPPA indicates Congress's judgment that only persons who did not consent are harmed—and thus only persons who did not give consent could have suffered an Article III injury.

Eichenberger confirms this conclusion. In *Eichenberger*, the Ninth Circuit analyzed the statutory text and held that the VPPA "protects generally a consumer's substantive privacy interest in his or her video-viewing history," 876 F.3d at 983, and that the plaintiff had standing because he "did not consent to Defendant's sharing his information with a third party," *id.* at 981; *see also id.* at 983-84 (the "*substantive* right to privacy" "suffers"—is harmed—only when the defendant "discloses *otherwise private information*"—that is, without consent (second emphasis added)). Where there is consent, there can be no harm flowing from a disclosure because lack of consent is built into the very *definition* of the harm. *See Bassett v. ABM Parking Servs., Inc.*, 883 F.3d 776, 782 (9th Cir. 2018) ("We recently held [in *Eichenberger*] that a statute barring video service providers from disclosing knowingly *and without consent* a consumer's 'personally identifiable information' to third parties establishes a 'substantive right to privacy.'" (emphasis added)); *cf., e.g.*, *Santana v. Take-Two Interactive Software, Inc.*,

717 F. App'x 12, 15 (2d Cir. 2017) (dismissing for lack of standing because "Plaintiffs concede that [the statute] is implicated only if their biometric data is collected or disseminated *without their authorization*," and plaintiffs consented to facial scans at issue) (emphasis added); *Am. Farm Bureau Fed'n v. EPA*, 836 F.3d 963 (8th Cir. 2016) (the "concrete and particularized injury in fact" was "the *nonconsensual* dissemination of personal information") (emphasis added).[8]

The California Constitution and California statutes on which Plaintiffs rely also do not help them satisfy the Article III standing requirements. "[T]he California Constitution protects only the 'dissemination or misuse of *sensitive* and *confidential* information.'" *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1041 (N.D. Cal. 2014) (quoting *Hill v. NCAA*, 7 Cal. 4th 1, 35 (1994)). The information Plaintiffs allege was disclosed—pages, likes, and other data they already shared with their friends—does not fit the bill. *See infra* pp. 40-42. And the only California statutes Plaintiffs cite, Civil Code §§ 1709-1710 (CCP), Business & Professions Code § 17200, *et seq.* (UCL), have nothing to do with privacy. Sections 1709 and 1710—which create a cause of action for "deceit"—allow a plaintiff who "alter[ed] his position to his injury or risk" to sue a defendant for deceit "for any *damage* which he thereby suffers." CCP § 1709. And the UCL provides a cause of action only where an individual "suffered injury in fact and has lost money or property as a result of [] unfair competition." Cal. Bus. & Prof. Code § 17204; *Kwikset Corp. v. Superior Ct.*, 51 Cal. 4th 310 (2011); *see also Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1058 (dismissing UCL claims in data privacy case for lack of standing because plaintiffs failed to show loss of money or property). These statutes reflect not any legislative decision to create standing for intangible injuries, but rather the longstanding and uncontroversial principle that those who have suffered money damages—tangible injuries—from wrongful conduct have standing to sue.

[8] Even if the VPPA requires consent to be given in a particular way—for example, "in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer." 18 U.S.C. § 2710(b)(2)(B)(i)—a deficiency in this technical sense would be a procedural rather than substantive violation of the VPPA. Such a "bare procedural violation, divorced from any concrete harm," cannot support Article III standing. *Spokeo*, 136 S. Ct. at 1549.

B. Plaintiffs Consented to All of the Alleged Practices

Whether for standing or merits purposes (or both), Plaintiffs' allegations are clear: they consented to each of the alleged practices they attack. The SRR and Data Use Policies[9] clearly explained how Facebook would collect and share data on its platform, and Plaintiffs consented to each of the challenged actions—either expressly (because the Data Use Policy was part of Facebook's contract with its users), or impliedly (because Facebook's contracts, layered website disclosures, accessible settings, and repeated explanations and instructions about data-sharing put users on notice of Facebook's data practices).

1. Facebook's policies explained to users exactly how data sharing and advertising worked on Facebook

Sharing information—with both friends and apps—is a central purpose of Facebook. As Plaintiffs acknowledge, Facebook "enabl[es] 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. ¶ 264. Two primary documents govern Facebook's and users' sharing of data: Facebook's Statement of Rights and Responsibilities ("SRR") and its Data Use Policy (previously referred to as the "Privacy Policy"). *See id.* ¶ 652 (Facebook's Data Policy governs "how [Facebook] collect[s] and can use your content and information"). Plaintiffs concede that the Data Use Policy complements the SRR by "discuss[ing] in more detail how users could use the Privacy Settings and App Settings to control whether and how other users or other entities could access one's own content and information." *Id.* ¶ 594. The SRR and the Data Use Policy address all of the policies and conduct Plaintiffs' Complaint characterizes as wrongful, including how Facebook shares data with third-party apps, serves 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 others.

As the Ninth Circuit recently held in analyzing these two documents and affirming the dismissal of a complaint against Facebook, "[Facebook's] Terms and Policies contain[ed] numerous disclosures

[9] Facebook's policies are incorporated by reference in the Complaint and may be considered. *Coto Settlement v. Eisenberg*, 593 F.3d 1031, 1038 (9th Cir. 2010). The exhibits cited are attached to the declaration of Michael Duffey ("D.D."). ECF. No. 187; *see also* ECF No. 236.

related to information collection" such that a "reasonable person viewing those disclosures would understand" the practices at issue in that case, thereby "constitut[ing] Plaintiffs' consent." *Smith v. Facebook, Inc.*, 745 F. App'x 8, 8-9 (9th Cir. 2018). The same conclusion applies here.

a. Sharing data with third-party apps. Throughout the relevant time period, Facebook's Data Use Policy informed users that third-party apps may access data not only from users who download the app, but also from their friends who download the app, if the users' settings allowed for such re-sharing. For example, beginning in September 2011, the Data Use Policy featured a bolded and underlined subheading, "Controlling what is shared when the people you share with use applications," that expressly told users that information they shared with friends could be shared by those friends, including with third-party apps: "Just like when you share information by email or elsewhere on the web, information you share on Facebook can be reshared. 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." D.D., Ex. 45 at 9. As this Court noted at the last hearing, "if you read the words [of the contracts], you come away knowing that even if you limit your settings so that you're sharing only with friends, these third-party apps can communicate with your friends and get all of the information that your friends have access to …. All of that seems to be disclosed." Tr. 135:3-11.

Plaintiffs try to evade these disclosures by arguing that prior versions of the Data Use Policy insufficiently disclosed sharing with third-party apps. That is incorrect and irrelevant. Users are bound by the then-current versions of policies, *infra* at pp. 25-26, and Kogan's app began operating in 2013. In any event, earlier versions of the policy plainly informed users that their friends could share any information they could see with apps. Before December 2009, for example, Facebook explained that "if a user's Friends used third-party applications, those applications 'may access and share certain information about you with others in accordance with your privacy settings.'" Compl. ¶ 626. And after December 2009, Facebook emphasized to users the common-sense rule that users who see your information can re-share that information: "You understand that information might be re-shared or copied by other users …. When you post information on another user's profile or comment on another user's post, that information will be subject to the other user's privacy settings." D.D., Ex. 39 at 2.

Plaintiffs also quote language in certain versions of the Data Use Policy where Facebook explained that "if a user's 'friend grants specific permission to [an] application or website,' the application or website 'will only be allowed to use that content and information *in connection with* that friend.'" Compl. ¶ 597. Plaintiffs contend this was false because Cambridge Analytica was "able" to obtain user data from Kogan. *Id.* ¶ 598. But Plaintiffs are conflating what apps were "allowed" to do under their contract with Facebook with what they were *able* to do. The disclosure means what it says: applications are contractually obligated to use the data they receive—whether the user's own data or the user's friends' data—only in connection with enhancing the user's own experience on the app. Apps must accept this obligation by agreeing to the platform policy. D.D., Ex. 23 at 5-6. But Facebook does not guarantee that apps won't *be able* to misuse user data in some way, *see* D.D., Ex. 45 at 8 (Dec. 11, 2012 Data Use Policy) (apps are not "controlled by" Facebook); D.D., Ex. 21 at 1 (Oct. 4, 2010 SRR) (Facebook "not responsible" for third party actions), nor could it: a company cannot promise that its business partners won't violate the terms of their own contracts. *See Smith*, 745 F. App'x at 9 (rejecting argument that Facebook "could not have gained consent" to collecting data where "the healthcare websites' privacy policies promised not to share data with third parties" because "Facebook's Terms and Policies make no such assurance, and Facebook is not bound by promises it did not make"). Plaintiffs do not allege that Facebook's platform rules *allowed* Kogan to sell user data to Cambridge Analytica—which they did not. And Kogan violating his own agreement with Facebook does not make Facebook liable to Plaintiffs, and is not inconsistent with Facebook's disclosure.

Plaintiffs also allege that Facebook removed users' privacy settings from metadata such that apps could not limit disclosure of users' photos consistent with those settings. Compl. ¶¶ 426-442, 607-612. But the disclosure that Plaintiffs quote—"We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information," *id.* ¶ 612—makes no reference to a user's privacy settings on Facebook. Rather, the disclosure clearly states that the *application's* user agreement controls how the data will be used. The app must comply with Facebook's platform policies and its own agreement with the user.

b. Advertising. Plaintiffs allege that they did not consent to advertising in two respects: (1) they did not consent to *sharing* their data with apps that are also advertisers, and (2) Facebook did

not disclose that third parties would use "content and information … aggregated with other information to build psychographic profiles on Facebook users." Compl. ¶¶ 603-606, 619. Both theories fail.

Facebook promised not to "give your content or information to advertisers ***without your consent***." Compl. ¶ 603 (emphasis added). Plaintiffs admit that the only "advertisers" who received user information were third-party apps and device manufacturers—entities with whom users had separately consented to share data. *Id*. ¶¶ 605-606. Thus, Facebook did not violate its policies here because sharing with this category of third parties was done "with[] your consent." In addition, the information shared with those apps and device manufacturers could not be used for advertising purposes, as Facebook's platform policies make clear. D.D., Ex. 23 at 5 (June 8, 2012 SRR) ("You will not include data you receive from us concerning a user in any advertising creative.").

Plaintiffs' separate contention regarding the creation of "psychographic profiles" by third parties is simply an argument against targeted advertising, as to which Plaintiffs previously admitted "[t]here is nothing wrong." Prior Compl. ¶ 110. Users know that Facebook is in the business of serving targeted advertisements, as it discloses in its policies. The Data Use Policy in effect during the relevant period 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). Facebook also explained that it provides information to advertisers, but only "when we have removed from it anything that personally identities you or combined it with other information so that it no longer personally identifies you." *Id.* at 11. Finally, Facebook told users that it uses the information it receives to help with targeted advertising: "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 the category." *Id.* at 11-12. Plaintiffs do not say what more they believe Facebook should have disclosed.

c. Device manufacturers. Plaintiffs allege that Facebook did not disclose that it shared information with its "Business Partners"—the device manufacturers who "buil[t] Facebook's Platform

on different devices and operating systems" prior to the implementation of the Facebook Mobile app that is widely used today. Compl. ¶ 486. But Facebook did disclose that practice, telling users that it would "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 [and] serve photos and videos." D.D., Ex. 45; Compl. ¶ 616.[10] Plaintiffs admit device manufacturers were helping to host Facebook's website by "building Facebook's Platform" on their own systems. *Id.* ¶ 486. This comports with common sense; the device you use to access a website might need to access your data to provide the service you are requesting. Plaintiffs do not allege that any of the service providers did anything with the data other than use it to provide Facebook to the user, at the user's own request.

d. Disclosures about third parties. Plaintiffs allege that third parties—including Kogan and Cambridge Analytica—misused user data and that Facebook should be held responsible. But Facebook's Data Use Policy explicitly 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," D.D., Ex. 21 at 1 (Oct. 4, 2010 SRR); Compl. ¶¶ 221-222. Consistent with these controls and disclosures, the SRR 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.

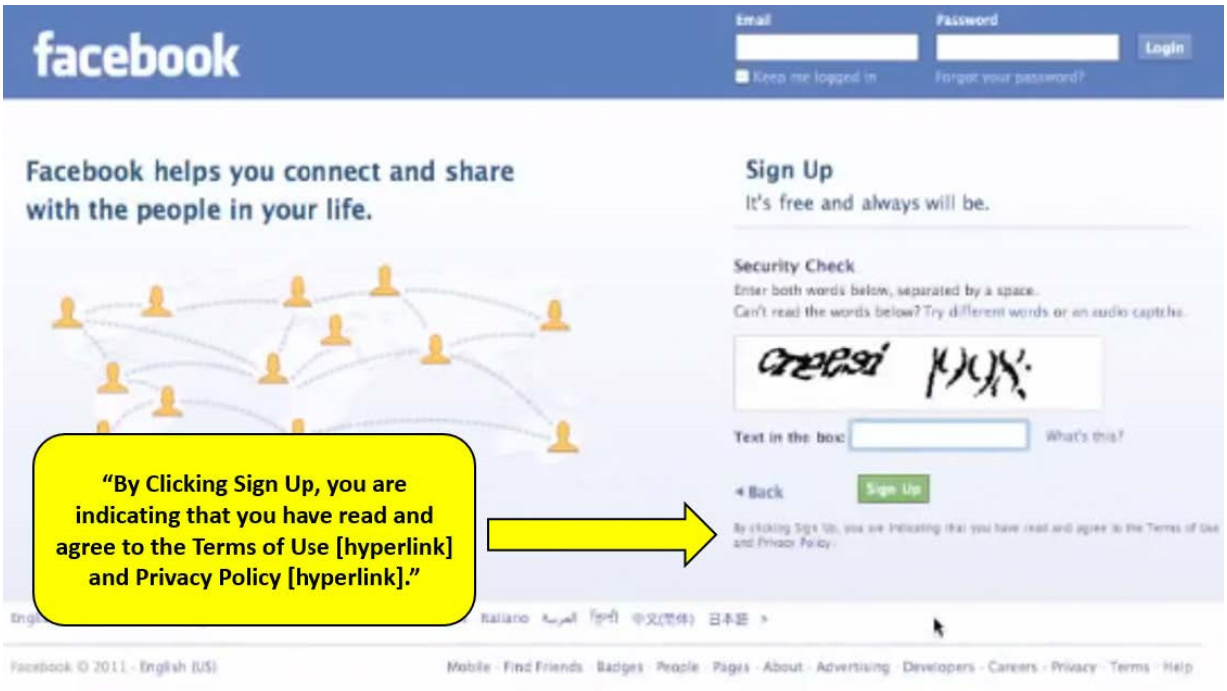
D.D., Ex. 21 at 3 (Oct. 4, 2010 SRR). This provision also expressly waived California Civil Code § 1542. *Id.* Plaintiffs cannot plausibly allege that Facebook violated its user agreements by failing to prevent third-party harm when it made no such promise. *Smith*, 745 F. App'x at 9 ("Facebook's Terms and Policies make no such assurance, and Facebook is not bound by promises it did not make.").

[10] 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." Prior Compl. ¶ 277.

2. Plaintiffs expressly consented to practices disclosed in the relevant policies

Because the documents reflect a binding contract between Facebook and its users, Plaintiffs expressly consented to each of the practices in question when they signed up for a Facebook account. It does not matter that users were required to click on links in order to review the policies. *See, e.g.*, *Fteja v. Facebook, Inc.*, 841 F. Supp. 2d 829, 840 (S.D.N.Y. 2012) ("Here, Fteja was informed of the consequences of his assenting click and he was shown, immediately below, where to click to understand those consequences. That was enough."); *Moule v. United Parcel Serv. Co.*, 2016 WL 3648961, at *5 (E.D. Cal. July 7, 2016) (plaintiff "manifested assent to the [defendant's] Terms" when the "screens asked the user to confirm acceptance of the ... Terms" before accepting and, "immediately below this statement, and above the 'Yes' button, a hyperlink to the 'Terms and Conditions' was provided"). Plaintiffs' assertions that these policies are ineffective fail as a matter of law.

First, Plaintiffs allege Facebook's contracts were not prominent enough to manifest assent. Compl. ¶ 649. But under the law, users are expected to read and familiarize themselves with terms of service. California courts presume a plaintiff has read the relevant contract, *see Constantian v. Mercedes-Benz Co.*, 5 Cal. 2d 631, 634 (1936), and a plaintiff is "chargeable with knowledge of its contents," *Taussig v. Bode & Haslett*, 134 Cal. 260, 266 (1901). That is why courts "routinely uphold" terms of service where the defendant's website requires an affirmative action to indicate consent to terms, *Meyer v. Uber Techs., Inc.*, 868 F.3d 66, 78 (2d Cir. 2017), as Facebook's website did here, Compl. ¶¶ 647-648. *See Nevarez v. Forty Niners Football Co.*, 2017 WL 3492110, at *11 (N.D. Cal. Aug. 15, 2017) (plaintiff expressly consented to website's terms where defendant "notified [plaintiffs] that their use of the [defendant's] [w]ebsite was governed by the [defendant] [w]ebsite's [Terms of Use], and Plaintiffs were provided with a hyperlink to the [Terms] when Plaintiffs registered for the" account); *Meyer*, 868 F.3d 66 at 78 (defendant provided reasonable notice "as a matter of California law" when it displayed "the warning that '[b]y creating an Uber account, you agree to the TERMS OF SERVICE & PRIVACY POLICY,'" with "the hyperlinks to the Terms and Conditions and Privacy Policy" placed "directly below the buttons for registration" in small font).



Plaintiffs assert they are not bound by Facebook's Data Use Policy. Compl. ¶ 642. But they concede they *are* bound by Facebook's SRR, *id.* ¶ 937, which incorporates the Data Use Policy by reference by informing users at sign-up that they should read that policy and that it explains "how we collect and can use your content and information." *Id.* ¶ 652. To incorporate a document into a contract, the "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) (quotation omitted), and 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." *Wolschlager v. Fid. Nat'l Title Ins. Co.*, 111 Cal. App. 4th 784, 791 (2003). Indeed, Plaintiffs' allegation that users did not agree to the Data Use Policy at sign-up—because the disclosure occurred *after* users had already entered personal information on a prior sign-up screen—makes no sense because those same concerns apply to the SRR, Compl. ¶¶ 644-650, which Plaintiffs concede constituted a binding contract.

Finally, Plaintiffs again assert that users are bound only by the versions of the polices that existed on the date they registered for Facebook. Compl. ¶¶ 623-625. But companies have the right, and should be encouraged, to update their policies periodically, and Plaintiffs admit that Facebook notified users of these changes by posting new versions of the policies, including on the Facebook Site Governance page. *See id.* ¶ 623; Prior Compl. ¶ 291. Continued use of the service after the publication of

these updates bound users to their terms. *E.g.*, D.D., Ex. 24 (Dec. 11, 2012 SSR) ("Your continued use of Facebook following changes to our terms constitutes your acceptance of our amended terms."); *see In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155, 1167 (N.D. Cal. 2016) (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).

3. Plaintiffs impliedly consented to the challenged practices

The Data Use Policy and SRR are standalone contracts that adequately disclosed all of the complained-of practices, and Plaintiffs assented to them. Even if the Court disagrees, the Complaint demonstrates that Plaintiffs gave their implied consent to each of the challenged practices. "[I]mplied consent rests on a theory of waiver, such as when a person uses a service after being informed of a policy of disclosure and monitoring." *Suzlon Energy Ltd. v. Microsoft Corp.*, 671 F.3d 726, 731 (9th Cir. 2011); *see also United States v. Van Poyck*, 77 F.3d 285, 292 (9th Cir. 1996) (explaining that the Wiretap Act permits courts to find consent "implied in fact from 'surrounding circumstances indicating that the [defendant] knowingly agreed to the surveillance'" (citation omitted)). "In the typical implied in fact consent scenario, a party is informed" of certain practices, and consent is implied by continued use "after receiving notice." *Nei Contracting & Eng'g, Inc. v. Hanson Aggregates Pac. Sw., Inc.*, 2016 WL 4886933, at *3 (S.D. Cal. Sept. 15, 2016).

When evaluating whether a party impliedly agreed to be bound the terms of an agreement with a website, courts look not only to the terms of the agreements, but also to whether the website's "general design" alerted users to the existence of these policies—for example, whether policy hyperlinks were posted in contrasting colored text. *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1177 (9th Cir. 2014). "Even if Facebook hid its practice, as long as users heard about it from somewhere and continued to use the relevant features, that can be enough to establish implied consent." *Campbell v. Facebook Inc.*, 315 F.R.D. 250, 266 (N.D. Cal. 2016) (explaining consent in the context of a motion for class certification); *see also Backhaut v. Apple Inc.*, 2015 WL 4776427, at *14 (N.D. Cal. 2015) (same).

Here, Plaintiffs received notice of Facebook's data-sharing practices in multiple ways that together establish implied consent. First, as explained above, the terms of the policies themselves put users on notice of each of the practices at issue, using all-caps disclaimers and top-line disclosures.

Second, Facebook made these policies readily accessible to users. Plaintiffs admit that Plaintiffs were shown links to both the SRR and Data Use Policy when they signed up for their accounts. Compl. ¶¶ 646-650; *see Meyer*, 868 F.3d at 78 (finding "design of the screen and language" provided reasonable notice where hyperlink to Terms and Conditions was "directly below the buttons for registration" and in a font that contrasted with background, even though "the sentence is in a small font"). And this policy was available at the bottom of every single page under the "Privacy" hyperlink, written in blue text over a gray background. Compl. ¶¶ 658, 660. Plaintiffs complain that at some point Facebook changed the layout of the Data Use Policy, requiring users to click on subheadings to view portions of the Data Use Policy. *Id.* ¶¶ 658-662. But those subheadings clearly directed users to relevant sections, including (1) a section titled "**Sharing with other websites and applications**[:] Find out about the ways your information is shared with the games, applications and websites you and your friends use off Facebook"; and (2) a subsection titled "**Controlling what is shared when the people you share with use applications**[:] Control how the people you share with share your information when they use games, applications, and websites." *Id.* ¶¶ 660-661.

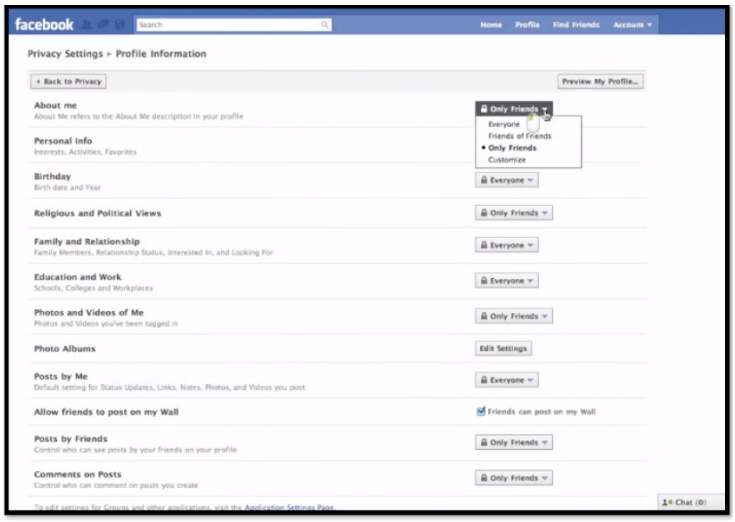
Third, Facebook's website was layered with disclosures explaining how users could control data-sharing with apps. For example, Facebook's Application Settings gave users granular control over what was shared, contained *more* disclosures, and was readily accessible to users. As Plaintiffs acknowledge, "Facebook told users that by using their App Settings, they could prevent an App from accessing their data via a Friend that used the App. This was true at all relevant times." Compl. ¶ 599. The App Settings provided users with clear instructions regarding how third-party apps might access user data and included a series of controls regarding "Apps others use." *Id.* ¶ 364. It allowed users to control two different components of privacy related to apps. It enabled users to select how apps that they installed could access their information, and it also allowed users to change their privacy settings with respect to apps their friends installed. It informed users: "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, and allowed users to check off which categories of data they wished to allow their friends to share with apps. *Id.* ¶ 368. The point of the App Settings' granular

information was to give users *more control*, so they could make precise selections about what to share.

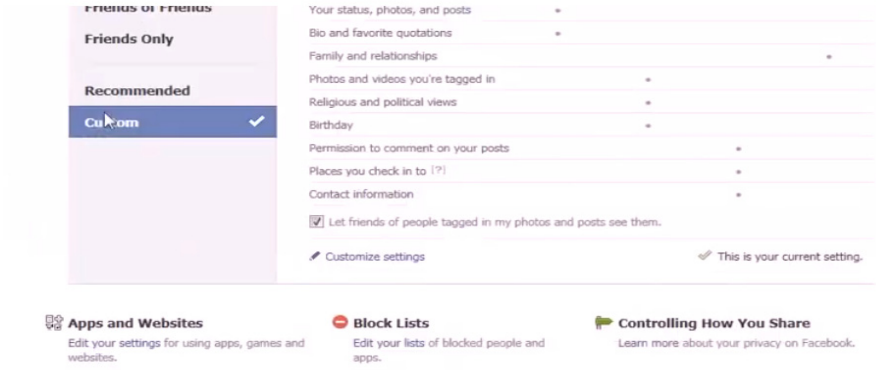
The same screen also informed users that "[i]f you don't want apps and websites to access other categories of information (like your friend list, gender or info you've made public) you can turn off all [p]latform apps." Compl. ¶ 368; *id.* ¶ 372 (image depicting "App Settings" page where users could turn off all apps). And on the "App Settings" page to turn off Platform, Facebook again informed users that certain information was "always publicly available, including to apps (Learn Why). Apps also have access to your friends list and any information you choose to make public." *Id.* ¶ 372.

Plaintiffs suggest that Facebook confused users with two different sets of controls—Privacy Controls, for sharing with users on Facebook, and App Settings, for sharing with apps off Facebook, Compl. ¶¶ 342-43—but their own allegations show that Facebook repeatedly informed users that App Settings and Privacy Controls were different. Plaintiffs admit this distinction was prominently disclosed in the SRR's first sentences: "you can control how [content and information you post on Facebook] is shared through your privacy [hyperlinked] and application [hyperlinked] settings." *Id.* ¶ 593. This admission itself is fatal to Plaintiffs' theory, as they admit that the SRR made this disclosure "at all relevant times," *id.* ¶ 593, and that the SRR represented a binding contract, *id.* ¶ 937. Logically, the policies *should* be different: Privacy Controls govern who sees users' information on Facebook, while App Settings govern what those people can do with the information off Facebook.

Facebook also structured the layout of its website to ensure that App Settings were clearly visible to any user who actually changed his or her Privacy Controls—as the Complaint alleges many Plaintiffs did. For example, the 2010 "Privacy Settings" screenshot includes an instruction below the Privacy Controls that "[t]o edit settings for Groups and other applications, visit the Application Settings Page." Compl. ¶ 346.

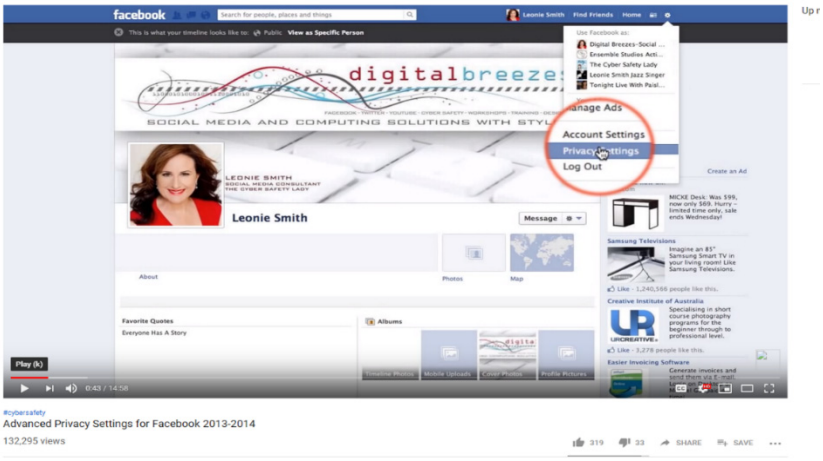


Similarly, when the screen "changed slightly … around 2010 to 2011," *id.* ¶ 348, the disclosure screen included a prompt for "Apps and Websites: Edit your settings for using apps, games and websites."[11]

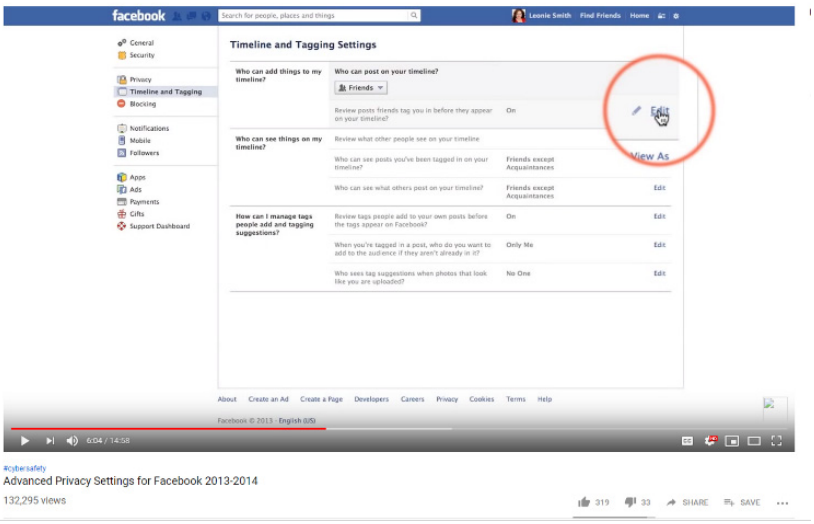


[11] *See* Kvchosting, *How to Manage Your Privacy Settings on Facebook*, YouTube (Mar. 25, 2013), https://www.youtube.com/watch?v=O378rrYcjlc (shot from 1:27). This screen shot is incorporated by reference because it is from the same YouTube video as is Plaintiffs' screen shot in ¶ 348. *See* Prior Compl. ¶ 186 n.45; *see also* Compl. ¶ 388.

And from "some time in 2012 ... until April 2018," the "Privacy" and "Apps" controls were separate tabs on the same interface, under the "Privacy Settings" header. *Id.* ¶ 349. So users could access both App Settings and Privacy Controls by clicking on "Privacy Settings" from a drop-down menu.[12]



This link brought users directly to a page containing tabs for "Privacy" and also for "Apps" on a left-hand toolbar. Compl. ¶ 349. Plaintiffs' own allegations show the design would attract a user's attention. Any Plaintiff who modified his or her Timeline settings, *id.* ¶ 914, would have seen that the "Privacy" tab did not contain all privacy controls.[13] In other words, Plaintiffs who visited this page would have known that they might want to click on other tabs, including "Apps."



[12] *See* L. Smith, Advanced Privacy Settings for Facebook 2013-2014, YouTube (Jan. 17, 2013), https://www.youtube.com/watch?v=OPRFQyGq-yM (at 0:43). This screen shot is taken from the same YouTube video that Plaintiffs rely on for the screen shot in ¶ 364; *see also* Compl. ¶ 364 n.88-89.

[13] *See* L. Smith, *supra* n.12 (at 6:04).

Fourth, the well-publicized[14] allegations in the 2011 FTC Complaint informed users that Facebook employed two separate sets of controls—app settings and privacy settings—and that Facebook shared data with third-party apps even if users' privacy settings were set to "Friends Only." Complaint, *In re Facebook, Inc.*, No. C-4365 ¶¶ 9, 18 (Nov. 29, 2011) ("FTC Complaint"), https://bit.ly/2OFeJyN. Plaintiffs' repeated references to the FTC Complaint, Consent Order, and media publicity show that they "could have learned of" Facebook's practices from outside sources, even if the Court disagreed that Facebook's own disclosures were adequate (which they were). *In re Google Inc. Gmail Litig.*, 2014 WL 1102660, at *16 (N.D. Cal. Mar. 18, 2014) ("All materials to which an individual has notice are relevant to consent, not just contractual agreements," including terms of service, defendant webpage, targeted hyperlinks, and media sources). In short, the "panoply of sources from which" a user "could have been put on notice" of Facebook's practices—ranging from the contracts, layered disclosures on Facebook's website, readily accessible instructions on how to change settings, and government and media reports—manifests implied consent. *Backhaut*, 2015 WL 4776427, at *14-15.

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

The first complaint in this case was filed in March 2018, but the facts underlying Plaintiffs claims were known many years ago—as Plaintiff's latest Complaint makes even more apparent—and the statutes of limitations for those theories have run.[15] For 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.

[14] *E.g.*, S. Sengupta, *F.T.C. Settles Privacy Issue at Facebook*, N.Y. Times (Nov. 29, 2011), https://nyti.ms/2F1CzRg; C. Kang, *Facebook settles FTC privacy complaint, agrees to ask users' permission for changes*, Wash. Post (Nov. 29, 2011), https://wapo.st/2HiuEmi; S. Raice & J. Angwin, *Facebook 'Unfair' on Privacy*, Wall St. J. (Nov. 30, 2011), https://on.wsj.com/2TPGJoM; E. Peralta, *Facebook Settles with FTC On Charges It Deceived Users On Privacy*, NPR (Nov. 29, 2011), https://n.pr/2Cl4Th0.

[15] SCA, 18 U.S.C. § 2707(f) (two years); VPPA, 18 U.S.C. § 2710(c)(3) (two years); invasion of privacy, negligence, and gross negligence, Cal. Code. Civ. P. § 335.1 (two years); Deceit by Concealment or Omission, Cal. Civ. Proc. Code § 338(d) (three years); breach of contract, Cal. Civ. Proc. Code § 337.1 (four years); UCL, Cal. Bus. & Prof. Code § 17208 (four years); implied covenant of good faith and fair dealing, *Eisenberg v. Ins. Co.*, 815 F.2d 1285, 1292 (9th Cir. 1987) (two years); quantum meruit, *Melchior v. New Line Prods., Inc.*, 106 Cal. App. 4th 779, 793 (2003) (limitations period governed by limitations applicable to underlying wrong); Cal. Civ. Proc. Code § 339 (two years for "an action upon" unwritten "contract, obligation or liability").

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," but the discovery rule provides a limited exception that "postpones accrual of a cause of action until the plaintiff discovers, or has reason to discover, the cause of action." *Fox v. Ethicon Endo-Surgery, Inc.*, 35 Cal. 4th 797, 806-807 (2005). This is not a "hypertechnical" inquiry, but rather asks whether "the plaintiffs have reason to at least suspect that a type of wrongdoing has injured them." *Id.* at 807. Plaintiffs' claims are time-barred in at least two ways.

First, Plaintiffs admit that the FTC's November 2011 Complaint—which was widely publicized in the national media—"outlines many of the same issues" as does the Complaint. Compl. ¶ 381; *see also supra* pp. 3-4, 31-32. The FTC's complaint and 2012 Consent Order—which Plaintiffs cite liberally in their Complaint (*see, e.g., id.* ¶¶ 381, 528, 554, 672)—put Plaintiffs on notice that third-party apps could access user data via permissions from their friends, and that App settings (not Privacy settings) directly controlled how users could limit the sharing of information with apps. *See* FTC Complaint ¶¶ 9, 18. Because all of Plaintiffs' claims have statutes of limitations well short of six years, they are time-barred.

Second, many of Plaintiffs' causes of action[16] are barred for the additional reason that events related to the thisisyourdigitallife app—the only third-party that any Plaintiff alleges acquired his or her data, *supra* p. 7—were widely reported more than two years before the first lawsuit was filed. On December 11, 2015, *The Guardian* published an article describing in detail the underlying facts concerning Cambridge Analytica's misuse of Facebook user data, and other publications followed suit shortly thereafter. *See* H. Davies, *Ted Cruz using firm that harvested data on millions of unwitting Facebook users*, The Guardian (Dec. 11, 2015), https://bit.ly/21HR0Ac; Prior MTD at 4-5, 28-29 (describing press account in detail). Similarly, Facebook did not hide that it had partnerships with so-called "whitelisted" companies; the media reported those partnerships as early as September 2014.[17] This, too, put Plaintiffs on notice of their claims.

[16] SCA, 18 U.S.C. § 2707(f) (two years); VPPA, 18 U.S.C. § 2710(c)(3) (two years); invasion of privacy, negligence, and gross negligence, Cal. Code. Civ. P. § 335.1 (two years); implied covenant of good faith and fair dealing, *Eisenberg*, 815 F.2d at 1292 (two years).

[17] See A. Fixmer, *Netflix (Finally) Understands You Don't Want to Share Everything on Facebook* (Sept. 2, 2014), https://bit.ly/2Fd2pDy.

D. Plaintiffs' Federal Statutory Counts Fail To State A Plausible Claim For Relief

Plaintiffs' federal-law claims fail on the merits for other reasons as well.

1. Stored Communications Act

Plaintiffs have not adequately alleged a violation of § 2702(a). Sections 2702(a)(1) and (a)(2) prohibit "electronic communication" and "remote computing" service providers from "knowingly divulg[ing] to any person or entity the contents of any communication" in electronic storage or carried or maintained on remote computing services. Plaintiffs assert that Facebook violated these provisions by disclosing their Facebook content directly "to unauthorized parties," such as Kogan, other apps, and device manufacturers, Compl. ¶ 847, and also by disclosing this content "indirectly to unauthorized parties including Cambridge Analytica and data brokers," for which Facebook allegedly is responsible because "[t]he subsequent disclosure of user information by Apps and Business Partners to additional unauthorized parties was reasonably foreseeable, and Facebook knew or should have known about this subsequent disclosure." *Id.* ¶ 851. These claims fail as a matter of law.

As an initial matter, as explained above, Plaintiffs consented to the data sharing at issue—both directly with apps and with apps via their friends—and consent is a complete defense to an alleged violation of Section 2702. *See* 18 U.S.C. § 2702(b)(3).

Even if users did not consent to sharing data with apps that their friends downloaded, the consent from those friends is sufficient. 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 1276; *In re Facebook, Inc.*, 923 F. Supp. 2d at 1206. By alleging that all of the relevant data—*e.g.,* messages, likes, status updates, pictures, videos—constituted electronic communications under the act, Plaintiffs acknowledge that the intended recipient also could consent to disclosure under the SCA. Compl. ¶ 832. For example, by adjusting their settings to allow the relevant information to be visible to "Friends" or "Friends of Friends," Plaintiffs designated their Facebook friends—including a friend who downloaded an app—as an "intended recipient" of the relevant information. And when a user downloaded an app, that user consented to provide the app with any friends' data in their possession: "App Developers sought all permissions, including the permissions that gave access to Friends' content and information, from the

App User when she downloaded or logged into the App." Compl. ¶ 414; *see also id.* ¶ 408 ("In order to gain access to nonpublic content and information, App Developers needed to request permission from the App User."); *id.* ¶ 400 (chart showing that app users "Get App & Allow permissions"). Plaintiffs further admitted in their prior complaint that apps accessed data *only* consistent with users' privacy settings. Prior Compl. ¶¶ 121-122.[18] This constitutes consent under the SCA.

Plaintiffs' "indirect disclosure" theory—that Facebook is liable not only for data transfers to Kogan and other apps, but also for any subsequent transfers by Kogan or other apps to third parties—also fails. The SCA predicates liability on "knowing" disclosures, 18 U.S.C. § 2702(a), but Plaintiffs' theory is premised on negligence—that subsequent disclosures were "reasonably foreseeable" and that Facebook "knew or should have known" they would take place. Compl. ¶ 851. Plaintiffs do not allege that Facebook was actually aware of any particular transfer by Kogan or anyone else. Indeed, Plaintiffs expressly allege that Facebook learned that Kogan had given user data to Cambridge Analytica only after the December 2015 *Guardian* article was published, long after Kogan had transferred the data to Cambridge Analytica. Compl. ¶ 454. In addition, the Ninth Circuit has made clear that the SCA does not allow secondary liability, *Freeman v. DirecTV, Inc.*, 457 F.3d 1001, 1005 (9th Cir. 2006), which is exactly what Plaintiffs' "indirect disclosure" theory seeks to establish.

In addition, because Plaintiffs have not alleged any injury that could plausibly result in damages, *supra* pp. 6-7, they cannot recover statutory damages under the SCA. Section 2707(c) permits damages equal to "the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000." 18 U.S.C. § 2707(c). The Supreme Court interpreted materially identical language in the Privacy Act, 5 U.S.C. § 552a(g)(4)(A), to preclude Privacy Act plaintiffs from recovering statutory minimum damages without first showing an actual injury. *Doe v. Chao*, 540 U.S. 614, 627 (2004). In other words, a bare statutory violation does not trigger statutory damages. The Fourth and Eleventh

[18] Plaintiffs cannot negate prior admissions by filing an 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)).

Circuits have applied *Doe* to the SCA and held that plaintiffs cannot recover statutory damages without first showing they suffered actual damages. *Vista Mtkg., LLC v. Burkett*, 812 F.3d 954, 971 (11th Cir. 2016); *Van Alstyne v. Elec. Sciptorium, Ltd.*, 560 F.3d 199, 206 (4th Cir. 2009).[19]

Finally, Plaintiffs' factual allegations fail in a number of ways. They do not allege that any app other than Kogan's—whitelisted or otherwise—obtained *their* information, nor do they allege that any device manufacturer obtained *their* information. And Plaintiffs still do not allege any facts to improve the plausibility that they were among the 1,500 users whose messages were obtained by Kogan's app—which, in any event, would have been shared only with their consent. Compl. ¶ 452.

2. Video Privacy Protection Act

Plaintiffs' claims that Facebook violated the VPPA—a 1988 statute passed in response to news reports that published Robert Bork's videotape rental history—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). "[T]he 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...." *Id.* § 2710(a)(4). This provision does not apply to every company "peripherally or passively involved in video content delivery"; a covered company's business must not only be "substantially involved in the conveyance of video content to consumers but also significantly tailored to serve that purpose." *In re Vizio, Inc., Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1221 (C.D. Cal. 2017). So the mere fact that a company can "deliver" video content does not mean that its business is "significantly tailored" to that end. The case law has unsurprisingly focused on companies that serve as the video-rental stores of the 21st century, including Hulu, Smart TVs, Disney, and Amazon in its capacity as seller of DVDs. *In re Hulu Privacy Litig.*, 2012 WL 3282960 (N.D. Cal. Aug. 10, 2012); *Vizio*, 238 F. Supp. 3d at 1222; *Amazon.com LLC v. Lay*, 758 F. Supp. 2d 1154 (W.D. Wash. 2010); *Robinson v. Disney Online*, 152 F. Supp. 3d 176 (S.D.N.Y. 2015).

In contrast, Facebook is not in the "business … of" selling, renting, or delivering videos to users

[19] Certain district courts in this circuit have held otherwise, but none sufficiently explains why *Doe* does not control. *See, e.g.*, *In re Hawaiian Airlines, Inc.*, 355 B.R. 225 (D. Haw. 2006).

as defined under the VPPA. Facebook operates a social media network that "allows users to connect with each other." Compl. ¶ 264. Plaintiffs do not allege that Facebook sold or rented videos to them. And Facebook did not "deliver" videos, as that word is understood in its proper context. *McDonnell v. United States*, 136 S. Ct. 2355, 2368 (2016) ("[A] word is known by the company it keeps."). "Rental" and "sale" connote a transaction geared toward sending video products to a consumer who requested them, and "deliver" should be understood in a similarly narrow way—not, as Plaintiffs allege, in a way that would encompass any defendant who facilitates access to a video, as nearly all modern websites do. Plaintiffs allege only that video was shared on Facebook just like any other Facebook data. Compl. ¶ 417. Although users can watch and engage with video content on Facebook, Facebook's "endeavor" as pled in the Complaint is not—like Blockbluster or its modem equivalents—to convey video content to consumers on demand, as part of a transaction. *Vizio*, 238 F. Supp. 3d at 1221. Even if video is a functional part of Facebook, its core business model does not fit the limited category of businesses who are "substantially involved" in renting, selling, or delivering videos to consumers and "significantly tailored to serve that purpose." *Id.*

Facebook did not release "personally identifiable information" under the VPPA. The VPPA states that "the 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 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. The Ninth Circuit has held that "personally identifiable information means only that information that would readily permit an ordinary person to identify a specific individual's video-watching behavior." *Eichenberger*, 876 F.3d at 985; *see In re Hulu*, 2014 WL 1724344, at *8 ("the statute protects personally identifiable information that identifies … particular videos *that the person watched*." (emphasis added)).

Unsurprisingly, the cases generally fit the classic fact pattern from Judge Bork's example—"a video clerk leaking an individual customer's video rental history. Every step away from that 1988 paradigm will make it harder for a plaintiff to make out a successful claim." *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 290 (3d Cir. 2016). There is no claim if the information would

force a third party to guess or infer whether the plaintiff had actually watched a particular video. *See Gonzalez v. Central Elec. Co-op, Inc.*, 2009 WL 3415235, at *11 (D. Or. Oct. 15, 2009) ("[T]he combined Doubletree evidence indicating that plaintiff purchased one of fifteen movies does not constitute personally identifiable information.").

Here, Plaintiffs have not alleged that Facebook maintains, or disclosed, any personally identifiable information, as understood by the VPPA. They have alleged only four categories of video-related data available to apps, and none reflects a record of videos that users watched on Facebook:[20]

- "users_videos" and "friends_video" show "the videos the user has uploaded and videos the user has been tagged in," not videos that users watched on Facebook. Compl. ¶ 420.
- "user_likes" and "friends_likes" do not even reveal data related to specific videos, but rather show "the list of all of the pages a user had liked"—meaning that the user or friend had liked "a public profile," not a particular video. Compl. ¶ 421. Whether any of these pages also showed videos is irrelevant because this "likes" category only relates to the pages themselves.
- "read_stream" shows "posts in the users' News Feed" which Plaintiffs allege include "any videos uploaded by the user as well as any videos or video hyperlinks shared with a user" and any posts regarding videos, such as a "critique of a specific movie." Compl. ¶ 423. But, again, none of this information communicates the videos that users actually viewed on Facebook.
- "read_mailbox" showed messages between users that Plaintiffs claim might include videos shared through messenger, but that still would not show videos actually watched. Compl. ¶ 424.

Unlike *Eichenberger*, where the plaintiff's viewing history was disclosed, none of the allegedly disclosed information here revealed videos that a user actually watched on Facebook. Thus, the information is not personally identifiable information, and Plaintiffs have no claim under the VPPA.

E. Plaintiffs' California State Law Claims Fail

Plaintiffs' California-law claims fail on the merits.

1. Facebook's liability disclaimer bars all claims based on third-party conduct

Several of Plaintiffs' claims focus on the alleged misconduct of third parties—advertisers who allegedly showed "offensive" advertisements and Kogan, the only identified third party alleged to have mishandled user data. But Plaintiffs cannot maintain actions on those theories because the SRR—

[20] Plaintiffs assert that additional categories of data related to videos, but do not explain what those categories actually provided. Compl. ¶ 419 ("users_subscriptions" and "friends_subscriptions"); *id.* ¶ 867 ("friends_actions_video, friends_likes, friends_photo_video_tags, and friends_status").

which Plaintiffs admit was binding, Compl. ¶ 937—expressly waived claims based on third-party conduct. *See supra* p. 23; Prior MTD at 32-34.[21]

Plaintiffs assert that "any purported waiver of liability" is contrary to public policy and unconscionable. Compl. ¶¶ 966-67. Both contentions lack merit. A contractual liability waiver may be invalid under California public policy when the business is "thought suitable for public regulation," "[t]he party seeking exculpation is engaged in performing a service" of "great importance" and "often a matter of practice necessity" to the public, and "[a]s a result of the essential nature of the service, in the economic setting of the transaction, the 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).

Facebook's services are not "essential" to the "public interest." 60 Cal. 2d at 101. The social media services Facebook provides are more like recreational services for which liability releases are upheld than essential public services like housing or child care. *Compare City of Santa Barbara v. Superior Court*, 41 Cal. 4th 747, 757-58 (2007) (citing cases upholding releases of liability in recreational context); *YMCA of Metro. L.A. v. Superior Court*, 55 Cal. App. 4th 22, 27 (1997) ("simple recreational offerings of games, socializing, shopping" "not so essential"), *with Henrioulle v. Marin Ventures, Inc.*, 20 Cal. 3d 512, 517-520 (1978) (residential landlord provides essential services); *Gavin W. v. YMCA of Metro. L.A.*, 106 Cal. App. 4th 662, 676 (2003) (provider of child care services).

Nor is Facebook "suitable for public regulation" or in "total control of its platform and services." Compl. ¶ 966. Facebook users have control over the content they choose to share and Facebook provides users with many tools to customize with whom they share it. *See, e.g., id.* ¶ 247 (named plaintiff alleging that he "customiz[ed] his privacy on a post-by-post, photo-by-photo, video-by-video basis"). As Plaintiffs' acknowledge, Facebook users can opt out of apps altogether or simply stop using Facebook's services, as at least one named plaintiff has done. *Id.* ¶ 371, ¶ 144 (named plaintiff alleges that she "deleted her Facebook account in approximately 2018"); *see, e.g.*, *YMCA*, 55 Cal. App. 4th at

[21] 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 are 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); *Goddard v. Google, Inc.*, 640 F. Supp. 2d 1193, 1201 (N.D. Cal. 2009).

28 (upholding release because plaintiff could "find[] another senior center or club").

Plaintiffs' vague assertion that Facebook's liability waiver is "unconscionable," Compl. ¶ 967, fails. "[U]nconscionability requires ... oppression or surprise due to unequal bargaining power [and] overly harsh or one-sided results." *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333, 340 (2011) (quotation marks omitted). The Complaint alleges no facts about oppression or surprise. Rather, most Plaintiffs do not recall the individual circumstances of contract formation, and only one alleges he had trouble understanding the "long and complex" terms, Compl. ¶ 52. These allegations are insufficient. *See Lancaster v. Alphabet Inc.*, 2016 WL 3648608, at *3 (N.D. Cal. July 8, 2016) (dismissing allegation that YouTube's Terms of Service are unconscionable). And Plaintiffs do not allege that Facebook's limitation of liability creates overly harsh or one-sided results so as to shock the conscience. *See Wayne v. Staples, Inc.*, 135 Cal. App. 4th 466, 480 (2006). Liability releases are routinely enforced in California, and are consistent with the expectation that a contracting party is not liable for third-party action.

2. Deceit by concealment or omission

Plaintiffs' concealment claim fails for three reasons: they (1) cannot point to any fact that Facebook was obligated, and failed, to disclose; (2) do not allege any personal injury; and (3) have not pled fraudulent concealment with particularity under Rule 9(b). *See Tenant Healthsystem Desert, Inc. v. Blue Cross of Cal.*, 245 Cal. App. 4th 821, 844 (2016) (quotation marks and brackets omitted).

Plaintiffs contend that Facebook failed to "disclose known risks that third party App Developers would sell or disperse user content and information." Compl. ¶ 880. This theory is barred by the parties' waiver of liability for third-party actions, *see supra* p. 23, but in any event, 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). Even assuming such a duty, Facebook satisfied it by telling 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 9.

Plaintiffs insist Facebook was required to "disclose … how Facebook allows other third parties ... to obtain their personal information notwithstanding their privacy settings." Compl. ¶ 890. But Facebook ***did*** disclose this information. *Supra* pp. 7, 20-23. And with the exception of the thisisyourdigitallife app, plaintiffs have not alleged that any third parties actually obtained their information. *Id.*

As for thisisyourdigitallife app, Plaintiffs admitted that apps could obtain data only "[a]s long as the request complie[d] with the users' and/or friends' privacy settings." Prior Compl. ¶¶ 121-22.

Plaintiffs' allegation that Facebook allowed apps to "circumvent users' privacy platform settings and access friends' information, even when the user disabled the Platform," also fails because plaintiffs do not allege they changed their app settings or turned off the app Platform to restrict sharing. *See* Compl. ¶¶ 27-263. They acknowledge the unchanged default settings permitted "*shar[ing]* all content with third-party applications, *see id.* ¶ 362, so no plaintiff was injured by this omission.

Plaintiffs' ancillary allegation that Facebook "stripped privacy settings from photos and videos," preventing apps from honoring users' privacy settings, also fails. Compl. ¶¶ 892. As explained *supra*, pp. 20-21, apps' use of photos or videos is controlled by the user's agreement with the app, and the explicit permissions he gives. D.D., Ex. 23. Moreover, apps are permitted to use that information only "in connection with [the] friend" from whom they collect it. As Facebook's Privacy Policy explains, "if a friend gives an application access to a photo you only shared with your friends, that application could allow your friend to view or print the photo, *but it cannot show that photo to anyone else*." D.D., Ex. 42 at 6 (emphasis added). So the app must comply with Facebook's platform policies and its own agreement with the user, and its disclosures cannot extend beyond a user's authorization.

Finally, Plaintiffs assert that Facebook failed to "disclose … how [its] content and information was being collected, shared and aggregated to develop digital profiles or dossiers of each user" for targeted advertising. Compl. ¶¶ 900-01. But Facebook fully disclosed that it uses the data it collects to serve paid ads, and Plaintiffs consented to those activities. *See supra* pp. 21-22. Plaintiffs also have not suffered any damages, and Plaintiffs' assertion that "Facebook received substantial advertising revenues," Compl. ¶ 907, is not enough. *Tenant Healthsystem*, 245 Cal. App. 4th at 844.

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. Plaintiffs 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). Plaintiffs' common law intrusion claim is governed by similar standards, and requires: "(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, 745 (2007).

Plaintiffs have not demonstrated a legally protected privacy interest. With few exceptions related to Facebook Messenger (which fail for separate reasons), Plaintiffs allege only categories of information that were shared, *see e.g.* Compl. ¶ 107, but that type of generalized allegation cannot establish what the California Constitution protects: "only the 'dissemination or misuse of *sensitive* and *confidential* information'" necessary to state a privacy claim. *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1039 (quoting *Hill*, 7 Cal. 4th at 35 (1994)). All but three named Plaintiffs fail to state exactly what *protected* information was disseminated. Courts have dismissed similar claims where plaintiffs failed to specify the protected information. *Id.* at 1041; *Zbitnoff v. Nationstar Mortg., LLC*, 2014 WL 1101161, at *4 (N.D. Cal. Mar. 18, 2014); *Scott-Codiga v. Cty. of Monterey*, 2011 WL 4434812, at *7 (N.D. Cal. Sept. 23, 2011).[22]

Plaintiffs have not alleged a reasonable expectation of privacy because they consented to disclosure. *See supra* pp. 19-31; *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1072 (N.D. Cal. 2016) ("[A] plaintiff cannot have a reasonable expectation of privacy if she consented to the intrusion.").

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," *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (2011), and "[e]ven disclosure of very personal information," *In re Yahoo*, 7 F. Supp. 3d at 1038, are not egregious breaches of social norms. Sharing *is* the social norm undergirding Facebook, and Facebook did not breach that norm by sharing user data consistent with users' preferences. Moreover, disseminating or failing to secure consumers' sensitive personal information is not enough. *See Razuki v. Caliber Home Loans, Inc.*, 2018 WL 2761818, at *2 (S.D. Cal. June 8, 2018) ("insufficient security" is not "an egregious

[22] The three named Plaintiffs that offer slightly more detail fare no better. *See* Compl. ¶ 51 (inspirational Facebook live video broadcast publicly); ¶ 54 (Facebook Events for upcoming church gatherings); ¶ 93 (public service announcement video); ¶ 197 (photos and videos relating to long-distance horseback rides).

breach of social norms"); *see also* Prior MTD at 37-38 (collecting cases).

4. Invasion of privacy—public disclosure of private facts

Plaintiffs have not alleged any actionable public disclosure of private facts. *See Moreno v. Hanford Sentinel, Inc.*, 172 Cal. App. 4th 1125, 1129-30 (2009) (listing elements).

No "public" disclosure. "Publicity" here means "communication to the public in general or to a large number of persons," not to a single person. *Del Llano v. Vivint Solar Inc.*, 2018 WL 656094, at *5 (S.D. Cal. Feb. 1, 2018) (quotation marks omitted). Plaintiffs have failed to allege that their data was disclosed to any third party other than the thisisyourdigitallife app.

No "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 now specify that they set their privacy setting to "Friends of Friends" or "Only Friends," but they still fail to sufficiently allege what data shared, much less what "private" facts were shared. And the only three named Plaintiffs that specify particular content or information that they shared fail to demonstrate how any alleged disclosure of that information rises 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) (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 "using and publishing Plaintiffs' name and likenesses for its advantage by allowing third parties ... to access, obtain, and use Plaintiffs' likenesses—including names, Likes, personal photographs, and personal videos—without first obtaining their consent." Compl. ¶ 1010. But this tort protects the "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) (quotation omitted). Allowing advertisers to target ads to a Facebook user in no way appropriates that user's "name, voice, signature, photograph, or likeness." "Demographic 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), and collecting such information has never been deemed to violate the right to publicity—or even implicate publicity at all.

6. Negligence

Plaintiffs' negligence claims fail for multiple reasons. First, Plaintiffs fail to plausibly allege facts establishing a legal duty to use due care and a breach that caused injury. The SRR's limitation of liability bars Plaintiffs' assertion that Facebook had a "duty [to] … ensur[e]" that third parties were not "improperly" treating Plaintiffs' "content and information." Compl. ¶ 953; *supra* p. 23. Nor would there be a duty even absent this contractual waiver. "[O]ne owes no duty to control the conduct of another, nor to warn those endangered by such conduct." *Davidson*, 32 Cal. 3d at 203. Courts have not imposed on companies an affirmative duty to prevent third-party app developers from committing torts. *Pirozzi v. Apple Inc.*, 913 F. Supp. 2d 840, 852 (N.D. Cal. 2012); *In re iPhone Application Litig.*, 2011 WL 4403963, at *9 (N.D. Cal. Sept. 20, 2011); *In re Google*, 2013 WL 1283236, at *13 (N.D. Cal. Mar. 26, 2013). Nor can Plaintiffs base a tort duty on allegations of negligent performance under a contract. *Applied Equip. Corp. v. Litton Saudi Arabia Ltd.*, 7 Cal. 4th 503, 514–15 (1994).

Second, Plaintiffs' claims are barred by the economic loss rule. *Kalitta Air, L.L.C. v. Cent. Tex. Airborne Sys., Inc.*, 315 F. App'x 603, 605 (9th Cir. 2008); *see In re iPhone Application Litigation*, 844 F. Supp. 2d 1040, 1064 (N.D. Cal. 2012) (dismissing negligence claim alleged only that the plaintiffs 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"); *see* Prior MTD at 40.

No exceptions apply. *Kalitta Air*, 315 F. App'x at 605. Plaintiffs have not alleged personal injury or physical damage to property. And they cannot allege a "special relationship" with Facebook under the six-factor test of: (1) whether the transaction was intended to affect the plaintiff, (2) the foreseeability of harm, (3) the degree of certainty of harm, (4) the connection between the conduct and the harm, (5) the moral blame attached to the conduct, and (6) the policy of preventing future harm. *J'Aire Corp. v. Gregory*, 24 Cal. 3d 799, 804 (1979). The first factor applies *only* when "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). Plaintiffs have not alleged Facebook's conduct toward them was any "different from any other purchaser of the same product." *Greystone Homes, Inc. v. Midtec, Inc.*, 168 Cal. App. 4th 1194, 1230-31 (2008). Further, Plaintiffs allege no cognizable harm, thus mooting any analysis of foreseeability or certainty. *Cf. J'Aire*, 24 Cal. 3d at 805 (third factor met

when complaint leaves "no doubt" of harm). As to factor four, the connection between Facebook's actions and Plaintiffs' alleged injuries is tenuous at best, as evidenced by Plaintiffs' focus on third parties. And there is little risk of future harm (factor six) because Facebook changed the Graph API to allow apps to access data only from the people who authorize the app.

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). Courts addressing data-access allegations consistently have found a failure to sufficiently allege harm. *See Razuki*, 2018 WL 2761818, at *2; *In re iPhone II*, 844 F. Supp. 2d at 1064; *Low*, 900 F. Supp. 2d at 1032.

7. Breach of contract

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 shared friends' data with third-party applications. Compl. ¶¶ 938-40 (emphasis added). This theory fails because Facebook disclosed each of these practices, and Facebook does not share user data with these third parties when they are acting as advertisers, *see supra* pp 21-22. Plaintiffs' allegation that Facebook breached the Contracts by failing to honor user privacy settings also fails because Plaintiffs admitted that all app obtain data only "[a]s long as the request complie[d] with the users' and/or friends' privacy settings." Prior Compl. ¶¶ 121-22.

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), but Plaintiffs cannot show any actual damage, *supra* pp. 6-7.

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

Breach of the implied covenant is a species of breach of contract, *Carson v. Mercury Ins. Co.*, 210 Cal. App. 4th 409, 429 (2012), so this claim fails because Plaintiffs have not alleged contract damages. *See supra* pp. 6-7. It also fails because the alleged wrongful actions were expressly covered by the Data Use Policy, which was part of Facebook's contract with users. Compl. ¶¶ 1030-32; *Third Story Music, Inc. v. Waits*, 41 Cal. App. 4th 798, 804 (1995) ("There can be no implied covenant where the subject is completely covered by the contract."). Plaintiffs' allegations that Facebook allowed

"whitelisted" Apps to access user's content and information and that "Facebook stripped privacy settings," Compl. ¶¶ 1027-29, also fail for the reasons discussed above, *supra* pp. 6-7, 19-32, 40.

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. ¶ 937. "[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).

10. Unfair Competition

Under the UCL, a plaintiff's "injury in fact" must involve "lost money or property." *Troyk v. Farmers Grp., Inc.*, 171 Cal. App. 4th 1305, 1348 n.31 (2009); Cal. Bus. & Prof. Code § 17204. Plaintiffs lack standing because Facebook's service are free, personal information is not "property or money," and any out-of-pocket expenses cannot be recovered because Plaintiffs have not pled a credible risk of identity theft. Prior MTD at 43-44; *see In re Sony*, 903 F. Supp. 2d at 966 (free services); *In re iPhone Application Litig.*, 2011 WL 4403963, at *14 (personal information is not property).

Plaintiffs also cannot plausibly allege that Facebook's conduct was unfair, unlawful, or fraudulent. Claims for "unfair" conduct are available only for competition claims. *See Durell v. Sharp Healthcare*, 183 Cal. App. 4th 1350, 1366 (2010). Facebook's conduct was not "unlawful" because Plaintiffs have not pled statutory or constitutional violations. Compl. ¶ 977. And Facebook did not behave fraudulently because 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. 19-32, 43. Finally, Plaintiffs have no right to restitution because Facebook has not taken "money or property" from them by means of "unfair competition." *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1149 (2003). And damages are not permitted under the UCL. *Id.* at 1144.

V. CONCLUSION

Facebook respectfully requests that this Court dismiss Plaintiffs' Amended Consolidated Complaint without leave to amend.

DATE: March 15, 2019

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.