UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

IN RE: FACEBOOK, INC., CONSUMER PRIVACY USER PROFILE LITIGATION	MDL No. 2843 Case No. 18-md-02843-VC
This document relates to: ALL ACTIONS	**PRETRIAL ORDER NO. 20: GRANTING IN PART AND DENYING IN PART MOTION TO DISMISS FIRST AMENDED COMPLAINT**

This lawsuit, which stems from the Cambridge Analytica scandal, is about Facebook's practice of sharing its users' personal information with third parties. The plaintiffs are current and former Facebook users who believe that their information was compromised by the company. Their principal allegations are that Facebook: (i) made sensitive user information available to countless companies and individuals without the consent of the users; and (ii) failed to prevent those same companies and individuals from selling or otherwise misusing the information. The plaintiffs do not merely allege that Facebook shared what we often describe as "data" – basic facts such as gender, age, address, and the like. They allege that Facebook shared far more substantive and revealing content that users intended only for a limited audience, such as their photographs, videos they made, videos they watched, their religious and political views, their relationship information, and the actual words contained in their messages.

Facebook has filed a motion to dismiss the lawsuit. Although the company makes many different arguments, there are three main ones. First, Facebook argues that people have no legitimate privacy interest in any information they make available to their friends on social media. This means, according to Facebook, that if people use social media to communicate

sensitive information with a limited number of friends, they have no right to complain of a privacy violation if the social media company turns around and shares that information with a virtually unlimited audience. As explained in Section II of this ruling, Facebook's argument could not be more wrong. When you share sensitive information with a limited audience (especially when you've made clear that you intend your audience to be limited), you retain privacy rights and can sue someone for violating them.

Second, Facebook argues that even if its users had a privacy interest in the information they made available only to friends, there is no standing to sue in federal court because there were no tangible negative consequences from the dissemination of this information. That too is wrong. As explained in Section III, the law has long recognized that a privacy invasion is itself the kind of injury that can be redressed in federal court, even if the invasion does not lead to some secondary economic injury like identity theft.

Facebook's third main argument is that even if users retained a privacy interest in the information that was disclosed, and even if a "bare" privacy invasion confers standing to sue in federal court, this lawsuit must be dismissed because Facebook users consented, in fine print, to the wide dissemination of their sensitive information. As discussed in Section IV, this question is more difficult than the first two. California law requires the Court to assume as a legal matter (even if it's not true as a factual matter) that users reviewed, understood, and agreed to all of Facebook's contractual terms when they signed up for their accounts. These terms included a description of at least some of Facebook's information-sharing practices, for at least a portion of the time period covered by this lawsuit. In particular, from roughly 2009 to 2015, Facebook disclosed its practice of allowing app developers to obtain, through a user's Facebook friends, any information about the user that the friends had access to.

That single disclosure, however, is relatively inconsequential for this motion to dismiss. The complaint adequately alleges that users who established their Facebook accounts prior to roughly 2009 never consented to this practice. Plaintiffs in this category may pursue claims based on information-sharing with app developers. Moreover, the complaint adequately alleges

that no users ever consented to Facebook's other information-sharing practices – specifically, sharing with certain "whitelisted apps" starting in 2015, and sharing with certain "business partners" during much of the relevant time period. Finally, the complaint adequately alleges that users never consented to Facebook's widespread practice of allowing companies to sell and otherwise misuse sensitive user information, as opposed to restricting the use of this information as Facebook promised it would. Therefore, even though Facebook's arguments regarding user consent have some legal force and will somewhat limit the scope of the lawsuit, they cannot defeat the lawsuit entirely, at least at the pleading stage.

Accordingly, as set forth in Section V (which discusses the specific legal claims asserted by the plaintiffs), although Facebook's motion to dismiss will be granted for a few of the claims, most claims survive.

I. BACKGROUND

Cambridge Analytica, a British political consulting firm, used personal information from millions of Facebook accounts to send targeted political messages during the 2016 presidential campaign. The firm obtained this information from Aleksandr Kogan, a researcher who had acquired it through his app, which Facebook had allowed him to deploy on its platform. The Cambridge Analytica incident began receiving significant press coverage in 2018, which in turn generated increased scrutiny of Facebook's information-sharing practices. In the months that followed, reports emerged suggesting that the ability of people like Kogan and entities like Cambridge Analytica to obtain sensitive Facebook user information was the norm rather than the exception. Broadly speaking, this case is about whether Facebook acted unlawfully in making user information widely available to third parties. It's also about whether Facebook acted unlawfully in failing to do anything meaningful to prevent third parties from misusing the information they obtained.

Following the Cambridge Analytica outcry, dozens of lawsuits were filed against Facebook in various courts around the country. The lawsuits were mostly in federal court, and they were mostly proposed class actions by individual Facebook users who contended that

Facebook disseminated their sensitive personal information to Kogan without their consent and failed to prevent him from transferring it to Cambridge Analytica. One of the first of these lawsuits was filed in the Northern District of California and randomly assigned to this Court.

When multiple, similar federal lawsuits are filed around the country, there is a process within the federal judiciary for handling them. Congress has created the Judicial Panel on Multidistrict Litigation, which considers whether to transfer similar cases to a single federal judge for pretrial proceedings. The purpose is to promote the orderly adjudication of multiple similar cases, avoiding conflicting rulings from different judges and alleviating the strain on the system that would result from many judges adjudicating the same complicated pretrial issues. The multidistrict litigation process contemplates that once the assigned judge adjudicates those issues, the individual cases are sent back for trial to the courts where they originated. In these cases against Facebook, the panel concluded that assignment to a single judge was warranted, and assigned the lawsuits to this Court.

This Court subsequently appointed two attorneys to serve as lead plaintiffs' counsel. Thereafter, lead counsel, representing roughly three dozen individual Facebook users, filed a consolidated class action complaint. The plaintiffs propose to represent a class consisting of all Facebook users in the United States and the United Kingdom whose personal information was improperly disseminated and/or inadequately protected by Facebook from 2007 to the present. The practical effect of the proposed class action is that this one consolidated complaint could potentially resolve all claims by private parties against Facebook arising from the company's practices of disseminating user information during this period. In other words, this proceeding has effectively become one large proposed class action, as opposed to a group of several dozen separate lawsuits.[1]

Facebook filed a motion to dismiss, and a lengthy hearing took place during which the

[1] Other lawsuits which are not part of this multidistrict litigation have been filed against Facebook by law enforcement entities from states or localities. Although Facebook attempted to fold one such lawsuit into this proceeding, the Court rejected that attempt. *See Illinois, ex rel. Kimberly M. Foxx v. Facebook*, 354 F. Supp. 3d 1122 (N.D. Cal. 2019).

parties and the Court discussed many potential deficiencies in the complaint. The hearing ended with the Court giving the plaintiffs permission to file an amended complaint to address any such deficiencies.

The amended complaint, which is the subject of the current motion to dismiss, runs 414 pages and includes 1,442 paragraphs. It appears to include all the claims that were asserted in the cases that were transferred here by the multidistrict litigation panel, and more. But for manageability purposes, the complaint is divided into "prioritized claims" and "nonprioritized claims." The idea is that the prioritized claims (which presumably reflect lead counsel's judgment about their relative strength or importance) will be adjudicated first, and the nonprioritized claims should be stayed and addressed later if necessary. The complaint names multiple defendants (for example, CEO Mark Zuckerberg, in addition to Facebook itself), but again divides those defendants into the "prioritized" and "non-prioritized" categories. Facebook is the only prioritized defendant.

It's worth noting that the case has expanded in scope. While the initial lawsuits focused largely on Facebook's conduct that was the subject of the Cambridge Analytica scandal, the case now includes allegations stemming from the subsequent revelations about Facebook's wider information-sharing practices. Moreover, although the complaint purports to assert 12 prioritized "claims," most of those purported claims actually consist of multiple distinct legal claims, based on distinct factual allegations. For example, the section entitled "Breach of Contract" appears to contain roughly half a dozen distinct claims for breach of contract, based on distinct acts of alleged wrongdoing. Indeed, at times it seems the plaintiffs sought to identify anything Facebook has ever been reported to have done wrong and then made sure to sprinkle in at least a few allegations about it.

This strategy interferes significantly with the clarity and effectiveness of the plaintiffs' presentation. Some of the allegations are quite vague. For example, the plaintiffs make an allegation, the significance of which the Court has not been able to understand, about Facebook stripping metadata from users' photos before allowing third parties to access them. Also

scattered throughout the complaint are allegations about something the plaintiffs call "psychographic marketing," without any meaningful explanation of the legal or factual difference between psychographic marketing and targeted advertising (the latter of which the plaintiffs appear to concede is perfectly legitimate).

Overall, the presence of so many disparate and vague allegations makes it nearly impossible for Facebook to meaningfully respond to all of them, much less for the Court to effectively address them. The conventional approach in a situation like this might be to sift through the complaint to try to identify each distinct claim, then dismiss with leave to amend all claims that are not adequately articulated. But that approach would likely result in many more rounds of motions to dismiss, bogging the case down at the pleading stage for years. In the interest of preventing that from happening to this multidistrict litigation, this ruling focuses on what the Court understands to be the plaintiffs' core allegations about Facebook's handling of sensitive user information. Claims based on these core factual allegations will largely survive the motion to dismiss. All other prioritized claims not addressed by this ruling will be stayed (effectively, relegated to non-prioritized status) and adjudicated, if necessary, at a later stage in the proceedings with the other non-prioritized claims.

The core allegations in the complaint describe four categories of wrongdoing by Facebook. In adjudicating Facebook's motion to dismiss, the Court is required to assume the truth of these allegations, so long as they are adequately articulated and not contradicted by any documents that the complaint explicitly relies on.

1. Giving app developers access to sensitive user information. Since roughly 2007, Facebook users have been able to access applications, or apps, directly from the Facebook platform to do things like play video games, read news content, or stream videos. According to the plaintiffs, this interaction among Facebook, its users, and third-party apps is one of the primary means by which Facebook has disseminated user information to third parties. The complaint alleges that when users accessed apps on the Facebook platform, the app developers were not merely able to obtain information about the users they were interacting with; they were

also able to obtain any information about the users' Facebook friends that the users themselves had access to. So, for example, if you decided to use an app on the Facebook platform to play a video game, the video game company would be able to access not only your information but also any information about your friends that you could obtain yourself. This includes a variety of things that your friends might have intended to share only with a limited audience, such as photographs, videos they made, videos they watched, religious preferences, posts, and even sometimes private one-on-one messages sent through Facebook. And since most people have dozens or hundreds of Facebook friends, each interaction with an app represents the disclosure of a great deal of information about dozens or hundreds of people.

The Cambridge Analytica story is an example of this. In 2013, Aleksandr Kogan created an app called "MyDigitalLife." Facebook allowed Kogan to market and operate this app on the Facebook platform. The app invited Facebook users to answer a series of questions to help them better understand themselves – a personality test of sorts. But when a user took the test, Kogan was not merely able to collect information about that user; he was able to collect information on the user's Facebook friends. This allowed Kogan to compile a database with information on roughly 87 million Facebook users, even though his app was only downloaded by around 300,000 people.

The plaintiffs allege that from roughly 2009 to 2015, tens of thousands of app developers like Kogan, operating on the Facebook platform, were able to interact with users to obtain this type of information about users' friends. The plaintiffs further allege that Facebook failed to adequately disclose that even if users adjusted their privacy settings to specify that only their friends would be allowed to see their information, this would not prevent app developers from getting it.

2. Continued disclosure to whitelisted apps. In 2014, in response to criticism of its information-sharing practices, Facebook announced it would restrict app developers so they would have access only to the information of the users the apps were interacting with (and not to information of the users' friends). But the plaintiffs allege that Facebook, despite its public

promises to restrict access, continued to allow a preferred list of app developers to access the information of users' friends. The complaint describes these preferred app developers as "whitelisted apps," and alleges that Facebook secretly continued to give these apps "special access" to friends' information because of the amount of revenue these apps generated for Facebook. Thousands of companies were allegedly on this list, including Airbnb, Netflix, UPS, Hot or Not, Salesforce, Lyft, Telescope, and Spotify.

3. Sharing sensitive user information with business partners. Meanwhile, Facebook has maintained a separate information-sharing program with companies that the plaintiffs describe as "business partners." The complaint's allegations about these business partners are somewhat more difficult to pin down than the allegations about app developers. Indeed, there may be some overlap between companies in the "app" category and the "business partner" category. Moreover, the plaintiffs allege that Facebook outsourced to business partners "the time, labor, and money required to build Facebook's Platform on different devices and operating systems," but that doesn't seem to describe all the "business partners" listed in the complaint. The non-exclusive list of companies that the complaint identifies as business partners includes device manufacturers, such as Blackberry and Samsung. It includes websites such as Yahoo, and the Russian search engine Yandex. And it includes companies such as Amazon, Microsoft, and Sony. This list came from Facebook itself, which asserted that it had "integration partnerships" with these companies in a letter to the Energy and Commerce Committee of the U.S. House of Representatives.

Although the category is somewhat vague, the alleged misconduct is relatively straightforward. The complaint alleges that Facebook shared information about its users with this non-exclusive list of business partners, and that those companies in turn shared data with Facebook. "These partnerships," the complaint alleges, "were built in part on 'data reciprocity.' Facebook and its partners agreed to exchange information about users' activities with each other." And as with app developers, Facebook allegedly would give a business partner access not only to information of the user with whom the business partner interacted, but also to

information of that user's friends. The plaintiffs allege that, for most of the period covered by the lawsuit, Facebook never disclosed that it was sharing user information with business partners in this fashion.

4. Failure to restrict the use of sensitive information. In addition to complaining about Facebook's dissemination of private user information to app developers, whitelisted apps, and business partners, the plaintiffs allege that Facebook did nothing to prevent these third parties from misusing the information Facebook allowed them to access. Specifically, the plaintiffs allege that: (i) Facebook purported to have a policy preventing app developers from using information for any purpose other than enhancing the interaction between the app and the person who was using the app on the Facebook platform; but (ii) Facebook did nothing to enforce this policy, thus giving users the impression that their information was protected, while in reality countless app developers were using it for other purposes.

Again, the Cambridge Analytica story is an example of this. According to the plaintiffs, if Facebook was truly enforcing a policy of limiting the use of user information by app developers, Kogan would have been precluded from extracting all that sensitive information about users' friends to employ for his own research, and he would certainly have been precluded from selling it to Cambridge Analytica. The plaintiffs allege that this was the norm with the tens of thousands of app developers who interacted with users on the Facebook platform – that any policy Facebook purported to have restricting the use of information by third parties was nonexistent in reality, because Facebook was intent solely on generating revenue from the access it was providing.

Based on the four core categories of misconduct described above, the plaintiffs assert a variety of legal claims. They bring a privacy-based tort claim under California law for the unauthorized disclosure of private facts. They assert another privacy-based tort claim for intrusion into private affairs, along with a similar claim based on the right to privacy enshrined in the California Constitution. They bring two claims based on federal statutes: the Stored Communications Act (which prohibits the unauthorized disclosure of information from

computers) and the Video Privacy Protection Act (which prohibits disclosure of a person's video viewing habits). And the plaintiffs bring a variety of other California law claims that don't relate as directly to privacy but are nonetheless based on assertions that Facebook failed to protect their privacy. Such claims include breach of contract (for allowing third parties to obtain sensitive user information despite promising to protect it), deceit (for tricking users about the degree to which their information could be accessed), and negligence (for failing to prevent third parties from misusing sensitive information despite Facebook's duty to protect that information). As mentioned earlier, many of these purported claims actually have multiple distinct claims built into them. Facebook has moved to dismiss all the claims, both for lack of standing and on the merits.

II. EXPECTATION OF PRIVACY

Facebook's motion to dismiss is littered with assumptions about the degree to which social media users can reasonably expect their personal information and communications to remain private. Because Facebook's view of this issue pervades so many of its individual legal arguments – and because Facebook's view is so wrong – it is addressed at the outset.

Facebook's view is that once you make information available to your friends on social media, you completely relinquish any privacy interest in that information. For this reason, Facebook insists, it does not matter whether Facebook users consented to the company's information-sharing practices. Facebook asserts that even if users didn't consent, and even if users intended to restrict access to friends only, and even if Facebook had explicitly promised not to share their information with anyone else, the users would have no right to complain that their privacy was invaded by the disclosure or misuse of their sensitive information. Although this argument was implicit in Facebook's papers, it became explicit at the hearing on the motion to dismiss. Dkt. No. 287 at 7 (hearing transcript).[2]

[2] Facebook appears to contend that this issue relates both to standing and to the merits of any claims in which the plaintiffs assert an expectation of privacy (such as the privacy claims brought under California tort law or the California Constitution). As discussed in Section IV with respect to consent, the issue of whether users have a reasonable expectation of privacy in

The problem with Facebook's argument is that it treats privacy as an all-or-nothing proposition – either you retain a full privacy interest by not sharing information with anyone, or you have no privacy interest whatsoever by virtue of sharing it even in a limited fashion. In reality, there can be "degrees and nuances to societal recognition of our expectations of privacy: the fact that the privacy one expects in a given setting is not complete or absolute does not render the expectation unreasonable as a matter of law." *Sanders v. American Broadcasting Companies, Inc.*, 20 Cal. 4th 907, 915 (1999); *see also Opperman v. Path, Inc.*, 84 F. Supp. 3d 962, 991-93 (N.D. Cal. 2015). Thus, as the U.S. Supreme Court has explained, "information may be classified as private if it is intended for or restricted to the use of a particular person *or group or class of persons*" rather than being "freely available to the public." *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749, 763-64 (1989) (emphasis added) (quoting Webster's Third New International Dictionary 1804 (1976)); *see also id.* at 763 ("Thus the extent of the protection accorded a privacy right at common law rested in part on the *degree* of dissemination of the allegedly private fact . . . ."). So, for example, if you are diagnosed with a medical condition, you can expect to conceal it completely only if you keep it between you and your doctor. But it does not follow that if you send an email to selected colleagues and friends explaining why you'll be out of commission for a while, you've relinquished any privacy interest in your medical condition, such that the email provider could disseminate your diagnosis to anyone who might be interested in your health status. Similarly, social media users can have their privacy invaded if sensitive information meant only for a few dozen friends is shared more widely.[3]

Although Facebook refuses in this case to acknowledge its users' privacy interests, it has done so in other court cases. For example, in a brief filed with the California Supreme Court, for

---

information they share with their social media friends is best understood as relating to the merits, not standing. *See, e.g.*, *American Farm Bureau Federation v. U.S. Environmental Protection Agency*, 836 F.3d 963, 968 (8th Cir. 2016).

[3] It seems quite possible that a user whose settings allow information to be shared not only with friends, but friends of friends, loses any expectation of privacy, although that issue is not squarely presented by this motion to dismiss.

a case where Facebook fought against the compelled disclosure of a user's posts, Facebook compared information kept on social media to information kept on a smartphone: "The data on a smartphone – like the data maintained in a social media account – can reveal an individual's private interests and concerns and where a person has been, which in turn reflects a wealth of detail about a person's familial, political, professional, religious, and sexual associations." Answer Brief on the Merits, *Facebook, Inc. v. Superior Court*, 2016 WL 684072 (Cal.), at *29 (brackets and internal quotations omitted) (quoting *Riley v. California*, 573 U.S. 373, 396 (2014)). For this reason, Facebook continued, "communications content of the kind maintained by [social media] providers" carries with it such a significant expectation of privacy that even law enforcement must get a warrant before accessing it from those providers. *Id*. In a different California Supreme Court brief, Facebook took pains to juxtapose users who share communications with the general public against users who share communications only with friends: "These settings cannot be overridden by others; if a post is set to be viewable only by a certain audience, it may not then be shared or forwarded through the Facebook platform to someone outside that audience." Answering Brief on the Merits, *Facebook, Inc. v. Superior Court*, 2018 WL 2060039 (Cal.), at *16. Facebook added that even if users designate their communications to be viewed by the general public, they can later "regain" their expectation of privacy in that information by switching their settings back to a more restricted audience. *See id.* at *28 n.4.

Perhaps Facebook's argument that social media accounts are like smartphones is an exaggeration in the other direction. But it's closer to the truth than the company's assertions in this case. Sharing information with your social media friends does not categorically eliminate your privacy interest in that information, and the plaintiffs' claims in this lawsuit must be analyzed against that backdrop, rather than the backdrop Facebook attempts to paint in its motion to dismiss.

III. STANDING

To bring their claims in federal court, the plaintiffs must adequately allege (and eventually prove) that they have "standing" under Article III of the United States Constitution. This means, among other things, that the plaintiffs must allege they suffered an actual injury from Facebook's conduct that is both "concrete" and "particularized." *See Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1545 (2016).

The plaintiffs allege three kinds of injury. First, they allege a simple "privacy injury" – that is, injury from Facebook's widespread disclosure of their sensitive information, including their photographs, videos they made, videos they watched, religious preferences, posts, and even private one-on-one messages sent through Facebook. Second, the plaintiffs allege they were injured because Facebook's dissemination of their personal information increased the risk that they would become victims of identity theft. Third, the plaintiffs allege they were deprived the economic value of their personal information as a result of its dissemination, the theory apparently being that if their information had remained private, they could have sold that information to advertisers or data brokers themselves.

The second and third alleged injuries do not confer Article III standing. Regarding the risk of identity theft, this is not a case involving, say, hackers, and it is not a case about the theft of, say, social security or credit card numbers. Although the risk of identity theft is admittedly greater than if Facebook had not made the plaintiffs' personal information available, the risk is too speculative to confer standing. *Compare In re Zappos.com, Inc.*, 888 F.3d 1020, 1024-29 (9th Cir. 2018). Regarding loss of value, although it's true that each user's information is worth a certain amount of money to Facebook and the companies Facebook gave it to, it does not follow that the same information, when not disclosed, has independent economic value to an individual user. The plaintiffs do not plausibly allege that they intended to sell their non-disclosed personal information to someone else. Nor, in any event, do they plausibly allege that someone else would have bought it as a stand-alone product. The plaintiffs' economic-loss theory is therefore purely hypothetical and does not give rise to standing. *See In re Facebook Internet Tracking Litigation*,

140 F. Supp. 3d 922, 931-32 (N.D. Cal. 2015); *Opperman v. Path, Inc*., 87 F. Supp. 3d 1018, 1057 (N.D. Cal. 2014); *Yunker v. Pandora Media, Inc.*, 2013 WL 1282980, at *4 (N.D. Cal. Mar. 26, 2013); *Low v. LinkedIn Corp*., 2011 WL 5509848, at *4-5 (N.D. Cal. Nov. 11, 2011).[4]

But the first alleged injury – that the plaintiffs' sensitive information was disseminated to third parties in violation of their privacy – is sufficient to confer standing. Facebook argues that a "bare" privacy violation, without "credible risk of real-world harm" such as identity theft or other economic consequences, cannot rise to the level of an Article III injury. But it's black-letter law that an injury need not be "tangible" to be cognizable in federal court. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016) ("Although tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete."). And courts have often held that this particular type of intangible injury – disclosure of sensitive private information, even without further consequence – gives rise to Article III standing.

Indeed, the Ninth Circuit has repeatedly explained that intangible privacy injuries can be redressed in the federal courts. This issue has tended to come up recently in cases where a plaintiff alleges standing based on the violation of a statute whose purpose is to protect privacy. In such cases, the alleged violation of the statute does not automatically give rise to standing. For a statutory violation to create standing, the statute must protect against a concrete and particularized injury that's cognizable within the meaning of Article III.

Most recently on this issue, the Ninth Circuit handed down an opinion in a different case against Facebook – a case involving Facebook's use of facial recognition technology in alleged violation of an Illinois statute. The Court held that "the development of a face template using facial recognition technology without consent (as alleged here) invades an individual's private affairs and concrete interests." *Patel v. Facebook, Inc.*, 2019 WL 3727424, at *5 (9th Cir. Aug.

[4] *But see In re Facebook Privacy Litigation*, 572 F. App'x 494, 494 (9th Cir. 2014); *Williams v. Facebook, Inc.*, No. 18-cv-01881-RS, Dkt. No. 128 at 11-13 (N.D. Cal. Aug. 29, 2019); *Svenson v. Google Inc*., 2015 WL 1503429, at *5 (N.D. Cal. Apr. 1, 2015).

8, 2019). Earlier, in *Eichenberger v. ESPN*, the Ninth Circuit held that an alleged violation of the Video Privacy Protection Act creates standing, explaining that the statute "protects privacy interests . . . generally by ensuring that consumers retain control over their personal information," and emphasizing that "privacy torts do not always require additional consequences to be actionable." 876 F.3d 979, 983 (9th Cir. 2017). And in *Van Patten v. Vertical Fitness Group, LLC*, the Ninth Circuit concluded that alleged violations of the Telephone Consumer Protection Act, which creates a cause of action to remedy the injury of receiving annoying telemarketing text messages, give rise to standing because such messages, "by their nature, invade the privacy and disturb the solitude of their recipients." 847 F.3d 1037, 1043 (9th Cir. 2017). The *Van Patten* court emphasized that a lawsuit alleging this type of intrusion under the statute may proceed in federal court even if no additional, tangible harm is alleged. *Id.*

There are many similar cases involving common law claims. For example, Judge Seeborg recently held that a lawsuit asserting common law privacy claims against Facebook based on the collection and disclosure of users' Android data could proceed in federal court despite the absence of any alleged economic injury. *Williams v. Facebook, Inc.*, 384 F. Supp. 3d 1043, 1050 (N.D. Cal. 2018) ("The complaint need not include economic injury to establish standing for the intrusion upon seclusion, invasion of privacy, or unjust enrichment claims."). In reaching this conclusion, Judge Seeborg quoted another decision involving Facebook – this one by Judge Davila – which held: "a plaintiff need not show actual loss to establish standing for common-law claims of invasion of privacy and intrusion upon seclusion." *In re Facebook Internet Tracking Litigation*, 263 F. Supp. 3d 836, 843 (N.D. Cal. 2017); *see also In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 806 F.3d 125, 134-35 (3d Cir. 2015) (holding that the plaintiffs had standing to assert federal statutory and California common law privacy claims based on allegations that the defendants implanted tracking cookies on their personal computers); *id.* at 134 ("For purposes of injury in fact, the defendants' emphasis on economic loss is misplaced."); *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1057 (N.D. Cal. 2014).

To be sure, Facebook cites a few cases that lean in the other direction. For example, in a

2012 case, Judge Grewal rejected the argument that the "loss of personal information, even in the absence of any cognizable economic harm, was sufficient to confer Article III standing." *In re Google, Inc. Privacy Policy Litigation*, 2012 WL 6738343, at *5 (N.D. Cal. Dec. 28, 2012). But Judge Grewal's ruling seems to *assume* that economic harm is required rather than examining whether it's required. This appears equally true of the earlier district court cases on which he relied. *See LaCourt v. Specific Media, Inc.*, 2011 WL 1661532, at *4 (C.D. Cal. Apr. 28, 2011); *In re iPhone Application Litigation*, 2011 WL 4403963, at *5 (N.D. Cal. Sept. 20, 2011). Ultimately, the only reason Judge Grewal gave for his ruling was that "nothing in the precedent of the Ninth Circuit or other appellate courts confers standing on a party that has brought statutory or common law claims based on nothing more than the unauthorized disclosure of personal information . . . ." *In re Google, Inc. Privacy Policy Litigation*, 2012 WL 6738343, at *5. Whether or not he was right about precedent at the time, the cases cited above provide ample support for the conclusion that this type of privacy invasion alone creates standing.

And those cases are right. To say that a "mere" privacy invasion is not capable of inflicting an "actual injury" serious enough to warrant the attention of the federal courts is to disregard the importance of privacy in our society, not to mention the historic role of the federal judiciary in protecting it. "In a democratic society privacy of communication is essential if citizens are to think and act creatively and constructively." *Bartnicki v. Vopper*, 532 U.S. 514, 533 (2001) (quoting President's Commission on Law Enforcement and Administration of Justice, The Challenge of Crime in a Free Society 202 (1967)). For this reason, our country has countless federal laws on the books designed to protect our privacy – laws that the federal courts are charged with enforcing.[5] Perhaps the most prominent of these is the Wiretap Act, colloquially

[5] *See, e.g.*, Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936; Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (2012); Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-2775 (2012); Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848; Privacy Protection Act of 1980, Pub. L. No. 96-440, 94 Stat. 1879; Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422 (2012); Privacy Act of 1974, 5 U.S.C. § 552a (2012).

known as "Title III," a bedrock privacy protection which makes it unlawful for either the government or a private party to intercept someone's "wire, oral, or electronic communication" without consent. 18 U.S.C. § 2511. Would Facebook really argue that a violation of this statute inflicts no "actual injury" on the participants in the conversation unless interception of the communication ends up visiting a more tangible, secondary harm on the participants?

Of course, a plaintiff cannot get into court by simply intoning that she suffered an intangible privacy injury. But once it is understood that an intangible privacy injury *can* be enough, it becomes easy to conclude that the alleged privacy injury here *is* enough. The alleged injury is "concrete" largely for the reasons already discussed – if you use a company's social media platform to share sensitive information with only your friends, then you suffer a concrete injury when the company disseminates that information widely. And the alleged injury is "particularized," at least for most of the plaintiffs. To be particularized, the injury must have been suffered directly by the individual plaintiff, and it must be distinct from the more general type of objection that members of the public at large might have to a defendant's unlawful conduct. *See Spokeo*, 136 S. Ct. at 1548. The plaintiffs allege that Facebook violated their privacy rights (and other rights) because: (i) they engaged in sensitive communications that included photographs, videos they made, videos they watched, Facebook posts, likes, and private one-on-one messages; (ii) they intended to share these communications only with a particular person or a group of people; (iii) Facebook made those communications widely available to third parties in a variety of ways; and (iv) as a result, third parties were able to develop detailed dossiers on the plaintiffs including information about their locations, their religious and political preferences, their video-watching habits, and other sensitive matters.[6]

Facebook makes one argument regarding particularity that, if successful, would merely

[6] It's possible that a few of the named plaintiffs have not adequately alleged a privacy injury based on their own Facebook experience. However, Facebook does not single out any particular named plaintiff in its motion, and most of the plaintiffs have adequately alleged standing. Facebook will be given an opportunity to attempt to knock out individual named plaintiffs on standing grounds at a later stage.

narrow the scope of this case rather than ending it entirely. Recall that this lawsuit arose from the Cambridge Analytica scandal, with the plaintiffs originally alleging that Facebook gave Aleksandr Kogan access to their information (with Kogan, in turn, giving it to Cambridge Analytica). The plaintiffs initially alleged, plausibly and with specificity, that Kogan likely accessed their own information. But the plaintiffs now allege that Facebook disseminated sensitive user information far more widely, to tens of thousands of app developers and business partners. Facebook argues that because the complaint lacks specific allegations about which app developers or business partners obtained which plaintiffs' private information, the plaintiffs have not alleged an injury particular to them, at least beyond the injury from the disclosure to Kogan.

This argument puts too great a burden on the plaintiffs, at least at the pleading stage (and probably at any stage). If, as alleged in the complaint, Facebook made users' "friends only" information readily available to such a broad swath of companies (Apple, Samsung, AT&T, Sprint, T-Mobile, Verizon, Google, Huawei, Microsoft, Mozilla, LG, and Amazon, to name just a few), it is virtually inevitable that some of these companies obtained information on the named plaintiffs. *Cf. Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1021 (N.D. Cal. 2012). This type of privacy invasion is no less an Article III injury simply because the plaintiffs are left to guess precisely which companies (other than Facebook) were involved.

Accordingly, for all the claims addressed by this ruling, Facebook cannot obtain dismissal for lack of Article III standing.

IV. CONSENT

There is one more global issue to discuss before proceeding to a claim-by-claim analysis of the complaint. Facebook contends that the plaintiffs agreed, when they signed up for their accounts, that Facebook could disseminate their "friends only" information in the way it has done. If the complaint and any judicially noticeable materials were to establish that Facebook users consented to the alleged misconduct, this would indeed require dismissal of virtually the entire case. However, the complaint adequately alleges that some users did not consent to any of Facebook's practices. And although Facebook is correct as a matter of law that some users

consented to the first category of conduct (sharing information with app developers), the complaint adequately alleges that those users did not consent to the other three categories (sharing information with whitelisted apps starting in 2015, sharing information with business partners, and failing to protect user information from misuse).

A.

As an initial matter, Facebook asserts that consent is actually a standing issue. It contends that there is no true Article III injury on the facts of this case because the plaintiffs cannot be injured by something they allowed Facebook to do.

But the whole point of Article III standing is that some claims don't belong in federal court even if the plaintiff would win on the merits. Therefore, the standing inquiry in this case is: assuming the plaintiffs could win on the merits, should their claims nonetheless be dismissed for lack of standing because the injury they allegedly suffered is not cognizable in federal court? The plaintiffs allege they did not consent – and this is an allegation they would need to prevail on if they are to succeed on the merits. Thus, the Court must assume, for purposes of the standing inquiry, that the plaintiffs did not consent. "A party need not prove that the action it attacks is unlawful in order to have standing to level that attack . . . . Rather, in determining whether plaintiffs have standing, we must assume that on the merits they would be successful in their claims." *Muir v. Navy Federal Credit Union*, 529 F.3d 1100, 1106 (D.C. Cir. 2008) (alterations omitted).

This rule holds even when the standing question overlaps substantially with the question of whether a plaintiff has stated a claim. "As a general rule, when the question of jurisdiction and the merits of the action are intertwined, dismissal for lack of subject matter jurisdiction is improper." *Williston Basin Interstate Pipeline Co. v. An Exclusive Gas Storage Leasehold & Easement in the Cloverly Subterranean Geological Formation*, 524 F.3d 1090, 1094 (9th Cir. 2008) (internal quotations and alterations omitted); *see also Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1040 (9th Cir. 2004) ("The district court erred in characterizing its dismissal of Safe Air's complaint under Rule 12(b)(1) because the jurisdictional issue and substantive issues in

this case are so intertwined that the question of jurisdiction is dependent on the resolution of factual issues going to the merits.").

In privacy cases, the standing and merits inquiries will often be intertwined. For example, the extent to which you have a reasonable expectation of privacy relates not only to whether you've stated a claim for invasion of privacy but whether you were injured by the invasion in the first place. And this will often be true of consent – if you agree to the disclosure of your personal information, it may be difficult to argue that you've been "injured" in a legal sense by the disclosure you permitted. But in virtually every privacy case, consent will be part of the merits inquiry. Because courts presume success on the merits when evaluating standing, these are not standing issues in privacy cases.[7]

A good illustration of this is *Van Patten v. Vertical Fitness Group, LLC*, 847 F.3d 1037 (9th Cir. 2017). In that case, which was in a summary judgment posture, the Ninth Circuit held that the plaintiffs established standing to sue based on the receipt of allegedly unwanted text solicitations. But in the same opinion, the Court held that the plaintiffs must lose on the merits, because they consented to receive those texts. *Id.* at 1044. Although courts occasionally conflate standing with the merits in privacy cases, they generally recognize the need to keep them separate. *See, e.g.*, *American Farm Bureau Federation v. U.S. Environmental Protection Agency*, 836 F.3d 963, 968 (8th Cir. 2016) ("The EPA reasons that because the disputed information was publicly available on the Internet or available for public review, further distribution of the information could not establish any injury. That conclusion, however, assesses the merits of the asserted privacy interest under FOIA rather than whether the associations' members had a legally cognizable interest in preventing the agency's release of their personal information."); *In re Vizio, Inc., Consumer Privacy Litigation*, 238 F. Supp. 3d 1204, 1216 (C.D. Cal. 2017)

[7] It's possible that a federal court confronted with truly frivolous privacy claims might reasonably consider intertwined issues as a matter of standing – for example, if the absence of a reasonable privacy expectation, or the presence of consent, were obviously and totally indisputable. *Cf. Williston Basin Interstate Pipeline*, 524 F.3d at 1094. But even in a rare case like that, it still probably makes more sense for the court to dismiss the claims on the merits (which, after all, is just as easy to do, and also gives the defendant the benefit of preclusion).

(rejecting, in a privacy case, a standing argument that "improperly conflates the merits of Plaintiffs' claims with their standing to bring suit"); *id.* ("Taken to its logical conclusion, Defendants' argument absurdly implies that a court could never enter judgment against a plaintiff on a VPPA claim if it found that the disclosed information was not within the statutory definition of personally identifiable information; instead, it would have to remand or dismiss for lack of jurisdiction."); *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1020 (N.D. Cal. 2012) (explaining that whether a plaintiff adequately alleges standing to assert privacy claims "in no way depends on the merits" of those claims (quoting *Warth v. Seldin*, 422 U.S. 490, 500 (1975))).

B.

Whether the plaintiffs consented to Facebook's information-sharing practices is thus a merits inquiry. And the parties actually agree on several aspects of that inquiry. First, they agree that, for virtually all claims, the question of whether Facebook users consented to the alleged conduct is one of contract interpretation governed by California law.[8] Second, the parties agree that California law requires the Court to pretend that users actually read Facebook's contractual language before clicking their acceptance, even though we all know virtually none of them did. Constrained by this fiction, the Court must analyze the relevant contractual language to assess whether the users "agreed" to allow Facebook to disseminate their sensitive information in the ways described in the lawsuit. Third, the parties agree that if the contract language at issue is reasonably susceptible to more than one interpretation, with one of those interpretations suggesting consent and another belying it, the Court cannot decide the consent issue in Facebook's favor at the motion to dismiss stage. And fourth, they agree that the contract language must be assessed objectively, from the perspective of a reasonable Facebook user. The

[8] For the claim under the federal Video Privacy Protection Act, consent is governed by the terms of the statute itself. This issue is discussed in the portion of Section V dealing with that claim. The federal Stored Communications Act precludes information-sharing by computer service providers without "lawful" consent; this is presumably a reference to state law, and the parties don't suggest otherwise, so this ruling assumes that California law applies to the consent issue relating to that claim.

upshot, at this early stage of the case, is that if a reasonable Facebook user could plausibly have interpreted the contract language as *not* disclosing that Facebook would engage in particular conduct, then Facebook cannot obtain dismissal of a claim about that conduct (at least not based on the issue of consent).[9]

One difficulty with the consent question is that the lawsuit covers a nearly 13-year period – from 2007 to the present. Obviously, Facebook said different things to its users over that period, and its practices changed as well. And it would be impossible at this stage to analyze which disclosures apply to which plaintiffs, because the parties have not presented the information necessary to conduct that inquiry. The analysis in this ruling will primarily focus on the documents presented to users who signed up for accounts in the middle of 2012. At least with respect to the four categories of alleged misconduct addressed in this ruling, these mid-2012 documents provide a good exemplar of what Facebook users agreed to during much of the period covered by this lawsuit; indeed, users agreed to substantially similar language between roughly 2009 and 2015. Thus, these documents allow the Court to assess consent as a general matter, even if the analysis might not apply to every single plaintiff.[10]

---

[9] The parties disagree about whether consent should be treated as an element of the plaintiffs' claims or as an affirmative defense to those claims. The answer is likely that consent is an element for some claims and an affirmative defense for others. But at least for purposes of this motion it does not matter, because in either case the question is whether the allegations in the complaint and any judicially noticeable materials definitively establish that the plaintiffs consented to the conduct. If the answer is yes, the Court must dismiss the claims regardless of whether consent is an element or a defense. *See, e.g.*, *Rivera v. Peri & Sons Farms, Inc*., 735 F.3d 892, 902 (9th Cir. 2013) ("When an affirmative defense is obvious on the face of a complaint . . . a defendant can raise that defense in a motion to dismiss."); *see also Jablon v. Dean Witter & Co.*, 614 F.2d 677, 682 (9th Cir. 1980).

[10] Incidentally, the fact that the plaintiffs seek to represent a class of people who used Facebook any time between 2007 and the present raises the possibility that some aspects of this lawsuit are time-barred, and Facebook presses this issue in its motion to dismiss. For example, Facebook notes that it was the subject of a consent order by the Federal Trade Commission in 2012, based on similar information-sharing practices. That consent order may have put the plaintiffs on notice of Facebook's conduct prior to the entry of the order (although presumably it would not have put them on notice of any misconduct by Facebook following entry of the consent order). Facebook also invokes a single news article from 2015 (which this Court may consider on a motion to dismiss because the article is incorporated by reference into the complaint). That article discusses the company's information-sharing practices, and Facebook asserts that this should have put

People who signed up for accounts in mid-2012 were required to accept Facebook's "Statement of Rights and Responsibilities," or "SRR." The SRR itself contains some statements about privacy and information-sharing. But it also references, and contains links to, several other policies, including the "Data Use Policy."[11] Although both sides agree that the language in the SRR is contractual, they dispute whether the Data Use Policy is part of that contract. This dispute matters because the Data Use Policy more explicitly discusses sharing information with third parties, and it contains the language Facebook primarily relies on to contend that its users consented to much of the alleged misconduct. The SRR is attached as Appendix A to this ruling, and the Data Use Policy is attached as Appendix B.[12]

The first section of the SRR, entitled "Privacy," calls out the Data Use Policy in the second sentence, provides a link to it, and encourages the user to read it. This first section of the SRR states in full: "Your privacy is very important to us. We designed our Data Use Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Data Use Policy, and to use it to help you make informed decisions." Appendix A at 2. Later on the same page, the SRR tells users to read the Data Use Policy to learn about "how you can control what information other people may share with applications." *Id.* And at the end, the SRR provides a

---

everyone on notice of its conduct. This seems more dubious than the argument about the FTC's 2012 consent order. But in any event, statutes of limitations provide an affirmative defense, which normally must be raised at summary judgment rather than on a motion to dismiss. *U.S. ex rel. Air Control Technologies, Inc. v. Pre Con Industries, Inc.*, 720 F.3d 1174, 1178 (9th Cir. 2013). The only exception is when it is absolutely clear from the allegations in the complaint and judicially noticeable material that a claim is untimely and no tolling doctrine could apply. That cannot be said here – at best Facebook has raised a significant possibility that claims relating to pre-2012 conduct may be time-barred, a defense that will need to be decided on summary judgment or at trial.

[11] Earlier versions of the "Statements of Rights and Responsibilities" were called "Terms of Service." Earlier versions of the "Data Use Policy" were called the "Privacy Policy."

[12] The request to consider these documents, which are exhibits 23 and 44 to Facebook's request for judicial notice at Docket Number 187, is granted because they are incorporated by reference into the complaint. The request to consider exhibits 14, 19, 26, 39, 40, 43, 46, and 47 is granted for the same reason. *Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 1002 (9th Cir. 2018). All other requests, beyond those granted in this footnote and in Footnote 10, are denied, although in any event they would not affect the outcome of this motion. *See id.*

list of additional documents the user "may also want to review," including the Data Use Policy, which "contains information to help you understand how we collect and use information." *Id.* at 11. This final section again includes a link to the Data Use Policy (along with several other documents that are described as governing the relationship between Facebook and its users).

This is sufficient to incorporate the Data Use Policy into the contractual agreement between Facebook and its users. Indeed, California case law makes it quite easy to incorporate a document by reference. "The contract need not recite that it incorporates another document, so long as it guides the reader to the incorporated document." *Shaw v. Regents of University of California*, 58 Cal. App. 4th 44, 54 (1997) (quotations omitted). What's needed is simply that the reference to the document be unequivocal, that the document be called to the attention of the contracting parties, and that the terms of the document be easily available to the contracting parties. *Id.*; *see also Wolschlager v. Fidelity National Title Insurance Co.*, 111 Cal. App. 4th 784, 790-91 (2003); *In re Anthem, Inc. Data Breach Litigation*, 2016 WL 3029783, at *8 (N.D. Cal. May 27, 2016); *Koffler Electrical Mechanical Apparatus Repair, Inc. v. Wartsila North America, Inc.*, 2011 WL 1086035, at *4-5 (N.D. Cal. Mar. 24, 2011). One could argue that the California appellate courts have been too quick to find incorporation by reference and that more explicit language should be required, particularly in the context of consumer contracts of adhesion. But this Court must apply California case law, which militates in favor of the conclusion that the Data Use Policy is incorporated into the SRR.

Thus, the true legal question is whether, by "agreeing" to the SRR and Data Use Policy, Facebook users consented to the alleged misconduct. In analyzing this question, it's important to reiterate the precise conduct at issue. Recall that the plaintiffs allege four categories of misconduct: (i) Facebook allowed app developers to access sensitive information, not merely of users they interacted with, but of the users' friends; (ii) even after Facebook announced it would no longer give app developers access to information of users' friends, it secretly continued to give "whitelisted apps" access; (iii) through some separate arrangement and by some separate means, Facebook shared sensitive user information with its business partners; and (iv) although

Facebook ostensibly had a policy of sharply limiting the use of the sensitive information it gave to third parties, in fact Facebook imposed no limits whatsoever.

It's easy to conclude, at the pleading stage, that the second category of conduct was not disclosed. In fact, Facebook does not even argue that its users assented to this practice. The same goes for the third category: although Facebook points to a section in its Data Use Policy entitled "Service Providers" which says "we give your information to the people and companies that help us provide, understand, and improve the services we offer," that statement does not come close to disclosing the massive information-sharing program with business partners that the plaintiffs allege in the complaint. Thus, for the claims based on sharing with whitelisted apps and business partners, Facebook cannot prevail on consent, at least at this stage.

In contrast, the first category of conduct – allowing the Aleksandr Kogans of the world to interact with users and obtain information of the users' friends through those interactions – was disclosed in the terms agreed to by Facebook users, at least for a portion of the period covered by this lawsuit. To begin, the SRR told users: "You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings." Appendix A at 2. As mentioned previously, the SRR also flagged for users the possibility that other people "may share" their information "with applications," and instructed users to read the Data Use Policy to learn more about this. *Id.* In turn, the Data Use Policy said 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." Appendix B at 10. And it instructed: "If you want to completely block applications from getting your information when your friends and others use them, you will need to turn off all Platform applications. This means you will no longer be able to use any third-party Facebook-integrated games, applications, or websites." *Id.*

Thus, contrary to the plaintiffs' argument, the language of these disclosures cannot be interpreted as misleading users into believing that they merely needed to adjust their privacy settings to "friends only" to protect their sensitive information from being disseminated to app developers. Users were told that they needed to adjust their application settings too. To be sure,

for the rare person who actually read the contractual language, it would have been difficult to isolate and understand the pertinent language among all of Facebook's complicated disclosures. Thus, in reality, virtually no one "consented" in a layperson's sense to Facebook's dissemination of this information to app developers. But under California law, users must be deemed to have agreed to the language quoted in the preceding paragraph, which means that users who did not properly adjust their application settings are deemed to have agreed that app developers could access their information.[13]

But there is a caveat. One inference from the complaint and the judicially noticeable materials is that Facebook began to disclose this practice of giving app developers access to friends' information only around 2009. Thus, users who established Facebook accounts before this time did not, at least based on the allegations in the complaint, agree to these terms when they signed up. Facebook contends this does not matter, because those users agreed to be bound by the SRR and Data Use Policy going forward, even when the terms changed. There appears to be some disagreement in the courts about whether a unilateral modification provision of this sort is permissible under California contract law, at least in circumstances where the party against whom it is being asserted did not receive adequate notice of the modification. *Compare Campos v. JPMorgan Chase Bank, NA*, 2019 WL 827634, at *10 (N.D. Cal. Feb. 21, 2019), *with Rodman*

[13] Incidentally, there is a pending case in which the Federal Trade Commission proposes a $5 billion civil penalty against Facebook, along with a 20-year consent decree. Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief, *USA v. Facebook, Inc.*, No. 19-cv-2184 (D.D.C. July 24, 2019). The lawsuit filed on behalf of the FTC accuses Facebook of, among other things, failing to adequately disclose the practice of allowing app developers to access user information through users' friends. At first glance, this ruling's conclusions regarding consent might appear inconsistent with some of the allegations in the FTC lawsuit. That lawsuit curiously neglects to mention the language that Facebook used in its Data Use Policy, and therefore does not paint a complete picture of the communications between Facebook and its users, at least with respect to users who signed up after 2009. But even considering the disclosures in the Data Use Policy, the FTC's position is not necessarily inconsistent with this ruling. The FTC's claims against Facebook are not based on California law; they are based on alleged violations of the Federal Trade Commission Act and the earlier FTC consent order from 2012. While California law, for better or worse, allows Facebook to bury a disclosure of its information-sharing practices in the fine print of its contractual language, the FTC consent order required Facebook to disclose such practices prominently, in a way that would likely come to the attention of Facebook users. More broadly, the consent order precluded Facebook from explicitly or implicitly misrepresenting the extent to which the company protects user privacy.

v. Safeway Inc., 2015 WL 604985, at *9-10 (N.D. Cal. Feb. 12, 2015), *aff'd*, 694 F. App'x 612 (9th Cir. 2017). But assuming for argument's sake the general validity of Facebook's unilateral modification provision, it does not automatically follow that users consented to the particular terms that Facebook subsequently added about sharing information with app developers. Even the cases upholding unilateral modification provisions recognize that any authority to modify the contract is constrained by the covenant of good faith and fair dealing. *See, e.g.*, *Campos*, 2019 WL 827634, at *9. This means that a Facebook user, when consenting to the unilateral modification provision, was consenting only to future modifications made in good faith. According to the plaintiffs, Facebook made a massive change in its contract without directly notifying its users, effectively adding a disclosure that "we will make your information readily available to tens of thousands of app developers unless you take complicated measures to prevent it." If that's true, it could very well constitute a breach of the covenant of good faith and fair dealing, which would mean that the users didn't consent to it.

And users who did not agree to the practice in their contracts could have been kept further in the dark about it by specific features of the Facebook platform. According to the complaint, in 2009 Facebook added a feature for users to select their audience for specific posts, choosing among "public," "friends," or a "custom" audience. Users were not informed, as part of this selection process, that designation of a limited audience would not prevent app developers from being part of that audience.

Thus, at this stage, the Court cannot conclude as a matter of law that early Facebook users consented to the later-announced information-sharing policy. This means that any plaintiff who signed up before roughly 2009 may pursue claims based on this conduct (assuming they can adequately allege the other elements of their claims).[14]

The fourth category of alleged misconduct – failing to limit how third parties could use

[14] As previously mentioned, neither side has attempted to specify which plaintiffs may pursue which claims, and it is unclear precisely when the disclosures changed on this issue; the parties will have an opportunity to parse this out at a subsequent phase in the case.

the sensitive information they accessed – is also somewhat complicated. The Data Use Policy, after explaining to users that applications could obtain their information from their friends, stated as follows: "If an application asks permission from someone else to access your information, the application will be allowed to use that information only in connection with the person that gave the permission and no one else." Appendix B at 10. The Policy gives an example of this: "one of your friends might want to use a music application that allows them to see what their friends are listening to. To get the full benefit of that application, your friend would want to give the application her friend list – which includes your User ID – so the application knows which of her friends is also using it." *Id.* From this example, it seems clear that the phrase "the application will be allowed to use that information only in connection with the person that gave the permission" means that if an app developer accesses your information through interaction with one of your Facebook friends, it may use your information only as part of its interaction with that friend. It therefore may not sell your information, or use it to develop a digital dossier on you for future targeted advertising.

Less clear is what Facebook is promising to do to protect users. Facebook interprets the disclosure to mean, in essence, "we tell app developers that they can only use your information to facilitate their interactions with your friends, but you can't really be sure they'll honor that." Perhaps a reasonable Facebook user could interpret the disclosure that way, which would mean that the user, upon agreeing to the Data Use Policy, assumed the risk that app developers would misuse the information. In other words, on this interpretation, users consented to an arrangement whereby app developers could end up obtaining their sensitive information for any purpose. But recall that in the context of this motion to dismiss the plaintiffs may be deemed to have consented to this arrangement only if that is the only plausible interpretation. It is not – there are at least two others. One equally plausible interpretation of the disclosure is that it assures users that Facebook is actively policing the activities of app developers on its platform, and thereby successfully preventing sensitive information from being misappropriated. Another plausible interpretation is that the word "allowed" references a technological block of sorts – that is,

perhaps a user could conclude that the Facebook platform has the ability to physically prevent app developers from being able to "see" friend information outside the context of their interactions with users. A user who has tried to access a fantasy football website at work, only to see a message on his screen that he's not "allowed" to access the site from that computer, might interpret the disclosure this way. Indeed, the Data Use Policy elsewhere uses the word "allowed" in a similar fashion, to connote a technological block. For example, it states: "If someone clicks on a link to another person's timeline, they'll only see the things that they are allowed to see." Appendix B at 8. Thus, there are at least three plausible interpretations of the contract language, two of which would lead to a conclusion that users did not consent but were misled, because Facebook allegedly did nothing to enforce its purported policy against tens of thousands of app developers who were freely making off with sensitive user information.[15]

The bottom line on the issue of consent is this: the complaint plausibly alleges that some users (and some plaintiffs) did not consent to the arrangement whereby app developers could access their sensitive information simply by interacting with their friends. For the remaining three categories of misconduct – sharing with whitelisted apps, sharing with business partners, and failing to prevent misuse of information by third parties – the complaint plausibly alleges that none of the users consented. The issue of consent therefore does not require dismissal in full of any of the prioritized claims in this lawsuit.[16]

---

[15] Incidentally, with respect to the allegation that Facebook failed to restrict the use of information by business partners (as opposed to app developers, to the extent those two categories don't overlap), it's unclear whether this contract language applies at all. If it does not apply, that would further weaken Facebook's argument that users were on notice that the company imposed no meaningful restriction on the use of information by business partners (although it could also undermine the plaintiffs' argument that Facebook committed a breach of contract by failing to prevent business partners from misusing information). Whether this language applies to restrictions on business partners, however, is not capable of firm resolution at this stage.

[16] Facebook makes an additional argument that even if the plaintiffs didn't explicitly consent to the alleged conduct in contractual language, they did so implicitly because they were put on notice of the conduct by Facebook's non-contractual disclosures. That issue cannot be resolved at the pleading stage in this case. *See, e.g.*, *In re Google Inc. Gmail Litigation*, 2014 WL 1102660, at *16 (N.D. Cal. Mar. 18, 2014) ("Implied consent is an intensely factual question that requires consideration of the circumstances . . . .").

V. INDIVIDUAL CLAIMS

The various global issues having been addressed (and the complaint having been narrowed, for now, to claims based on the plaintiffs' core allegations), it becomes less difficult to sift through the individual claims asserted by the plaintiffs. Most of the claims will survive. The specific outcome for each claim is as follows:

- Facebook's motion to dismiss is granted in part and denied in part for the three privacy-based torts asserted under California law (public disclosure of private facts, intrusion into private affairs, and violation of the constitutional right to privacy).
- The motion is granted in part and denied in part for the claim based on the federal Stored Communications Act.
- The motion is denied in full for the federal Video Privacy Protection Act claim.
- The motion is denied in full for the California claim based on negligence and gross negligence.
- For the California claims based on deceit by concealment, breach of contract, breach of the implied covenant of good faith and fair dealing, and unjust enrichment, the motion is granted in part and denied in part.
- The motion is granted in full for violation of the right of publicity and the Unfair Competition Law.

Public disclosure of private facts. For this tort to give rise to liability, the following must occur: (i) the defendant must disclose a private fact about the plaintiff; (ii) the private fact must not be a matter of public concern; (iii) the disclosure must be to the public; and (iv) the disclosure must be offensive and objectionable to a reasonable person. *See Doe v. Gangland Productions., Inc*., 730 F.3d 946, 958 (9th Cir. 2013). The plaintiffs have adequately alleged that Facebook engaged in this conduct.

Facebook argues that the information about users that it disclosed to app developers was not "private" because users had allowed their Facebook friends to access that information. But as discussed in Section II, your sensitive information does not lose the label "private" simply because your friends know about it. Your privacy interest in that information may diminish

because you've shared it with your friends, but it does not necessarily disappear. For example, the plaintiffs allege that app developers accessed information about their religious preferences and political views. Your friends may know about your religious and political views, but the widespread dissemination of them can still invade your privacy. The plaintiffs also allege that some of the information app developers received would allow them to discern a user's location (for example, a post saying "Check out where I'm staying in June!"). If you've told your friends where you'll be at a particular time, that does not preclude a lawsuit based on the widespread, nonconsensual distribution of that information.

Facebook also argues that the user information was not disseminated to "the public." This is based on the erroneous assumption, already rejected in Section III, that the plaintiffs have failed to allege with sufficient particularity that their information was disclosed to anyone other than Aleksandr Kogan. And dissemination of your private information to tens of thousands of individuals and companies is generally going to be equivalent to making that information "public." Perhaps Facebook could have made a better argument, which is that there's a difference between publicizing your sensitive information for actual human beings to scrutinize (like, in a newspaper) and allowing your information to be added to the vast sea of "big data" that computers rather than humans analyze for the purpose of sending targeted advertising on behalf of companies. Perhaps there is an argument that the former is the "public disclosure" of information within the meaning of California law while the latter is not. But that is not an issue that can be resolved at this stage of the litigation: Facebook does not pursue this argument, and in any event the plaintiffs do not allege that their information was merely subject to relatively anonymous computer analysis.

Finally, Facebook contends that its disclosure of sensitive user information to app developers and business partners would not be offensive to a reasonable person. Facebook makes a similar argument for the next two claims discussed below (intrusion into private affairs and the constitutional right to privacy), because those claims also require the plaintiff to allege (and eventually prove) that the privacy violation was a serious breach of social norms. "Sharing is the

social norm undergirding Facebook," the company argues, "and Facebook did not breach that social norm by sharing user data consistent with users' preferences." Motion to Dismiss at 41, Dkt. No. 261-1. There are a number of problems with this assertion. First, it again erroneously assumes a "norm" that there is no privacy interest in the information kept on social media. The social norm Facebook created with its product is purposefully sharing with one's friends, not having one's information shared by Facebook with unknown companies and individuals. Second, it assumes that users consented to the widespread disclosure of their sensitive information, but the plaintiffs have adequately alleged that they didn't. Thus, at this stage of the case, the plaintiffs have adequately alleged that Facebook's conduct was offensive and an egregious breach of social norms: it disclosed to tens of thousands of app developers and business partners sensitive information about them without their consent, including their photos, religious preferences, video-watching habits, relationships, and information that could reveal location. It even allegedly disclosed the contents of communications between two people on Facebook's ostensibly private messenger system.[17]

The motion to dismiss this claim is granted with respect to the first category of conduct for plaintiffs who consented to this conduct, as discussed in Section IV. It is denied in all other respects.[18]

Intrusion on private affairs and violation of the constitutional right to privacy. The analysis for these two tort claims is functionally identical, even though each claim is described somewhat differently in the case law. "When both claims are present, courts conduct a combined inquiry that considers (1) the nature of any intrusion upon reasonable expectations of privacy, and (2) the offensiveness or seriousness of the intrusion, including any justification or other relevant interests." *In re Facebook Internet Tracking Litigation*, 263 F. Supp. 3d 836, 846 (N.D.

[17] The "big data" concept referenced in the preceding paragraph may also have relevance to whether the privacy invasion is "offensive or serious," but not at this stage.
[18] Unless stated otherwise, dismissal is without leave to amend because the Court cannot conceive of a way the plaintiffs could successfully amend the claim based on the particular factual theory involved.

Cal. 2017) (internal quotations omitted). Under California law, courts must be reluctant to reach a conclusion at the pleading stage about how offensive or serious the privacy intrusion is. *Williams v. Facebook, Inc.*, 384 F. Supp. 3d 1043, 1054 (N.D. Cal. 2018) (Whether conduct rises to the level of highly offensive "is indeed a factual question best left for a jury." (internal quotations omitted)); *Opperman v. Path, Inc*., 205 F. Supp. 3d 1064, 1080 (N.D. Cal. 2016) ("A judge should be cautious before substituting his or her judgment for that of the community."). For the reasons already discussed, the plaintiffs have adequately alleged that they suffered an egregious invasion of their privacy when Facebook gave app developers and business partners their sensitive information on a widespread basis.

The motion to dismiss this claim is granted with respect to the first category of conduct for plaintiffs who consented to this conduct, as discussed in Section IV. It is denied in all other respects.

Stored Communications Act. The Stored Communications Act ("SCA") is a federal law that restricts when a computer service provider like Facebook may share the contents of a communication with someone who is not party to that communication. *See* 18 U.S.C. § 2702. The plaintiffs have plausibly alleged that Facebook violated the SCA.

Facebook notes that there is an exception to SCA liability when one of the parties to the communication consents to its disclosure by the computer service provider. 18 U.S.C. § 2702(b)(3). In the social media context, this means that whenever people make information available to one another, there is no SCA violation if one of those people consents to the disclosure of the information. Facebook contends that this exception applies here, because even if a user didn't directly consent to Facebook's disclosure of information to app developers, the user's friend consented when that friend interacted with the app.

There are two problems with this argument, at least at the pleading stage. First, it does not respond to the allegations about Facebook's decision to share user information with whitelisted apps starting in 2015 or with business partners – nothing in the complaint or the judicially noticeable material would permit a conclusion that either a plaintiff or a plaintiff's

Facebook friend permitted disclosure to those entities. Second, as to the typical app developer, as discussed in Section IV, plaintiffs who signed up for Facebook before 2009 did not (if the allegations of the complaint are to be believed) authorize Facebook to share information through their friends with app developers. Nor is there a basis to conclude as a matter of law that their friends authorized the app developers to receive this information. Neither side describes with any specificity the dialogue that would have taken place between the friend and the app developer that resulted in the app developer's acquisition of communications that would otherwise be protected by the SCA.

The motion to dismiss this claim is granted with respect to the first category of conduct for plaintiffs who consented to this conduct, as discussed in Section IV. It is denied in all other respects.

Video Privacy Protection Act. The Video Privacy Protection Act ("VPPA") was passed by Congress after a newspaper published a Supreme Court nominee's video rental history. The statute prohibits knowing disclosure of "personally identifiable information" by a "video tape service provider." 18 U.S.C. § 2710. The plaintiffs have adequately alleged that Facebook violated the VPPA.

Facebook first contends that the user information it shared with app developers, whitelisted apps, and business partners is not "personally identifiable information." But the VPPA defines this broadly as "information which identifies a person as having requested or obtained specific video materials or services. . . ." 18 U.S.C. § 2710(a)(3). Or as the Ninth Circuit has put it, "information that would readily permit an ordinary person to identify a specific individual's video-watching behavior." *Eichenberger*, 876 F.3d 979, 985 (9th Cir. 2017) (quotations omitted). The plaintiffs adequately allege that Facebook regularly shared information about the videos that users received in their private messages and about videos they "liked." Complaint ¶¶ 424, 867, 868. And it is reasonable to infer, at least at the pleading stage, that when a user receives a video or likes a video, he watches the video, such that this information sheds significant light on his video-watching behavior.

Facebook also contends it is not a "video tape service provider" within the meaning of the VPPA, but that too cannot be decided in Facebook's favor on this motion to dismiss. The statute defines a video tape service provider as anyone "engaged in the business . . . of rental, sale, *or delivery* of prerecorded video cassette tapes or similar audio visual materials . . . ." 18 U.S.C. § 2710(a)(4) (emphasis added).[19] The plaintiffs allege that Facebook "regularly delivers" video content to users and maintains a cache of videos and visual materials, including from content providers like Netflix, for their delivery to users. Complaint ¶¶ 862, 864. Although one could imagine a different conclusion at summary judgment once the evidence is examined, it is plausible to conclude from these and related allegations that Facebook engages in the business of delivering audio visual materials, and that its business is "significantly tailored to serve that purpose." *See, e.g.*, *In re Vizio, Inc., Consumer Privacy Litigation*, 238 F. Supp. 3d 1204, 1221 (C.D. Cal. 2017).

Facebook also did not obtain the type of consent necessary to authorize the sharing of this information. The VPPA outlines specific requirements for consent in the context of sharing video-information, including that it be set out in a separate form. *See* 18 U.S.C. § 2710(b)(2)(B). Facebook does not argue that it obtained this type of consent from its users. Therefore, even beyond the reasons discussed in Section IV relating to consent more generally, the plaintiffs adequately allege that they did not consent within the meaning of the VPPA, and this applies to all the information-sharing, for all time periods, discussed in this ruling.

The motion to dismiss this claim is denied.

Negligence and Gross Negligence. Negligence has four elements under California law: duty, breach, causation, and injury. See *Vasilenko v. Grace Family Church*, 3 Cal. 5th 1077, 1083 (2017). The plaintiffs' negligence claim is based on the fourth category of conduct, and it adequately alleges each of the required elements as to that conduct. As discussed at length above,

[19] There is no dispute in this motion that at least some video files that get distributed on Facebook's platform qualify as "similar audio visual materials." 18 U.S.C. § 2710(a)(4).

the plaintiffs have alleged present and non-speculative privacy injuries.[20] The plaintiffs have also plausibly alleged that Facebook breached a duty to them. Facebook had a responsibility to handle its users' sensitive information with care. *See Bass v. Facebook, Inc.*, 2019 WL 2568799, at *10 (N.D. Cal. June 21, 2019). And contrary to Facebook's argument, the plaintiffs do not seek to hold Facebook liable for the conduct of the app developers and business partners; they seek to hold the company liable for its own misconduct with respect to their information. Specifically, the plaintiffs allege that they entrusted Facebook with their sensitive information, and that Facebook failed to use reasonable care to safeguard that information, giving third parties access to it without taking any precautions to constrain that access to protect the plaintiffs' privacy, despite assurances it would do so. This lawsuit is first and foremost about how Facebook handled its users' information, not about what third parties did once they got hold of it.

The various exculpatory clauses in Facebook's terms also do not require dismissing the negligence claim. While such clauses can successfully waive liability for ordinary negligence, California law forbids limiting liability for gross negligence. *City of Santa Barbara v. Superior Court*, 41 Cal. 4th 747, 777 (2007) ("[P]ublic policy generally precludes enforcement of an agreement that would remove an obligation to adhere to even a minimal standard of care."). The complaint plausibly alleges gross negligence, since it contends that Facebook did essentially nothing to safeguard users' information – conduct that might well be characterized as lacking "even scant care." *Id*. at 754. Ordinary and gross negligence are not separate causes of action in California. *See Nypl v. Crisis Prevention Institute*, 2018 WL 4488760, at *9 n.6 (N.D. Cal. Sept. 17, 2018). Thus, the applicability of the waiver will turn at least in part on the degree of negligence (if any) that the plaintiffs can ultimately prove.

The motion to dismiss this claim is denied.

---

[20] The parties' briefs focus on the economic loss rule, which governs the availability of recovery for purely economic losses in a tort action. But as previously discussed, the plaintiffs' allegations of various sorts of economic injury are too speculative to support either standing or substantive legal claims. The economic loss rule is therefore irrelevant. There perhaps remains a question whether the plaintiffs can recover for their intangible injuries on a negligence theory, but the parties haven't briefed this issue, and its resolution may require further factual development.

Deceit by concealment or omission. For a defendant to be liable for deceit by concealment under California law, a variety of things must have occurred. *See* Cal. Civ. Code §§ 1709-1710. First, the defendant must have: (i) had a duty to disclose a material fact to the plaintiff; and (ii) intentionally concealed that fact with intent to defraud the plaintiff. *Tae Youn Shim v. Lawler,* 2019 WL 2996443, at *17 (N.D. Cal. July 9, 2019). In addition, the plaintiff must have: (iii) been unaware of that fact (and would have acted differently if he were aware), and (iv) sustained some damage as a result. *See id*; *see also* Cal. Civ. Code § 1710(3). Because this claim sounds in fraud, the plaintiffs are subject to a heightened pleading standard, which means that they "must state with particularity the circumstances constituting fraud . . . ." *See* Federal Rules of Civil Procedure 9(b).

With respect to the allegations that Facebook improperly shared information with standard app developers and failed to prevent third parties from improperly using sensitive information, the plaintiffs have not satisfied the heightened pleading requirements necessary to state a claim for deceit by concealment.[21] However, if the plaintiffs' allegations are true, Facebook's conduct with respect to whitelisted apps and business partners crosses into the realm of fraudulent conduct. As discussed earlier, the plaintiffs have sufficiently alleged that their privacy interests were harmed through the disclosure of their information to these entities. The plaintiffs have also adequately alleged that Facebook intended to defraud its users regarding this conduct: the plaintiffs contrast Facebook's public-facing statements about protecting privacy and restricting information-sharing with the reality of Facebook's alleged practices, and that contrast is a sufficient basis from which to infer fraudulent intent at the pleading stage.

As with the negligence claim, Facebook is wrong to assert that its exculpatory clause relieves it from liability for this claim. Under California law, Facebook's exculpatory clause does not apply to a claim sounding in fraud such as deceit by concealment. *See* Cal. Civ. Code § 1668

[21] Of course, dismissal of a subset of claims with prejudice does not preclude a plaintiff from seeking revival if discovery reveals a factual basis that justifies reconsideration of this order. *See* Fed. R. Civ. P. 54(b); *WPP Luxembourg Gamma Three Sarl v. Spot Runner, Inc.*, 655 F.3d 1039, 1059 (9th Cir. 2011), *abrogated on other grounds by Lorenzo v. SEC*, 139 S. Ct. 1094 (2019).

("All contracts which have for their object, directly or indirectly, to exempt anyone from responsibility for his own fraud, or willful injury to the person or property of another, or violation of law, whether willful or negligent, are against the policy of the law."); *see also, e.g.*, *Manderville v. PCG&S Group, Inc.*, 146 Cal. App. 4th 1486, 1500 (2007) ("It is well-established in California that a party to a contract is precluded under section 1668 from contracting away his or her liability for fraud or deceit based on intentional misrepresentation.").

The motion to dismiss is granted with respect to the first and fourth categories of conduct, and denied with respect to the second and third categories of conduct.

Breach of contract. The elements for breach of contract under California law are: (i) the existence of a contract; (ii) the plaintiff's performance or excuse for nonperformance of its side of the agreement; (iii) the defendant's breach; and (iv) resulting damage to the plaintiff. *See Buschman v. Anesthesia Bus. Consultants LLC*, 42 F. Supp. 3d 1244, 1250 (N.D. Cal. 2014).

As discussed in Section IV, the contract between Facebook and its users does not merely consist of the SRR, as the plaintiffs contend. It also includes the Data Use Policy. This makes it somewhat challenging to discern whether the plaintiffs have adequately alleged claims for breach of contract, because the plaintiffs' arguments are largely based on the assumption that the Data Use Policy is not part of the contract. Nonetheless, once it's understood that the Policy is part of the contract, it becomes clear that the second, third, and fourth categories of alleged wrongdoing addressed in this ruling give rise to claims for breach of contract. *See Johnson v. City of Shelby*, 574 U.S. 10, 10 (2014) (per curiam) ("Federal pleading rules . . . do not countenance dismissal of a complaint for imperfect statement of the legal theory supporting the claim asserted."); *Skinner v. Switzer*, 562 U.S. 521, 530 (2011) ("[U]nder the Federal Rules of Civil Procedure, a complaint need not pin plaintiff's claim for relief to a precise legal theory."). The SRR states: "You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings." Appendix A at 2. The plaintiffs have adequately alleged that Facebook breached this promise when it disclosed user information to whitelisted apps and business partners without permission, and without giving the plaintiffs the

ability to prevent this disclosure. In addition, for the allegations that Facebook allowed companies to misuse the information, the complaint sufficiently alleges that Facebook did not fulfill its promise in the Data Use Policy that apps would be allowed to use information "only in connection with" that user's friends. Complaint ¶ 569; Appendix B at 10.

In contrast, the plaintiffs have not adequately alleged a breach of contract based on the first category of wrongdoing: allowing standard app developers to obtain user information through users' friends. As discussed in Section IV, Facebook began disclosing this practice in its contractual language starting in roughly 2009, which means that this conduct does not give rise to a breach of contract claim for users who established their Facebook accounts after that time. For users who established their accounts beforehand, the complaint plausibly alleges that the practice wasn't disclosed. But simple failure to disclose a practice doesn't constitute a breach of contract. And although it's certainly conceivable that the practice violated provisions of Facebook's earlier contractual language, the plaintiffs do not identify or rely on any such language in their complaint. Therefore, for all plaintiffs, the complaint does not articulate a breach of contract theory based on the disclosure of sensitive user information to standard app developers, even though the complaint alleges that some users didn't consent to it.

Facebook argues that the plaintiffs have not adequately alleged that they were damaged by any breaches. But that is wrong. The plaintiffs can seek damages for "the detriment caused by the breach." *Stephens v. City of Vista*, 994 F.2d 650, 657 (9th Cir. 1993). As discussed in Sections II and III, the detriment the plaintiffs suffered was an invasion of their privacy. Perhaps some of the individual plaintiffs suffered a harm from this privacy invasion that can be measured by compensatory damages. *See, e.g.*, *Windeler v. Scheers Jewelers*, 8 Cal. App. 3d 844, 850-52 (Cal. Ct. App. 1970); *Leavy v. Cooney*, 214 Cal. App. 2d 496, 501-02 (Cal. Ct. App. 1963). Perhaps others did not, but under California law even those plaintiffs may recover nominal damages. Judicial Council of California Civil Jury Instruction 360; *In re Facebook Privacy Litigation*, 192 F. Supp. 3d 1053, 1062 (N.D. Cal. 2016).

The motion to dismiss this claim is granted with respect to the first category of

wrongdoing. Because it is possible that the complaint could be amended to allege a breach of contract claim for plaintiffs who established their accounts before Facebook disclosed the practice, dismissal is with leave to amend for these plaintiffs only. The motion to dismiss this claim is denied in all other respects.

Breach of the implied covenant of good faith and fair dealing. In addition to explicit promises, every contract includes an implicit promise not to take an action that would deprive the other contracting party of the benefits of their agreement. *See Rockridge Trust v. Wells Fargo, N.A.*, 985 F. Supp. 2d 1110, 1156 (N.D. Cal. 2013). This obligation is known as the "implied covenant of good faith and fair dealing," and it protects the parties' "reasonable expectations . . . based on their mutual promises." *Digerati Holdings, LLC v. Young Money Entertainment, LLC*, 194 Cal. App. 4th 873, 885 (2011). To state a claim for breach of this implied promise, "a plaintiff must identify the specific contractual provision that was frustrated" by the defendant's conduct. *Perez v. Wells Fargo Bank, N.A.*, 2011 WL 3809808, at *18 (N.D. Cal. Aug. 29, 2011). This doctrine cannot, however, "impose substantive duties or limits on the contracting parties beyond those incorporated in the specific terms of their agreement." *Guz v. Bechtel National Inc.*, 24 Cal. 4th 317, 350 (2000).

Just as they've stated claims for breach of contract with respect to the second, third, and fourth categories of conduct, the plaintiffs have stated claims for breach of the implied covenant of good faith and fair dealing for that conduct. Indeed, the case for breach of the implied covenant is stronger, because even if Facebook were, at a later stage in the litigation, able to identify a technical argument for why it did not *quite* violate the literal terms of its contract with its users, it would be difficult to conclude (if the factual allegations in the complaint are true) that Facebook did not frustrate the purposes of the contract, and intentionally so. But for the first category of conduct, the plaintiffs have not offered sufficient information about the earlier contractual language to assess whether the conduct frustrated the purpose of Facebook's contract with its users.

Accordingly, with respect to the first category of conduct, this claim for breach of the

implied covenant is, along with the parallel claim for breach of contract, dismissed. Dismissal is with leave to amend for plaintiffs who signed up before the information-sharing practice was included in the contractual language, and without leave to amend for those who signed up after it was disclosed.[22]

Unjust Enrichment. The plaintiffs also state a claim for unjust enrichment. Specifically, they allege that even if they have no remedy for breach of contract, they should be able to recover amounts that Facebook gained by improperly disseminating their information. The plaintiffs are permitted to plead claims for breach of contract and unjust enrichment in the alternative. *Bruton v. Gerber Production Co.*, 703 F. App'x 468 (9th Cir. 2017); *In re Vizio, Inc., Consumer Privacy Litigation*, 238 F. Supp. 3d 1204, 1233 (C.D. Cal. 2017); *Hartford Casualty Insurance Co. v. J.R. Marketing., L.L.C.*, 61 Cal. 4th 988, 998 (2015). And even if the plaintiffs suffered no economic loss from the disclosure of their information, they may proceed at this stage on a claim for unjust enrichment to recover the gains that Facebook realized from its allegedly improper conduct. *See Hadley v. Kellogg Sales Co.*, 324 F. Supp. 3d 1084, 1113 (N.D. Cal. 2018).[23] The motion to dismiss this claim is granted as to the plaintiffs who consented as discussed in Section IV, but otherwise denied.

Right of Publicity. California's common law right of publicity makes unlawful the appropriation of someone's name or likeness without his consent when it both (1) injures that person and (2) is used to the defendant's advantage. *See Perkins v. LinkedIn Corp*., 53 F. Supp. 3d 1190, 1214 (N.D. Cal. 2014).

Facebook's motion to dismiss this claim is granted. The allegations about how Facebook shared the plaintiffs' information with third parties is categorically different from the type of

[22] The Court will likely stay, along with the other non-prioritized claims, the claims that this ruling dismisses with leave to amend, although the Court will discuss this matter with the parties at the next case management conference.

[23] The complaint, in articulating the unjust enrichment claim, frequently uses the term "quantum meruit." It appears that the complaint uses this term incorrectly; no true theory of quantum meruit recovery has been articulated by the plaintiffs. *See Maglica v. Maglica*, 66 Cal. App. 4th 442, 449 (Cal. Ct. App. 1998) (describing quantum meruit as recovery of "the reasonable value of the services rendered provided they were of direct benefit to the defendant.").

conduct made unlawful by this tort, such as using a plaintiff's face or name to promote a product or service. *See Comedy III Productions., Inc. v. Gary Saderup, Inc.*, 25 Cal. 4th 387, 399 (2001) ("The right of publicity, like copyright, protects a form of intellectual property that society deems to have some social utility. Often considerable money, time and energy are needed to develop one's prominence in a particular field. Years of labor may be required before one's skill, reputation, notoriety or virtues are sufficiently developed to permit an economic return through some medium of commercial promotion." (internal quotations omitted)*; see also Abdul-Jabbar v. General Motors Corp.*, 85 F.3d 407, 415 (9th Cir. 1996); *cf. Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1217 (N.D. Cal. 2014). Because the Court cannot conceive of a way that the plaintiffs could successfully allege this claim, dismissal is without leave to amend.

California's Unfair Competition Law. California's Unfair Competition Law ("UCL") prohibits business practices that are unlawful, unfair, or fraudulent. *See* Cal. Bus. & Prof. Code § 17200, *et seq.* To have standing under California law to pursue this claim (a standard that is different from Article III standing), the plaintiffs must show that they "lost money or property" because of Facebook's conduct. *See* Cal. Bus. & Prof. Code § 17204; *see also Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 317 (2011). The plaintiffs' UCL claim fails because they have not adequately alleged lost money or property. As discussed in Section III, the plaintiffs' theory of economic loss is purely hypothetical. It's true, as discussed in connection with the unjust enrichment claim, that Facebook may have gained money through its sharing or use of the plaintiffs' information, but that's different from saying the plaintiffs lost money. Further, the plaintiffs here do not allege that they paid any premiums (or any money at all) to Facebook to potentially give rise to standing under California law. *Compare In re Anthem, Inc. Data Breach Litigation,* 2016 WL 3029783, at *30 (N.D. Cal. May 27, 2016). This claim is also dismissed without leave to amend.

VI. CONCLUSION

The motion to dismiss is granted in part and denied in part. The deadline for Facebook to file an answer to the complaint, along with all other scheduling matters, will be discussed at a

case management conference on October 1, 2019 at 2:00 p.m. The parties should file a joint case management statement by September 24, 2019.

IT IS SO ORDERED.

Dated: September 9, 2019

VINCE CHHABRIA
United States District Judge

Appendix A

This agreement was written in English (US). To the extent any translated version of this agreement conflicts with the English version, the English version controls. Please note that Section 16 contains certain changes to the general terms for users outside the United States.

Date of Last Revision: June 8, 2012.

Statement of Rights and Responsibilities

This Statement of Rights and Responsibilities ("Statement," "Terms," or "SRR") derives from the Facebook Principles, and is our terms of service that governs our relationship with users and others who interact with Facebook. By using or accessing Facebook, you agree to this Statement, as updated from time to time in accordance with Section 14 below. Additionally, you will find resources at the end of this document that help you understand how Facebook works.

1. **Privacy**

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

2. **Sharing Your Content and Information**

   You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings. In addition:

   1. For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.
   2. When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others).
   3. When you use an application, the application may ask for your permission to access your content and information as well as content and information that others have shared with you. 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. (To learn more about Platform, including how you can control what information other people may share with applications, read our Data Use Policy and Platform Page.)
   4. When you publish content or information using the Public setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information,

and to associate it with you (i.e., your name and profile picture).

5. We always appreciate your feedback or other suggestions about Facebook, but you understand that we may use them without any obligation to compensate you for them (just as you have no obligation to offer them).

3. **Safety**

We do our best to keep Facebook safe, but we cannot guarantee it. We need your help to keep Facebook safe, which includes the following commitments by you:

1. You will not post unauthorized commercial communications (such as spam) on Facebook.
2. You will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our prior permission.
3. You will not engage in unlawful multi-level marketing, such as a pyramid scheme, on Facebook.
4. You will not upload viruses or other malicious code.
5. You will not solicit login information or access an account belonging to someone else.
6. You will not bully, intimidate, or harass any user.
7. You will not post content that: is hate speech, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence.
8. You will not develop or operate a third-party application containing alcohol-related, dating or other mature content (including advertisements) without appropriate age-based restrictions.
9. You will follow our Promotions Guidelines and all applicable laws if you publicize or offer any contest, giveaway, or sweepstakes (“promotion”) on Facebook.
10. You will not use Facebook to do anything unlawful, misleading, malicious, or discriminatory.
11. You will not do anything that could disable, overburden, or impair the proper working or appearance of Facebook, such as a denial of service attack or interference with page rendering or other Facebook functionality.
12. You will not facilitate or encourage any violations of this Statement or our policies.

4. **Registration and Account Security**

Facebook users provide their real names and information, and we need your help to keep it that way. Here are some commitments you make to us relating to registering and maintaining the security of your account:

1. You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission.
2. You will not create more than one personal account.
3. If we disable your account, you will not create another one without our permission.
4. You will not use your personal timeline for your own commercial gain (such as selling your status update to an advertiser).

5. You will not use Facebook if you are under 13.
6. You will not use Facebook if you are a convicted sex offender.
7. You will keep your contact information accurate and up-to-date.
8. You will not share your password (or in the case of developers, your secret key), let anyone else access your account, or do anything else that might jeopardize the security of your account.
9. You will not transfer your account (including any Page or application you administer) to anyone without first getting our written permission.
10. If you select a username or similar identifier for your account or Page, we reserve the right to remove or reclaim it if we believe it is appropriate (such as when a trademark owner complains about a username that does not closely relate to a user's actual name).

5. **Protecting Other People's Rights**

We respect other people's rights, and expect you to do the same.

1. You will not post content or take any action on Facebook that infringes or violates someone else's rights or otherwise violates the law.
2. We can remove any content or information you post on Facebook if we believe that it violates this Statement or our policies.
3. We provide you with tools to help you protect your intellectual property rights. To learn more, visit our How to Report Claims of Intellectual Property Infringement page.
4. If we remove your content for infringing someone else's copyright, and you believe we removed it by mistake, we will provide you with an opportunity to appeal.
5. If you repeatedly infringe other people's intellectual property rights, we will disable your account when appropriate.
6. You will not use our copyrights or trademarks (including Facebook, the Facebook and F Logos, FB, Face, Poke, Book and Wall), or any confusingly similar marks, except as expressly permitted by our Brand Usage Guidelines or with our prior written permission.
7. If you collect information from users, you will: obtain their consent, make it clear you (and not Facebook) are the one collecting their information, and post a privacy policy explaining what information you collect and how you will use it.
8. You will not post anyone's identification documents or sensitive financial information on Facebook.
9. You will not tag users or send email invitations to non-users without their consent. Facebook offers social reporting tools to enable users to provide feedback about tagging.

6. **Mobile and Other Devices**

1. We currently provide our mobile services for free, but please be aware that your carrier's normal rates and fees, such as text messaging fees, will still apply.
2. In the event you change or deactivate your mobile telephone number, you will update your account information on Facebook within 48 hours to ensure that your messages are

not sent to the person who acquires your old number.

3. You provide consent and all rights necessary to enable users to sync (including through an application) their devices with any information that is visible to them on Facebook.

7. **Payments**

If you make a payment on Facebook or use Facebook Credits, you agree to our Payments Terms.

8. **Special Provisions Applicable to Social Plugins**

If you include our Social Plugins, such as the Share or Like buttons on your website, the following additional terms apply to you:

1. We give you permission to use Facebook's Social Plugins so that users can post links or content from your website on Facebook.
2. You give us permission to use and allow others to use such links and content on Facebook.
3. You will not place a Social Plugin on any page containing content that would violate this Statement if posted on Facebook.

9. **Special Provisions Applicable to Developers/Operators of Applications and Websites**

If you are a developer or operator of a Platform application or website, the following additional terms apply to you:

1. You are responsible for your application and its content and all uses you make of Platform. This includes ensuring your application or use of Platform meets our Facebook Platform Policies and our Advertising Guidelines.
2. Your access to and use of data you receive from Facebook, will be limited as follows:
    1. You will only request data you need to operate your application.
    2. You will have a privacy policy that tells users what user data you are going to use and how you will use, display, share, or transfer that data and you will include your privacy policy URL in the Developer Application.
    3. You will not use, display, share, or transfer a user's data in a manner inconsistent with your privacy policy.
    4. You will delete all data you receive from us concerning a user if the user asks you to do so, and will provide a mechanism for users to make such a request.
    5. You will not include data you receive from us concerning a user in any advertising creative.
    6. You will not directly or indirectly transfer any data you receive from us to (or use such data in connection with) any ad network, ad exchange, data broker, or other advertising related toolset, even if a user consents to that transfer or use.
    7. You will not sell user data. If you are acquired by or merge with a third party, you can continue to use user data within your application, but you cannot transfer user data outside of your application.
    8. We can require you to delete user data if you use it in a

way that we determine is inconsistent with users' expectations.
9. We can limit your access to data.
10. You will comply with all other restrictions contained in our Facebook Platform Policies.

3. You will not give us information that you independently collect from a user or a user's content without that user's consent.
4. You will make it easy for users to remove or disconnect from your application.
5. You will make it easy for users to contact you. We can also share your email address with users and others claiming that you have infringed or otherwise violated their rights.
6. You will provide customer support for your application.
7. You will not show third party ads or web search boxes on www.facebook.com.
8. We give you all rights necessary to use the code, APIs, data, and tools you receive from us.
9. You will not sell, transfer, or sublicense our code, APIs, or tools to anyone.
10. You will not misrepresent your relationship with Facebook to others.
11. You may use the logos we make available to developers or issue a press release or other public statement so long as you follow our Facebook Platform Policies.
12. We can issue a press release describing our relationship with you.
13. You will comply with all applicable laws. In particular you will (if applicable):
    1. have a policy for removing infringing content and terminating repeat infringers that complies with the Digital Millennium Copyright Act.
    2. comply with the Video Privacy Protection Act (VPPA), and obtain any opt-in consent necessary from users so that user data subject to the VPPA may be shared on Facebook. You represent that any disclosure to us will not be incidental to the ordinary course of your business.
14. We do not guarantee that Platform will always be free.
15. You give us all rights necessary to enable your application to work with Facebook, including the right to incorporate content and information you provide to us into streams, timelines, and user action stories.
16. You give us the right to link to or frame your application, and place content, including ads, around your application.
17. We can analyze your application, content, and data for any purpose, including commercial (such as for targeting the delivery of advertisements and indexing content for search).
18. To ensure your application is safe for users, we can audit it.
19. We can create applications that offer similar features and services to, or otherwise compete with, your application.

10. **About Advertisements and Other Commercial Content Served or Enhanced by Facebook**

Our goal is to deliver ads and commercial content that are valuable to our users and advertisers. In order to help us do that, you agree to the following:

1. You can use your privacy settings to limit how your name and

profile picture may be associated with commercial, sponsored, or related content (such as a brand you like) served or enhanced by us. You give us permission to use your name and profile picture in connection with that content, subject to the limits you place.

2. We do not give your content or information to advertisers without your consent.
3. You understand that we may not always identify paid services and communications as such.

11. **Special Provisions Applicable to Advertisers**

You can target your desired audience by buying ads on Facebook or our publisher network. The following additional terms apply to you if you place an order through our online advertising portal (Order):

1. When you place an Order, you will tell us the type of advertising you want to buy, the amount you want to spend, and your bid. If we accept your Order, we will deliver your ads as inventory becomes available. When serving your ad, we do our best to deliver the ads to the audience you specify, although we cannot guarantee in every instance that your ad will reach its intended target.
2. In instances where we believe doing so will enhance the effectiveness of your advertising campaign, we may broaden the targeting criteria you specify.
3. You will pay for your Orders in accordance with our Payments Terms. The amount you owe will be calculated based on our tracking mechanisms.
4. Your ads will comply with our Advertising Guidelines.
5. We will determine the size, placement, and positioning of your ads.
6. We do not guarantee the activity that your ads will receive, such as the number of clicks your ads will get.
7. We cannot control how clicks are generated on your ads. We have systems that attempt to detect and filter certain click activity, but we are not responsible for click fraud, technological issues, or other potentially invalid click activity that may affect the cost of running ads.
8. You can cancel your Order at any time through our online portal, but it may take up to 24 hours before the ad stops running. You are responsible for paying for all ads that run.
9. Our license to run your ad will end when we have completed your Order. You understand, however, that if users have interacted with your ad, your ad may remain until the users delete it.
10. We can use your ads and related content and information for marketing or promotional purposes.
11. You will not issue any press release or make public statements about your relationship with Facebook without our prior written permission.
12. We may reject or remove any ad for any reason.
13. If you are placing ads on someone else's behalf, you must have permission to place those ads, including the following:
    1. You warrant that you have the legal authority to bind the advertiser to this Statement.
    2. You agree that if the advertiser you represent violates this Statement, we may hold you responsible for that violation.

12. **Special Provisions Applicable to Pages**

If you create or administer a Page on Facebook, you agree to our Pages Terms.

13. **Special Provisions Applicable to Software**

1. If you download our software, such as a stand-alone software product or a browser plugin, you agree that from time to time, the software may download upgrades, updates and additional features from us in order to improve, enhance and further develop the software.
2. You will not modify, create derivative works of, decompile or otherwise attempt to extract source code from us, unless you are expressly permitted to do so under an open source license or we give you express written permission.

14. **Amendments**

1. We can change this Statement if we provide you notice (by posting the change on the Facebook Site Governance Page) and an opportunity to comment. To get notice of any future changes to this Statement, visit our Facebook Site Governance Page and "like" the Page.
2. For changes to sections 7, 8, 9, and 11 (sections relating to payments, application developers, website operators, and advertisers), we will give you a minimum of three days notice. For all other changes we will give you a minimum of seven days notice. Comments to proposed changes will be made on the Facebook Site Governance Page.
3. If more than 7,000 users post a substantive comment on a particular proposed change, we will also give you the opportunity to participate in a vote in which you will be provided alternatives. The vote shall be binding on us if more than 30% of all active registered users as of the date of the notice vote.
4. If we make changes to policies referenced in or incorporated by this Statement, we may provide notice on the Site Governance Page.
5. We can make changes for legal or administrative reasons, or to correct an inaccurate statement, upon notice without opportunity to comment.
6. Your continued use of Facebook following changes to our terms constitutes your acceptance of our amended terms.

15. **Termination**

If you violate the letter or spirit of this Statement, or otherwise create risk or possible legal exposure for us, we can stop providing all or part of Facebook to you. We will notify you by email or at the next time you attempt to access your account. You may also delete your account or disable your application at any time. In all such cases, this Statement shall terminate, but the following provisions will still apply: 2.2, 2.4, 3-5, 8.2, 9.1-9.3, 9.9, 9.10, 9.13, 9.15, 9.18, 10.3, 11.2, 11.5, 11.6, 11.9, 11.12, 11.13, and 15-19.

16. **Disputes**

1. You will resolve any claim, cause of action or dispute (claim) you have with us arising out of or relating to this Statement or Facebook exclusively in a state or federal court located in Santa Clara County. The laws of the State of California will govern this Statement, as well as any claim that might arise between you and us, without regard to conflict of law provisions. You agree to submit to the personal jurisdiction of the courts located in Santa Clara County, California for the purpose of litigating all such claims.
2. If anyone brings a claim against us related to your actions, content or information on Facebook, you will indemnify and hold us harmless from and against all damages, losses, and expenses of any kind (including reasonable legal fees and costs) related to such claim. Although we provide rules for user conduct, we do not control or direct users' actions on Facebook and are not responsible for the content or information users transmit or share on Facebook. We are not responsible for any offensive, inappropriate, obscene, unlawful or otherwise objectionable content or information you may encounter on Facebook. We are not responsible for the conduct, whether online or offline, or any user of Facebook.
3. WE TRY TO KEEP FACEBOOK UP, BUG-FREE, AND SAFE, BUT YOU USE IT AT YOUR OWN RISK. WE ARE PROVIDING FACEBOOK AS IS WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. WE DO NOT GUARANTEE THAT FACEBOOK WILL ALWAYS BE SAFE, SECURE OR ERROR-FREE OR THAT FACEBOOK WILL ALWAYS FUNCTION WITHOUT DISRUPTIONS, DELAYS OR IMPERFECTIONS. 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. IF YOU ARE A CALIFORNIA RESIDENT, YOU WAIVE CALIFORNIA CIVIL CODE §1542, WHICH SAYS: A GENERAL RELEASE DOES NOT EXTEND TO CLAIMS WHICH THE CREDITOR DOES NOT KNOW OR SUSPECT TO EXIST IN HIS FAVOR AT THE TIME OF EXECUTING THE RELEASE, WHICH IF KNOWN BY HIM MUST HAVE MATERIALLY AFFECTED HIS SETTLEMENT WITH THE DEBTOR. WE WILL NOT BE LIABLE TO YOU FOR ANY LOST PROFITS OR OTHER CONSEQUENTIAL, SPECIAL, INDIRECT, OR INCIDENTAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS STATEMENT OR FACEBOOK, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR AGGREGATE LIABILITY ARISING OUT OF THIS STATEMENT OR FACEBOOK WILL NOT EXCEED THE GREATER OF ONE HUNDRED DOLLARS ($100) OR THE AMOUNT YOU HAVE PAID US IN THE PAST

TWELVE MONTHS. APPLICABLE LAW MAY NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY OR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. IN SUCH CASES, FACEBOOK'S LIABILITY WILL BE LIMITED TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW.

17. **Special Provisions Applicable to Users Outside the United States**

We strive to create a global community with consistent standards for everyone, but we also strive to respect local laws. The following provisions apply to users and non-users who interact with Facebook outside the United States:

1. You consent to having your personal data transferred to and processed in the United States.
2. If you are located in a country embargoed by the United States, or are on the U.S. Treasury Department's list of Specially Designated Nationals you will not engage in commercial activities on Facebook (such as advertising or payments) or operate a Platform application or website.
3. Certain specific terms that apply only for German users are available here.

18. **Definitions**

1. By "Facebook" we mean the features and services we make available, including through (a) our website at www.facebook.com and any other Facebook branded or co-branded websites (including sub-domains, international versions, widgets, and mobile versions); (b) our Platform; (c) social plugins such as the Like button, the Share button and other similar offerings and (d) other media, software (such as a toolbar), devices, or networks now existing or later developed.
2. By "Platform" we mean a set of APIs and services (such as content) that enable others, including application developers and website operators, to retrieve data from Facebook or provide data to us.
3. By "information" we mean facts and other information about you, including actions taken by users and non-users who interact with Facebook.
4. By "content" we mean anything you or other users post on Facebook that would not be included in the definition of information.
5. By "data" or "user data" or "user's data" we mean any data, including a user's content or information that you or third parties can retrieve from Facebook or provide to Facebook through Platform.
6. By "post" we mean post on Facebook or otherwise make available by using Facebook.
7. By "use" we mean use, copy, publicly perform or display, distribute, modify, translate, and create derivative works of.
8. By "active registered user" we mean a user who has logged into Facebook at least once in the previous 30 days.
9. By "application" we mean any application or website that uses or accesses Platform, as well as anything else that receives or has received data from us. If you no longer access Platform

but have not deleted all data from us, the term application will apply until you delete the data.

19. **Other**

1. If you are a resident of or have your principal place of business in the US or Canada, this Statement is an agreement between you and Facebook, Inc. Otherwise, this Statement is an agreement between you and Facebook Ireland Limited. References to "us," "we," and "our" mean either Facebook, Inc. or Facebook Ireland Limited, as appropriate.
2. This Statement makes up the entire agreement between the parties regarding Facebook, and supersedes any prior agreements.
3. If any portion of this Statement is found to be unenforceable, the remaining portion will remain in full force and effect.
4. If we fail to enforce any of this Statement, it will not be considered a waiver.
5. Any amendment to or waiver of this Statement must be made in writing and signed by us.
6. You will not transfer any of your rights or obligations under this Statement to anyone else without our consent.
7. All of our rights and obligations under this Statement are freely assignable by us in connection with a merger, acquisition, or sale of assets, or by operation of law or otherwise.
8. Nothing in this Statement shall prevent us from complying with the law.
9. This Statement does not confer any third party beneficiary rights.
10. We reserve all rights not expressly granted to you.
11. You will comply with all applicable laws when using or accessing Facebook.

You may also want to review the following documents, which provide additional information about your use of Facebook:

- Data Use Policy: The Data Use Policy contains information to help you understand how we collect and use information.
- Payment Terms: These additional terms apply to all payments made on or through Facebook.
- Platform Page: This page helps you better understand what happens when you add a third-party application or use Facebook Connect, including how they may access and use your data.
- Facebook Platform Policies: These guidelines outline the policies that apply to applications, including Connect sites.
- Advertising Guidelines: These guidelines outline the policies that apply to advertisements placed on Facebook.
- Promotions Guidelines: These guidelines outline the policies that apply if you offer contests, sweepstakes, and other types of promotions on Facebook.
- Brand Permissions Center: These guidelines outline the policies that apply to use of Facebook trademarks, logos and screenshots.
- How to Report Claims of Intellectual Property Infringement
- Pages Terms: These guidelines apply to your use of Facebook Pages.
- Community Standards: These guidelines outline our expectations regarding the content you post to Facebook and your activity on Facebook.

To access the Statement of Rights and Responsibilities in several different languages, change the language setting for your Facebook session by clicking on the language link in the left corner of most pages. If the Statement is not available in the language you select, we will default to the English version.

Appendix B

Data Use Policy

Date of Last Revision: June 8, 2012

I. Information we receive and how it is used

Information we receive about you

We receive a number of different types of information about you, including:

Your information
Your information is the information that's required when you sign up for the site, as well as the information you choose to share.

- **Registration information**: When you sign up for Facebook, you are required to provide your name, email address, birthday, and gender.

- **Information you choose to share**: Your information also includes 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.

It also includes the information you choose to share when you take an action, such as when you add a friend, like a Page or a website, add a place to your story, find friends using our contact importers, or indicate you are in a relationship.

Your name, profile pictures, cover photos, gender, networks, username and User ID are treated just like information you choose to make public.
Your birthday allows us to do things like show you age-appropriate content and advertisements.

Information others share about you
We receive information about you from your friends and others, such as when they upload your contact information, post a photo of you, tag you in a photo or status update, or at a location, or add you to a group.

When people use Facebook, they may store and share information about you and others that they have, such as when they upload and manage their invites and contacts.

Other information we receive about you
We also receive other types of information about you:

- We receive data about you whenever you interact with Facebook, such as when you look at another person's timeline, send or receive a message, search for a friend or a Page, click on, view or otherwise interact with things, use a Facebook mobile app, or purchase Facebook Credits or make other purchases through Facebook.
- When you post things like photos or videos on Facebook, we may receive additional related data (or metadata), such as the time, date, and place you took the photo or video.
- We receive data from the computer, mobile phone or other device you use to access Facebook, including when multiple users log in from the same device. This may include your IP address and other information about things like your internet service, location, the type (including identifiers) of browser you use, or the pages you visit. For example, we may get your GPS or other location information so we can tell you if any of your friends are nearby.
- We receive data whenever you visit a game, application, or website that uses Facebook Platform or visit a site with a Facebook feature (such as a social plugin), sometimes through cookies. This may include the date and time you visit the site; the web address, or URL, you're on; technical information about the IP address, browser and the operating system you use; and, if you are logged in to Facebook, your User ID.
- Sometimes we get data from our advertising partners, customers and other third parties that helps us (or them) deliver ads, understand online activity, and generally make Facebook better. For example, an advertiser may tell us information about you (like how you responded to an ad on Facebook or on another site) in order to measure the effectiveness of - and improve the quality of - ads.

We also put together data from the information we already have about you and your friends. For example, we may put together data about you to determine which friends we should show you in your News Feed or suggest you tag in the photos you post. We may put together your current city with GPS and other location information we have about you to, for example, tell you and your friends about people or events nearby, or offer deals to you that you might be interested in. We may also put together data about you to serve you ads that might be more relevant to you.

When we get your GPS location, we put it together with other location information we have about you (like your current city). But we only keep it until it is no longer useful to provide you services, like keeping your last GPS coordinates to send you relevant notifications.
We only provide data to our advertising partners or customers after we have removed your name or any other personally identifying information from it, or have combined it with other people's data in a way that it is no longer associated with you.

Public information

When we use the phrase "public information" (which we sometimes refer to as "Everyone information"), we mean the information you choose to make public, as well as information that is always publicly available.

Information you choose to make public

Choosing to make your information public is exactly what it sounds like: **anyone**, including people off of Facebook, will be able to see it.

Choosing to make your information public also means that this information:

- can be associated with you (i.e., your name, profile pictures, cover photos, timeline, User ID, username, etc.) even off Facebook;
- can show up when someone does a search on Facebook or on a public search engine;
- will be accessible to the Facebook-integrated games, applications, and websites you and your friends use; and
- will be accessible to anyone who uses our APIs such as our Graph API.

Sometimes you will not be able to select an audience when you post something (like when you write on a Page's wall or comment on a news article that uses our comments plugin). This is because some types of stories are always public stories. As a general rule, you should assume that if you do not see a sharing icon, the information will be publicly available.
When others share information about you, they can also choose to make it public.

Information that is always publicly available

The types of information listed below are always publicly available, and are treated just like information you decided to make public.

- **Name**: This helps your friends and family find you. If you are uncomfortable sharing your real name, you can always delete your account.
- **Profile Pictures and Cover Photos**: These help your friends and family recognize you. If you are uncomfortable making any of these photos public, you can always delete it. Unless you delete them, when you add a new profile picture or cover photo, the previous photo will remain public in your profile picture or cover photo album.
- **Network**: This helps you see whom you will be sharing information with before you choose "Friends and Networks" as a custom audience. If you are uncomfortable making your network public, you can leave the network.
- **Gender**: This allows us to refer to you properly.
- **Username and User ID**: These allow you to give out a custom link to your timeline or Page, receive email at your Facebook email address, and help make Facebook Platform possible.

Usernames and User IDs

A Username (or Facebook URL) is a custom link to your timeline that you can give out to people or post on external websites. Usernames appear in the URL on your timeline. We also use your User ID to identify your Facebook account.

If someone has your Username or User ID, they can use it to access information about you through the facebook.com website. For example, if someone has your Username, they can type facebook.com/Username into their browser and see your public information as well as anything else you've let them see. Similarly, someone with your Username or User ID can access information about you through our APIs, such as our Graph API. Specifically, they can access your public information, along with your age range, language and country.

If you do not want your information to be accessible to Platform applications, you can turn off all Platform applications from your Privacy Settings. If you turn off Platform you will no longer be able to use any games or other applications until you turn Platform back on. For more information about the information that apps receive when you visit them, see Other websites and applications.

If you want to see information available about you through our Graph API, just type **https://graph.facebook.com/[User ID or Username]?metadata=1** into your browser.
Your Facebook email address includes your public username like so: username@facebook.com. You can control who can start a message thread with you using your "How You Connect" settings. If they include others on that message, the others can reply too.

How we use the information we receive

We use the information we receive about you in connection with the services and features we provide to you and other users like your friends, our partners, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use. For example, we may use the information we receive about you:

- as part of our efforts to keep Facebook products, services and integrations safe and secure;
- to protect Facebook's or others' rights or property;
- to provide you with location features and services, like telling you and your friends when something is going on nearby;
- to measure or understand the effectiveness of ads you and others see, including to deliver relevant ads to you;
- to make suggestions to you and other users on Facebook, such as: suggesting that your friend use our contact importer because you found friends using it, suggesting that another user add you as a friend because the user imported the same email address as you did, or suggesting that your friend tag you in a picture they have uploaded with you in it; and
- for internal operations, including troubleshooting, data analysis, testing, research and service improvement.

Granting us this permission not only allows us to provide Facebook as it exists today, but it also allows us to provide you with innovative features and services we develop in the future that use the information we receive about you in new ways.

While you are allowing us to use the information we receive about you, you always own all of your information. Your trust is important to us, which is why we don't share information we receive about you with others unless we have:

- received your permission;
- given you notice, such as by telling you about it in this policy; or
- removed your name or any other personally identifying information from it.

Of course, for information others share about you, they control how it is shared.

We store data for as long as it is necessary to provide products and services to you and others, including those described above. Typically, information associated with your account will be kept until your account is deleted. For certain categories of data, we may also tell you about specific data retention practices.

We are able to suggest that your friend tag you in a picture by scanning and comparing your friend's pictures to information we've put together from the other photos you've been tagged in. This allows us to make these suggestions. You can control whether we suggest that another user tag you in a photo using the "How Tags work" settings. Learn more at: https://www.facebook.com/help/tag-suggestions

Deleting and deactivating your account

If you want to stop using your account, you can either **deactivate** or **delete** it.

Deactivate

Deactivating your account puts your account on hold. Other users will no longer see your timeline, but we do not delete any of your information. Deactivating an account is the same as you telling us not to delete any information because you might want to reactivate your account at some point in the future. You can deactivate your account at: https://www.facebook.com/editaccount.php
Your friends will still see you listed in their list of friends while your account is deactivated.

Deletion

When you delete an account, it is permanently deleted from Facebook. It typically takes about one month to delete an account, but some information may remain in backup copies and logs for up to 90 days. You should only delete your account if you are sure you never want to reactivate it. You can delete your account at: https://www.facebook.com/help/contact.php?show_form=delete_account
Learn more at: https://www.facebook.com/help/?faq=356107851084108

Certain information is needed to provide you with services, so we only delete this information after you delete your account. Some of the things you do on Facebook aren't stored in your account, like posting to a group or sending someone a message (where your friend may still have a message you sent, even after you delete your account). That information remains after you delete your account.

II. Sharing and finding you on Facebook

Control each time you post

Whenever you post content (like a status update, photo or check-in), you can select a specific audience, or even customize your audience. To do this, simply click on the sharing icon and choose who can see it.

Choose this icon if you want to make something **Public**. Choosing to make something public is exactly what it sounds like. It means that anyone, including people off of Facebook, will be able to see or access it.
Choose this icon if you want to share with your Facebook **Friends**.
Choose this icon if you want to **Customize** your audience. You can also use this to hide your story from specific people.

If you tag someone, that person and their friends can see your story no matter what audience you selected. The same is true when you approve a tag someone else adds to your story.

Always think before you post. Just like anything else you post on the web or send in an email, information you share on Facebook can be copied or re-shared by anyone who can see it.

Although you choose with whom you share, there may be ways for others to determine information about you. For example, if you hide your birthday so no one can see it on your timeline, but friends post "happy birthday!" on your timeline, people may determine your birthday.
When you comment on or "like" someone else's story, or write on their timeline, that person gets to select the audience. For example, if a friend posts a Public story and you comment on it, your comment will be Public. Often, you can see the audience someone selected for their story before you post a comment; however, the person who posted the story may later change their audience.

You can control who can see the Facebook Pages you've "liked" by visiting your timeline, clicking on the Likes box on your timeline, and then clicking "Edit."
Sometimes you will not see a sharing icon when you post something (like when you write on a Page's wall or comment on a news article that uses our comments plugin). This is because some types of stories are always public stories. As a general rule, you should assume that if you do not see a sharing icon, the information will be publicly available.

Control over your timeline

Whenever you add things to your timeline you can select a specific audience, or even customize your audience. To do this, simply click on the sharing icon and choose who can see it.

Choose this icon if you want to make something **Public**. Choosing to make something public is exactly what it sounds like. It means that anyone, including people off of Facebook, will be able to see or access it.
Choose this icon if you want to share with your Facebook **Friends**.
Choose this icon if you want to **Customize** your audience. You can also use this to hide the item on your timeline from specific people.

When you select an audience for your friend list, you are only controlling who can see the entire list of your friends on your timeline. We call this a timeline visibility control. This is because your friend list is always available to the games, applications and websites you use, and your friendships may be visible elsewhere (such as on your friends' timelines or in searches). For example, if you select "Only Me" as the audience for your friend list, but your friend sets her friend list to "Public," anyone will be able to see your connection on your friend's timeline.

Similarly, if you choose to hide your gender, it only hides it on your timeline. This is because we, just like the applications you and your friends use, need to use your gender to refer to you properly on the site.

When someone tags you in a story (such as a photo, status update or check-in), you can choose whether you want that story to appear on your timeline. You can either approve each story individually or approve all stories by your friends. If you approve a story and later change your mind, you can remove it from your timeline.

People on Facebook may be able to see mutual friends, even if they cannot see your entire list of friends.
Some things (like your name, profile pictures and cover photos) do not have sharing icons because they are always publicly available. As a general rule, you should assume that if you do not see a sharing icon, the information will be publicly available.

Finding you on Facebook

To make it easier for your friends to find you, we allow anyone with your contact information (such as email address or telephone number) to find you through the Facebook search bar at the top of most pages, as well as other tools we provide, such as contact importers - even if you have not shared your contact information with them on Facebook.

You can choose who can look up your timeline using the email address or telephone number you added to your timeline through your privacy settings. But remember, if you choose Friends, only your current Facebook friends will be able to find you this way.

Your “How You Connect” settings do not control whether people can find you or a link to your timeline when they search for content they have permission to see, like a photo or other story you’ve been tagged in.

Access on phones and other devices

Once you share information with your friends and others, they may be able to sync it with or access it via their mobile phones and other devices. For example, if you share a photo on Facebook, someone viewing that photo could save it using Facebook tools or by other methods offered by their device or browser. Similarly, if you share your contact information with someone or invite someone to an event, they may be able to use Facebook or third party applications or devices to sync that information. Or, if one of your friends has a Facebook application on one of their devices, your

information (such as the things you post or photos you share) may be stored on or accessed by their device.

You should only share information with people you trust because they will be able to save it or re-share it with others, including when they sync the information to a device.

Activity log

Your activity log is a place where you can go to view most of your information on Facebook, including things you've hidden from your timeline. You can use this log to manage your content. For example, you can do things like delete stories, change the audience of your stories or stop an application from publishing to your timeline on your behalf.

When you hide something from your timeline, you are not deleting it. This means that the story may be visible elsewhere, like in your friends' News Feed. If you want to delete a story you posted, choose the delete option.

What your friends share about you

Links and Tags

Anyone can add a link to a story. Links are references to something on the Internet; anything from a website to a Page or timeline on Facebook. For example, if you are writing a story, you might include a link to a blog you are referencing or a link to the blogger's Facebook timeline. If someone clicks on a link to another person's timeline, they'll only see the things that they are allowed to see.

A tag is a special type of link to someone's timeline that suggests that the tagged person add your story to their timeline. In cases where the tagged person isn't included in the audience of the story, it will add them so they can see it. Anyone can tag you in anything. Once you are tagged, you and your friends will be able to see it (such as in News Feed or in search).

You can choose whether a story you've been tagged in appears on your timeline. You can either approve each story individually or approve all stories by your friends. If you approve a story and later change your mind, you can always remove it from your timeline.

If you do not want someone to tag you, we encourage you to reach out to them and give them that feedback. If that does not work, you can block them. This will prevent them from tagging you going forward.

If you are tagged in a private space (such as a message or a group) only the people who can see the private space can see the tag. Similarly, it you are tagged in a comment, only the people who can see the comment can see the tag.

Groups

Once you are in a Group, anyone in that Group can add you to a subgroup. When someone adds you to a Group, you will be listed as "invited" until you visit the Group. You can always leave a Group, which will prevent others from adding you to it again.

About Pages

Facebook Pages are public pages. Companies use Pages to share information about their products. Celebrities use Pages to talk about their latest projects. And communities use pages to discuss topics of interest, everything from baseball to the opera.

Because Pages are public, information you share with a Page is public information. This means, for example, that if you post a comment on a Page, that comment may be used by the Page owner off Facebook, and anyone can see it.

When you "like" a Page, you create a connection to that Page. The connection is added to your timeline and your friends may see it in their News Feeds. You may be contacted by or receive updates from the Page, such as in your News Feed and your messages. You can remove the Pages you've "liked" through your timeline or on the Page.

Some Pages contain content that comes directly from the Page owner. Page owners can do this through online plugins, such as an iframe, and it works just like the games and other applications you use through Facebook. Because this content comes directly from the Page owner, that Page may be able to collect information about you, just like any website.

Page administrators may have access to insights data, which will tell them generally about the people that visit their Page (as opposed to information about specific people). They may also know when you've made a connection to their Page because you've liked their Page or posted a comment.

III. Other websites and applications

About Facebook Platform

Facebook Platform (or simply Platform) refers to the way we help you share your information with the games, applications, and websites you and your friends use. Facebook Platform also lets you bring your friends with you, so you can connect with them off of Facebook. In these two ways, Facebook Platform helps you make your experiences on the web more personalized and social.

Remember that these games, applications and websites are created and maintained by other businesses and developers who are not part of Facebook, so you should always make sure to read their terms of service and privacy policies.

Controlling what information you share with applications

When you connect with a game, application or website - such as by going to a game, logging in to a website using your Facebook account, or adding an app to your timeline - we give the game, application, or website (sometimes referred to as just "Applications" or "Apps") your basic info, which includes your User ID, as well your friends' User IDs (or your friend list) and your public information.

Your friend list helps the application make your experience more social because it lets you find your friends on that application. Your User ID helps the application personalize your experience because it can connect your account on that application with your Facebook account, and it can access your basic info, which includes your public information and friend list. This includes the information you choose to make public, as well as information that is always publicly available. If the application needs additional information, such as your stories, photos or likes, it will have to ask you for specific permission.

The "Apps you use" setting lets you control the applications you use. You can see the permissions you have given these applications, the last time an application accessed your information, and the audience on Facebook for your timeline stories and activity the application posts on your behalf. You can also remove applications you no longer want, or turn off all Platform applications. When you turn all Platform applications off, your User ID is no longer given to applications, even when your friends use those applications. But you will no longer be able to use any games, applications or websites through Facebook.

When you first visit an app, Facebook lets the app know your language, your country, and whether you are under 18, between 18-20, or 21 and over. Age range lets apps provide you with age-appropriate content. If you install the app, it can access, store and update the information you've shared. Apps you've installed can update their records of your basic info, age range, language and country. If you haven't used an app in a while, it won't be able to continue to update the additional information you've given them permission to access. Learn more at: https://www.facebook.com/help/how-apps-work

Sometimes a game console, mobile phone, or other device might ask for permission to share specific information with the games and applications you use on that device. If you say okay, those applications will not be able to access any other information about you without asking specific permission from you or your friends.

Sites and apps that use Instant Personalization receive your User ID and friend list when you visit them.

You always can remove apps you've installed by using your app settings at: https://www.facebook.com/settings/?tab=applications. But remember, apps may still be able to access your information when the people you share with use them. And, if you've removed an application and want them to delete the information you've already shared with them,

you should contact the application and ask them to delete it. Visit the application's page on Facebook or their own website to learn more about the app.

Controlling what is shared when the people you share with use applications

Just like when you share information by email or elsewhere on the web, information you share on Facebook can be re-shared. This means that if you share something on Facebook, anyone who can see it can share it with others, including the games, applications, and websites they use.

Your friends and the other people you share information with often want to share your information with applications to make their experiences on those applications more personalized and social. For example, one of your friends might want to use a music application that allows them to see what their friends are listening to. To get the full benefit of that application, your friend would want to give the application her friend list – which includes your User ID – so the application knows which of her friends is also using it. Your friend might also want to share the music you "like" on Facebook. If you have made that information public, then the application can access it just like anyone else. But if you've shared your likes with just your friends, the application could ask your friend for permission to share them.

You can control most of the information other people can share with applications they use from the "Ads, Apps and Websites" settings page. But these controls do not let you limit access to your public information and friend list.

If you want to completely block applications from getting your information when your friends and others use them, you will need to turn off all Platform applications. This means that you will no longer be able to use any third-party Facebook-integrated games, applications or websites.

If an application asks permission from someone else to access your information, the application will be allowed to use that information only in connection with the person that gave the permission and no one else.

Logging in to another site using Facebook

Facebook Platform lets you log into other applications and websites using your Facebook account. When you log in using Facebook, we give the site your User ID (just like when you connect with any other application), but we do not share your email address or password with that website through this process.

If you already have an account on that website, the site may also be able to connect that account with your Facebook account. Sometimes it does this using what is called an "email hash", which is similar to searching for someone on Facebook using an email address. Only the email addresses in this case are hashed so no email addresses are actually shared between Facebook and the website.

How it works

The website sends over a hashed version of your email address, and we match it with a database of email addresses that we have also hashed. If there is a match, then we tell the website the User ID associated with the email address. This way, when you log into the website using Facebook, the website can link your Facebook account to your account on that website.

About social plugins

Social plugins are buttons, boxes, and stories (such as the Like button) that other websites can use to present Facebook content to you and create more social and personal experiences for you. While you view these buttons, boxes, and stories on other sites, the content comes directly from Facebook.

Sometimes plugins act just like applications. You can spot one of these plugins because it will ask you for permission to access your information or to publish information back to Facebook. For example, if you use a registration plugin on a website, the plugin will ask your permission to share your basic info with the website to make it easier for you to register for the website. Similarly, if you use an Add To Timeline plugin, the plugin will ask your permission to publish stories about your activities on that website to Facebook.

If you make something public using a plugin, such as posting a public comment on a newspaper's website, then that website can access your comment (along with your User ID) just like everyone else.

If you post something using a social plugin and you do not see a sharing icon, you should assume that story is Public. For example, if you post a comment through a Facebook comment plugin on a site, your story is Public and everyone, including the website, can see your story.

Websites that use social plugins can sometimes tell that you have engaged with the social plugin. For example, they may know that you clicked on a Like button in a social plugin.

We receive data when you visit a site with a social plugin. We keep this data for a maximum of 90 days. After that, we remove your name or any other personally identifying information from the data, or combine it with other people's data in a way that it is no longer associated with you. Learn more at: https://www.facebook.com/help/social-plugins

About instant personalization

Instant personalization is a way for Facebook to help partners (such as Bing and Rotten Tomatoes) on and off Facebook create a more personalized and social experience for logged in users than a social plugin can offer. When you visit a site or app using instant personalization, it will know some information about you and your friends the moment you arrive. This is because sites and apps using instant personalization can access your User ID, your friend list, and your public information.

The first time you visit a site or app using instant personalization, you will see a notification letting you know that the site or app has partnered with Facebook to provide a personalized experience.

The notification will give you the ability to disable or turn off instant personalization for that site or app. If you do that, that site or app is required to delete all of the information about you it received from Facebook as part of the instant personalization program. In addition, we will prevent that site from accessing your information in the future, even when your friends use that site.

If you decide that you do not want to experience instant personalization for all partner sites and apps, you can disable instant personalization from the “Ads, Apps and Websites” settings page.

If you turn off instant personalization, partner third party sites and apps will not be able to access your public information, even when your friends visit those sites.

If you turn off an instant personalization site or app after you have been using it or visited it a few times (or after you have given it specific permission to access your data), it will not automatically delete your data received through Facebook. But the site is contractually required to delete your data if you ask it to.

How it works

To join the instant personalization program, a potential partner must enter into an agreement with us designed to protect your privacy. For example, this agreement requires that the partner delete your data if you turn off instant personalization when you first visit the site or app. It also prevents the partner from accessing any information about you until you or your friends visit its site.

Instant personalization partners sometimes use an email hash process to see if any of their users are on Facebook and get those users' User IDs. This process is similar to searching for someone on Facebook using an email address, except in this case the email addresses are hashed so no actual email addresses are exchanged. The partner is also contractually required not to use your User ID for any purpose (other than associating it with your account) until you or your friends visit the site.

When you visit a site or app using instant personalization, we provide the site or app with your User ID and your friend list (as well as your age range, locale, and gender). The site or app can then connect your account with that partner with your friends' accounts to make the site or app instantly social. The site can also access public information associated with any of the User IDs it receives, which it can use to make them instantly personalized. For example, if the site is a

music site, it can access your music interests to suggest songs you may like, and access your friends' music interests to let you know what they are listening to. Of course it can only access your or your friends' music interests if they are public. If the site or app wants any additional information, it will have to get your specific permission.

Public search engines

Your public search setting controls whether people who enter your name on a public search engine may see your public timeline (including in sponsored results). You can find your public search setting on the "Ads, Apps and Websites" settings page.

This setting does not apply to search engines that access your information as an application using Facebook Platform. If you turn your public search setting off and then search for yourself on a public search engine, you may still see a preview of your timeline. This is because some search engines cache information for a period of time. You can learn more about how to request a search engine to remove you from cached information at: https://www.facebook.com/help/?faq=13323

IV. How advertising and Sponsored Stories work

Personalized ads

We do not share any of your information with advertisers (unless, of course, you give us permission). As described in this policy, we may share your information when we have removed from it anything that personally identifies you or combined it with other information so that it no longer personally identifies you.

We use the information we receive to deliver ads and to make them more relevant to you. This includes all of the things you share and do on Facebook, such as the Pages you like or key words from your stories, and the things we infer from your use of Facebook. Learn more at: https://www.facebook.com/help/?page=226611954016283

When an advertiser creates an ad, 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. For example, an advertiser can choose to target 18 to 35 year-old women who live in the United States and like basketball. An advertiser could also choose to target certain topics or keywords, like "music" or even people who like a particular song or artist.

Try this tool yourself to see one of the ways advertisers target ads and what information they see at: https://www.facebook.com/ads/create/

If the advertiser chooses to run the ad (also known as placing the order), we serve the ad to people who meet the criteria the advertiser selected, but we do not tell the advertiser who any of those people are. So, for example, if a person views or otherwise interacts with the ad, the advertiser might infer that the person is an 18-to-35-year-old woman who lives in the U.S. and likes basketball. But we would not tell the advertiser who that person is.

After the ad runs, we provide advertisers with reports on how their ads performed. For example we give advertisers reports telling them how many users saw or clicked on their ads. But these reports are anonymous. We do not tell advertisers who saw or clicked on their ads.

Advertisers sometimes place cookies on your computer in order to make their ads more effective. Learn more about cookies, pixels and other system technologies.
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. For example, if a person "likes" the "Star Trek" Page and mentions "Star Wars" when they check into a movie theater, we may conclude that this person is likely to be a sci-fi fan. Advertisers of sci-fi movies, for example, could ask us to target "sci-fi fans" and we would target that group, which may include you. Or if you "like" Pages that are car-related and mention a particular car brand in a post, we might put you in the "potential car buyer" category and let a car brand target to that group, which would include you.

Ads + social context

Facebook Ads are sometimes paired with social actions your friends have taken. For example, an ad for a sushi restaurant may be paired with a news story that one of your friends likes that restaurant's Facebook page.

This is the same type of news story that could show up in your News Feed, only we place it next to a paid advertisement to make that ad more relevant and interesting.

When you show up in one of these news stories, we will only pair it with ads shown to your friends. If you do not want to appear in stories paired with Facebook Ads, you can opt out using your "Edit social ads" setting.

Learn what happens when you click "Like" on an advertisement or an advertiser's Facebook Page at: https://www.facebook.com/help/?faq=19399
We may serve ads, including those with social context (or serve just social context), on other sites. These work just like the ads we serve on Facebook - the advertisers do not receive any of your information. Only people that could see the Facebook action (like on your timeline) would see it paired in this way.
Your "Show my social actions in Facebook Ads" setting only controls ads with social context. It does not control Sponsored Stories, ads or information about Facebook's services and features, or other Facebook content.
Games, applications and websites can serve ads directly to you or help us serve ads to you or others if they have information like your User ID or email address.

Sponsored stories

Many of the things you do on Facebook (like "liking" a Page) are posted to your timeline and shared in News Feed. But there's a lot to read in News Feed. That's why we allow people to "sponsor" your stories to make sure your friends see them. For example, if you RSVP to an event hosted by a local restaurant, that restaurant may want to make sure your friends see it so they can come too.

If they do sponsor a story, that story will appear in the same place ads usually do or in your News Feed under the heading "Sponsored" or something similar. Only people that could originally see the story can see the sponsored story, and no personal information about you (or your friends) is shared with the sponsor.

Your "Show my social actions in Facebook Ads" setting only controls ads with social context. It does not control Sponsored Stories, ads or information about Facebook's services and features, or other Facebook content.

Facebook content

We like to tell you about some of the features and tools your friends and others use on Facebook, to help you have a better experience. For example, if your friend uses our friend finder tool to find more friends on Facebook, we may tell you about it to encourage you to use it as well. This of course means your friend may similarly see suggestions based on the things you do. But we will try to only show it to friends that could benefit from your experience.

Your "Show my social actions in Facebook Ads" setting only controls ads with social context. It does not control Sponsored Stories, ads or information about Facebook's services and features, or other Facebook content.

V. Cookies, pixels and other similar technologies

Cookies are small pieces of data that are stored on your computer, mobile phone or other device. Pixels are small blocks of code on webpages that do things like allow another server to measure viewing of a webpage and often are used in connection with cookies.

We use technologies like cookies, pixels, and local storage (like on your browser or device, which is similar to a cookie but holds more information) to provide and understand a range of products and services. Learn more at: https://www.facebook.com/help/cookies

We use these technologies to do things like:

- make Facebook easier or faster to use;
- enable features and store information about you (including on your device or in your browser cache) and your use of Facebook;
- deliver, understand and improve advertising;
- monitor and understand the use of our products and services; and
- to protect you, others and Facebook.

For example, we may use them to know you are logged in to Facebook, to help you use social plugins and share buttons, or to know when you are interacting with our advertising or Platform partners.

We may ask advertisers or other partners to serve ads or services to computers, mobile phones or other devices, which may use a cookie, pixel or other similar technology placed by Facebook or the third party (although we would not share any other information that identifies you with an advertiser).

Most companies on the web use cookies (or other similar technological tools), including our advertising and Platform partners. For example, our Platform partners, advertisers or Page administrators may use cookies or similar technologies when you access their apps, ads, Pages or other content.

Cookies and things like local storage help make Facebook work, like allowing pages to load faster because certain content is stored on your browser or by helping us authenticate you to deliver personalized content.
To learn more about how advertisers generally use cookies and the choices advertisers provide, visit the Network Advertising Initiative at http://www.networkadvertising.org/managing/opt_out.asp, the Digital Advertising Alliance at http://www.aboutads.info/, the Internet Advertising Bureau (US) at http://www.iab.net or the Internet Advertising Bureau (EU) at http://youronlinechoices.eu/.
You can remove or block cookies or other similar technologies or block or remove other data stored on your computer or device (such as by using the various settings in your browser), but it may affect your ability to use Facebook or other websites and apps.

VI. Some other things you need to know

Safe harbor

Facebook complies with the EU Safe Harbor framework as set forth by the Department of Commerce regarding the collection, use, and retention of data from the European Union. To view our certification, visit the U.S. Department of Commerce's Safe Harbor website at: https://safeharbor.export.gov/list.aspx. As part of our participation in the Safe Harbor program, we agree to resolve disputes you have with us in connection with our policies and practices through TRUSTe. If you would like to contact TRUSTe, visit:https://feedback-form.truste.com/watchdog/request

Contact us with questions or disputes

If you have questions or complaints regarding our Data Use Policy or practices, please contact us by mail at 1601 Willow Road, Menlo Park, CA 94025 if you reside in the U.S. or Canada, or at Facebook Ireland Ltd., Hanover Reach, 5-7 Hanover Quay, Dublin 2 Ireland if you live outside the U.S. or Canada. Anyone may also contact us through this help page: https://www.facebook.com/help/contact_us.php?id=173545232710000

Responding to legal requests and preventing harm

We may access, preserve and share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so. This may include responding to legal requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards. We may also access, preserve and share information when we have a good faith belief it is necessary to: detect, prevent and address fraud and other illegal activity; to protect ourselves, you and others, including as part of investigations; and to prevent death or imminent bodily harm. Information we receive about you, including financial transaction data related to purchases made with Facebook Credits, may be accessed, processed and retained for an extended period of time when it is the subject of a legal request or obligation, governmental investigation, or investigations concerning possible violations of our terms or policies, or otherwise to prevent harm.

Access requests

You can access and correct most of your personal data stored by Facebook by logging into your account and viewing your timeline and activity log. You can also download a copy of your personal data by visiting your "Account Settings", clicking on "Download a copy of your Facebook data" and then clicking on the link for your expanded archive. Learn more at: https://www.facebook.com/help/?faq=226281544049399

Notifications and Other Messages

We may send you notifications and other messages using the contact information we have for you, like your email address. You can control most of the notifications you receive, including ones from Pages you like and applications you use, using your "Notifications" settings.

Friend finder

We offer tools to help you upload your friends' contact information so that you and others can find friends on Facebook, and invite friends who do not use Facebook to join. If you do not want us to store this information, visit this help page at: https://www.facebook.com/contact_importer/remove_uploads.php

If you give us your password, we will delete it after you upload your friends' contact information.

Invitations

When you invite a friend to join Facebook, we send a message on your behalf using your name, and up to two reminders. We may also include names and pictures of other people your friend might know on Facebook. The invitation will also give your friend the opportunity to opt out of receiving other invitations to join Facebook.

Memorializing accounts

We may memorialize the account of a deceased person. When we memorialize an account, we keep the timeline on Facebook, but limit access and some features. You can report a deceased person's timeline at: https://www.facebook.com/help/contact.php?show_form=deceased

We also may close an account if we receive a formal request that satisfies certain criteria.

Service Providers

We give your information to the people and companies that help us provide, understand and improve the services we offer. For example, we may use outside vendors to help host our website, serve photos and videos, process payments, analyze data, measure the effectiveness of ads, or provide search results. In some cases we provide the service jointly with another company, such as the Facebook Marketplace. In all of these cases our partners must agree to only use your information consistent with the agreement we enter into with them, as well as this Data Use Policy.

Security and bugs

We do our best to keep your information secure, but we need your help. For more detailed information about staying safe on Facebook, visit the Facebook Security Page. We try to keep Facebook up, bug-free and safe, but can't make guarantees about any part of our services or products.

Change of Control

If the ownership of our business changes, we may transfer your information to the new owner so they can continue to operate the service. But they will still have to honor the commitments we have made in this Data Use Policy.

Notice of Changes

If we make changes to this Data Use Policy we will notify you by publication here and on the Facebook Site Governance Page. If the changes are material, we will provide you additional, prominent notice as appropriate under the circumstances. You can make sure that you receive notice directly by liking the Facebook Site Governance Page.

Opportunity to comment and vote

Unless we make a change for legal or administrative reasons, or to correct an inaccurate statement, we will give you seven (7) days to provide us with comments on the change. If we receive more than 7000 comments concerning a particular change, we will put the change up for a vote. The vote will be binding on us if more than 30% of all active

registered users as of the date of the notice vote.

Information for users outside of the United States and Canada

Company Information: The website under www.facebook.com and the services on these pages are being offered to users outside of the U.S. and Canada by Facebook Ireland Ltd., Hanover Reach, 5-7 Hanover Quay, Dublin 2 Ireland. The company Facebook Ireland Ltd. has been established and registered in Ireland as a private limited company, Company Number: 462932, and is the data controller responsible for your personal information.
Directors: Cipora Herman (American), Theodore Ullyot (American).

Your California privacy rights

California law permits residents of California to request certain details about what personal information a company shares with third parties for the third parties' direct marketing purposes. Facebook does not share your information with third parties for the third parties' own and independent direct marketing purposes unless we receive your permission. Learn more about the information we receive and how it is used and other websites and applications. If you have questions about our sharing practices or your rights under California law, please write us at 1601 Willow Road, Menlo Park, CA 94025 or contact us through this help page: https://www.facebook.com/help/contact_us.php?id=173545232710000