Sanford P. Dumain
Peter E. Seidman
Melissa Ryan Clark
Charles Slidders
Anne Marie Vu (SBN 238771)
MILBERG LLP
One Pennsylvania Plaza
New York, NY 10119
Telephone: (212) 594-5300
Facsimile: (212) 868-1229

Michael R. Reese (SBN 206773)
Kim E. Richman
REESE RICHMAN LLP
875 Avenue of the Americas
New York, NY 10001
Telephone: (212) 579-4625
Facsimile: (212) 253-4272

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

RYAN UNG, CHI CHENG, and ALICE ROSEN, on Behalf of Themselves and All Others Similarly Situated, Plaintiffs, v. FACEBOOK, INC., Defendant.	Case No. CV-11-02829 PLAINTIFFS' OPPOSITION TO FACEBOOK INC.'S MOTION TO DISMISS CLASS ACTION COMPLAINT FED. R. CIV. P. 12(b)(1), 12 (b)(6) DATE: TBD TIME: TBD JUDGE: HON. JEREMY FOGEL COURTROOM: 3

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

Plaintiffs Ryan Ung, Chi Cheng, and Alice Rosen ("Plaintiffs") respectfully submit the following in opposition to the motion to dismiss filed by defendant Facebook, Inc. ("Defendant"). Defendant's motion is without merit and should be denied.

STATEMENT OF ISSUES TO BE DECIDED

1) Does the complaint meet the minimal standards of Article III standing?

2) Does the complaint state a cause of action for violation the right to privacy guaranteed by California's constitution?

3) Does the complaint state a cause of action for unjust enrichment?

INTRODUCTION AND STATEMENT OF FACTS

The ubiquitous Facebook Like button is an image, found on millions of websites, that displays a thumbs-up symbol accompanied by the word "Like." When a Facebook member clicks the Like button, an item appears on the member's Facebook profile page with a link back to the website. Thus, by "Liking" a website, the Facebook member recommends the website to his or her Facebook "friends."

Unbeknownst to Internet users, the Like button is also a component of what might aptly be called Facebook's Like button surveillance and personal information collection program ("Like Button Surveillance Program"). Facebook uses the Like button to track Facebook members and non-members alike as they browse the Internet. Facebook then links its records of each new page a user visits into Facebook's record of all the Like button pages that the user has visited in the previous minutes, months, and years. The Like Button Surveillance Program thereby records discrete bits of sensitive personal information derived from users' visits to particular websites and also obtains information sufficient to construct and update a long-term profile based on the users' choice of website destinations over a prolonged period. ***The information is collected even if the website visitor does not click on the Like button, and Internet users have no way of knowing in advance which websites contain Like buttons***. Compl. ¶ 14. Therefore, unless a person forgoes use of the Internet altogether, the Like buttons, and all they entail, are unavoidable. *Id.* at ¶ 12.

Facebook begins to collect information about an Internet user—whether they are a Facebook member or not—as soon as the Internet user creates a Facebook account *or* simply visits a page that contains a Like Button. Facebook's processes for tracking members and non-members, and associating their browsing history with their personal identity and information, are as follows:

(a) Facebook Members: Upon registration, Facebook implants tracking devices (e.g., "cookies") on a member's computer. Each time the member visits a site displaying the Facebook Like button, the updated Facebook tracked information, including the member's most recent browsing history, is sent to Facebook. Facebook can then link the tracked information with the member's actual identity and the personally-sensitive information associated with the particular user's account and/or profile. ***This occurs regardless of whether the Facebook member clicks the Like button.***

If a Facebook member had visited a webpage (or several) with a Like button *before* becoming a Facebook member, all of her browsing history, before she became a Facebook member, would also become associated with her account (and thus actual identity) at the time of registration.

If a Facebook member deactivates her account through the process Facebook provides, the entire account is nevertheless kept by Facebook, which can continue to link browsing data to the Internet user's closed account (and thus actual identity) just as when the account was active. If the member wishes to delete the account entirely, such that Facebook no longer has access to his or her personal data, she must make a specific request to Facebook that takes two weeks to process. *Id.* ¶ 15.

(b) Non-Facebook Members: Facebook implants tracking devices (e.g., cookies) on the computers of non-Facebook members when the non-Facebook members visit one of the million websites in the Facebook Connect network.[1] Thereafter, Facebook's anonymous profile of the non-members is updated each time a non-member visits a site displaying the Facebook

[1] Facebook Connect enables Facebook members to log onto third-party websites, applications, mobile devices, and gaming systems with their Facebook identities. While logged on, users can connect with friends via these media and post information and updates to their Facebook profiles. *Id.* ¶ 13.

"Like" button, ***even if the non-member does not click the "Like" button***. Facebook thus tracks and collects extensive information about individuals who consciously choose not to become Facebook members. Furthermore, if and when a non-member subsequently joins Facebook, Facebook can associate the previously anonymous file with the member and her account information, which includes, at a minimum, the member's name and address. And from that time on, all subsequent requests for Facebook content are associated with the Facebook account and, thus, the Facebook member's identity. *Id.* at ¶ 15.

Defendant's motion to dismiss is based on three arguments, each of which ignores salient facts of this case. First, Defendant argues that Plaintiffs lack Article III standing because they have not alleged injury in fact. Defendant, however, violated Plaintiffs' inalienable right to privacy, as guaranteed by Article I, Section I of the California Constitution. *Id.* ¶¶ 1, 28-33. This is more than sufficient harm to confer Article III standing. Pt. I.

Second, Defendant argues that Plaintiffs have not alleged facts sufficient to establish a violation of the California constitutional right to privacy. This argument, however, cannot avoid the fact that courts have held that far less egregious surveillance programs are unconstitutional. Pt. II.

Finally, Defendant argues that Plaintiffs' unjust enrichment claim should be dismissed because California courts do not recognize unjust enrichment as an independent cause of action. Defendant, however, acknowledges, as have courts in this District, that litigants may seek restitution using an unjust enrichment claim. Defendant then argues that, even if a restitution claim were acknowledged, Plaintiffs have not alleged that they have suffered any detriment to a property right as a result of Defendant's unjust conduct. The cited precedent does not apply to the circumstances of this case and, moreover, Plaintiffs have clearly alleged that Defendant's conduct has caused Plaintiffs to lose money through the sale of Plaintiffs' personal information to third parties without Plaintiffs' knowledge. Pt. III.

In short, Plaintiffs have adequately pleaded that Facebook has stripped them of their constitutional right to control the personal information they reveal about themselves and to whom they reveal it and that Facebook unjustly obtains and divulges personal and embarrassing

information to data aggregators for its own enrichment. Accordingly, Defendant's motion to dismiss must be denied.

ARGUMENT

I. PLAINTIFFS HAVE ESTABLISHED ARTICLE III STANDING

Article III standing limits the subject matter jurisdiction of a federal court to cases or controversies that are "justiciable"—i.e., capable of being appropriately decided by resolution of the particular case or controversy before the court.[2] Defendant argues that Plaintiffs lack standing in this case because Plaintiffs have not alleged harm that constitutes injury in fact, Def. Mem. 8, but Plaintiffs have in fact alleged such harm.

To satisfy the standing requirements of Article III, a plaintiff must show that he has suffered an "injury in fact" that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical. *Gest v. Bradbury*, 443 F.3d 1177, 1181 (9th Cir. 2006). "The injury required by Article III can exist solely by virtue of 'statutes creating legal rights, the invasion of which creates standing.'" *Fulfillment Servs. Inc. v. UPS, Inc.*, 528 F.3d 614, 618-19 (9th Cir. 2008); *Edwards v. First Am. Corp.*, 610 F.3d 514, 517 (9th Cir. 2010). In such cases, the "'standing question . . . is whether the constitutional or statutory provision on which the claim rests properly can be understood as granting persons in the plaintiff's position a right to judicial relief.'" *Edwards*, 610 F.3d at 517 (citation omitted); *see also In re Facebook Privacy Litig.*, No. 10-02389, --- F. Supp. 2d ---- , 2011 WL 2039995, at *4 (N.D. Cal. May 12, 2011) (Ware, J.) (holding that the plaintiffs had standing).

"Injury-in-fact is not Mount Everest." *Danvers Motor Co. v. Ford Motor Co.*, 432 F.3d 286, 294 (3d Cir. 2005). To the contrary, it suffices for federal standing purposes to allege some specific, "'identifiable trifle'" of injury. *Council of Ins. Agents & Brokers v. Molasky-Arman*, 522 F.3d 925, 932 (9th Cir. 2008) (quoting *United States v. Students Challenging Regulatory Agency Procedures (SCRAP)*, 412 U.S. 669, 689 n.14 (1973)). The U.S. Supreme Court has allowed important interests to be vindicated by plaintiffs with "no more at stake in the outcome

[2] *See* 13A Charles Alan Wright, Arthur R. Miller, *et al.*, *Federal Practice and Procedure* § 3531.4 (3d ed. 2011).

of an action than a fraction of a vote, a $5 fine and costs, and a $1.50 poll tax." *Id.* (internal quotations omitted). "'The basic idea that comes out in numerous cases is that ***an identifiable trifle is enough to fight out a question of principle***; the trifle is the basis for standing and the principle provides the motivation.'" *Id.* (emphasis added) (quoting *SCRAP*, 412 U.S. at 689 n.14). Here, where constitutionally-protected rights to privacy have been violated, Plaintiffs' alleged injuries are certainly more than a "trifle." Compl. ¶¶ 1, 28-33.

Because Plaintiffs can establish standing based on the alleged infringement of their privacy rights under the California Constitution, Defendant's arguments regarding economic loss are irrelevant. *See* Def. Mem. 10-11. Likewise, Defendant erroneously relies on precedent addressing economic loss and personally-identifiable information. *See id.* (citing *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 525 (S.D.N.Y. 2001); *LaCourt v. Specific Media, Inc.*, No. 10-1256, 2011 WL 1661532, at *3-5 (C.D. Cal. Apr. 28, 2011)). As the court in *Specific Media* specifically stated, the discussion in the *DoubleClick* case regarding economic loss was "not in the context of evaluating Article III standing." *Specific Media*, 2011 WL 1661532, at *5.[3] Furthermore, the *Specific Media* decision clearly rested on a deficiency of *facts* in the complaint indicating that any named plaintiff was affected by the defendant's alleged conduct. *See Specific Media*, 2011 WL 1661532, at *4.[4] In contrast, the named Plaintiffs here have alleged sufficient facts to indicate they were affected by the defendant's alleged conduct, as they have each alleged an invasion of a constitutional right to privacy. Compl. ¶¶ 1, 28-33.

The recent Ninth Circuit case of *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), is on point here. In *Krottner*, the plaintiffs alleged that defendant Starbucks had violated

---

[3] Moreover, the portion of the decision in *DoubleClick* that Defendant cites discusses a claim by plaintiffs under the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 *et seq.*, which imposes a $5,000 threshold. *See DoubleClick*, 154 F. Supp. 2d at 523-26 (finding that the plaintiffs had failed to allege facts that could support the inference that the damages and losses they incurred from the defendant's access to the plaintiffs' computers could meet § 1030(e)(8)(A)'s damage threshold). Here, Plaintiffs are not relying on the CFAA.

[4] While noting the inadequacy of the plaintiffs' complaint, the *Specific Media* court *did* recognize the viability in the abstract of such concepts as "opportunity costs," "value-for-value exchanges," "consumer choice," and other concepts referred to in the plaintiffs' opposition brief, and, therefore, the court allowed the plaintiffs to amend their complaint to allege facts related to such theories. 2011 WL 2473399, at *4; *see also id.* at *6.

their privacy when the defendant failed to encrypt personal information regarding the plaintiffs on a company laptop that was stolen from a Starbucks store. *Id.* at 1140. The defendant moved to dismiss, arguing that the plaintiffs did not have Article III standing. The Ninth Circuit rejected this argument, stating: "we hold that Plaintiffs-Appellants, whose personal information has been stolen but not misused, have suffered an injury sufficient to confer standing under Article III, Section 2 of the U.S. Constitution." *Id.*; *see also Pisciotta v. Old Nat'l Bancorp,* 499 F.3d 629, 634 (7th Cir. 2007) (reasoning that person who had his private information taken without plaintiff's permission, but not misused, had standing under Article III). Hence, under the governing authority of *Krottner*, Plaintiffs clearly have Article III standing.

II. FACEBOOK VIOLATED THE RIGHT TO PRIVACY ARISING FROM CALIFORNIA'S STATE CONSTITUTION

Try as it might, Facebook cannot get around the fact that its Like Button Surveillance Program involves precisely the type of conduct proscribed by Article 1, Section 1 of the California Constitution.

Article 1, Section 1 was amended on November 7, 1972, following a ballot initiative to create an express right to privacy. The "Privacy Initiative"—i.e., the privacy amendment—"is to be interpreted and applied in a manner consistent with the probable intent of the body enacting it: the voters of the State of California." *Hill v. NCAA*, 7 Cal. 4th 1, 16 (1994). The intent of the voters is clear:

> The principal focus of the Privacy Initiative is readily discernable. The Ballot Argument warns of unnecessary information gathering, use, and dissemination by public and private entities -- images of "government snooping," computer stored and generated "dossiers" and "'cradle-to-grave' profiles on every American" dominate the framers' appeal to the voters.... The evil addressed is ... business conduct in "collecting and stockpiling unnecessary information ... and misusing information ..."

Id. at 21 (quoting Ballot Pamp., Proposed Stats. and Amends. to Cal. Const. with arguments to voters, Gen. Elec. (Nov. 7, 1972), at 26, 27).

This is exactly what Facebook's Like Button Surveillance Program does—it uses the ubiquitous Like button to "collect and store sensitive, private, and personally identifiable

information," Compl. ¶ 1, and "to track Internet users as they browse the web and thereby collect[] private and, in some cases, sensitive information about them," *id.* ¶ 14.

California courts have held that a plaintiff must satisfy three elements to establish a violation of the Privacy Initiative: "(1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy." *Ruiz v. Gap, Inc.*, 380 F. App'x 689, 692 (9th Cir. 2010) (quoting *Hill*, 7 Cal. 4th at 26). As set forth herein, Plaintiffs satisfy each of these elements.[5]

A. Plaintiffs Have a Legally Protected Privacy Interest in Their Personal Browsing History

1. Plaintiffs Have a Legally Protected Interest in the Whole of Their Browsing History

Defendant asserts that Plaintiffs failed to allege a legally protected privacy interest because "the Complaint does not allege that Facebook has either collected - or disclosed - *any* such highly personal information from any of the Plaintiffs or that any of the Plaintiffs even have such interests to protect." Def. Mem. 12 (emphasis in original). However, Plaintiffs have a legally protected privacy interest in their browsing history regardless of whether they visited any single web site from which sensitive information about them could be inferred.

The Supreme Court addressed this situation—in which the whole of the information obtained is something different from the sum of its parts—in *United States Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989).[6] In upholding the FBI's

---

[5] "Legally recognized privacy interests are generally of two classes: (1) interests in precluding the dissemination or misuse of sensitive and confidential information ('informational privacy'); and (2) interests in making intimate personal decisions or conducting personal activities without observation, intrusion or interference ('autonomy privacy')." *Hill*, 7 Cal. 4th at 35. "Informational privacy is the core value furthered by the Privacy Initiative." *Id.* (citing *White v. Davis*, 13 Cal. 3d 757, 774 (1975)); *see also Pettus v. Cole*, 49 Cal. App. 4th 402, 440-41 (1996) (w*ith regard to the protection afforded by the Privacy Initiative*, "[t]he right to control circulation of personal information is fundamental." (internal citations omitted)). Facebook has also compromised Plaintiffs' privacy interests in "autonomy privacy" because tracking a person's use of the Internet to browse websites—often from the privacy of the person's home and, in almost all cases, outside of public view—is a form of "observation, intrusion or interference" in her decisions regarding which websites to visit.

[6] *See United States v. Maynard,* 615 F.3d 544, 561 n.*[4] (D.C. Cir. 2010), *cert. granted, U.S. v. Jones*, No. 10-1259, 2011 WL 1456728 (June 27, 2011) ("The colloquialism that 'the whole is greater than the sum of its parts' is not quite correct. 'It is more correct to say that the whole is something different than the sum of its parts.' Kurt Koffa, Principles of Gestalt Psychology 176

invocation of the privacy exception of the Freedom of Information Act, the Court explained that the appellant had a privacy interest in the whole of his rap sheet even though the individual events in the summary were matters of public record. *Id.* at 764. The court in *Maynard* also recognized a distinct privacy interest in the whole of collected information. 615 F.3d at 568 (holding that the prolonged GPS tracking of an individual without a warrant defeated his expectation of privacy and violated the Fourth Amendment). The court noted that "[w]hen it comes to privacy, . . . precedent suggests that the whole may be more revealing than the parts." *Id.* at 561. The court explained its rationale as follows:

> . . . Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. ***Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month.*** The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.

Id. at 562 (emphasis added; footnote omitted). *See also In re Historical Cell-Site Info.*, No. 10-MC-897, 2011 WL 3678934, at *5 (E.D.N.Y. Aug. 22, 2011); *People v. Weaver*, 12 N.Y.3d 433, 442 (2009) (prolonged monitoring "yields . . . a highly detailed profile, not simply of where we go, but by easy inference, of our associations -- political, religious, amicable and amorous, to name only a few -- and of the pattern of our professional and avocational pursuits."); *State v. Jackson*, 150 Wash. 2d 251, 262 (2003) (en banc) ("In this age, vehicles are used to take people to a vast number of places that can reveal preferences, alignments, associations, personal ails and

---

(1935). That is what the Court was saying in *Reporters Committee* and what we mean to convey throughout this opinion.").

foibles. The GPS tracking devices record all of these travels, and thus can provide a detailed picture of one's life.").[7]

This case is no different. In this age, the Internet takes people to a vast number of web sites just as vehicles take them to a vast number of physical locations, and the Internet destinations they choose are at least as revealing and in the same way.[8] Thus, "[r]epeated visits to a church [website], a gym [website], a bar [website], or [an online] bookie tell a story not told by any single visit, as does one's not visiting any of these [websites] over the course of a month", and "[a] person who knows all of another's [web browsing history] can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts." *Maynard,* 615 F.3d at 562. Likewise here, it is the aggregation of information, the profile or dossier of an individual, created from that person's web browsing history, in which there is a legally protected interest. Moreover, this is precisely the type of "stockpiling" of information to create a personal "profile" or "dossier" that the Privacy Initiative was specifically intended to prevent.[9]

---

[7] *Cf* Cal. Penal Code § 637.7, Stats. 1998, c. 449 (S.B. 1667), §§ 1-2 (making it unlawful for anyone but a law enforcement agency to "use an electronic tracking device to determine the location or movement of a person" and specifically declaring that "electronic tracking of a person's location without that person's knowledge violates that person's reasonable expectation of privacy.").

[8] If anything, surveillance of Internet "travel" is much more revealing than vehicle travel; Internet travel is much speedier than vehicular travel and, therefore, surveillance of Internet travel allows for the collection of much larger data sets in a much shorter time period.

[9] Defendant might try to argue that the Ninth Circuit rejected this approach in *United States v. Pineda–Moreno*, 591 F.3d 1212 (9th Cir. 2010). But *Pineda-Moreno* is distinguishable in several important aspects. First, the travel that police tracked occurred "on public thoroughfares" and the GPS tracking data "could have [been] obtained by following the car." The court held that, for this reason, a person "has no reasonable expectation of privacy in his movements from one place to another." 591 F.3d at 1216. In contrast, Internet transmissions are not over public thoroughfares (but rather invisible or through cables buried deep underground), and a person's Internet browsing is not open to public view. Moreover, Internet browsing often occurs on computers that are password protected for the very purpose of keeping Internet search histories secret. Second, the state had a substantial countervailing interest in the information collected—it was to be used to obtain a felony conviction on drug charges. In contrast, there is no such state interest (if any legitimate interest whatsoever) in Facebook's Like Button Surveillance Program Finally, the appellant in *Pineda-Moreno* did not squarely raise the issue of, and the Court did not perceive, a distinction between the privacy interest compromised by short-term surveillance on the one hand and long-term surveillance on the other. Consequently, it did not address the issue,

2. Plaintiffs Adequately Alleged That Facebook Collected Sensitive Information from Them as a Result of Their Visits to Specific Websites

In any event, Plaintiffs adequately alleged having visited sites of a sensitive nature. The Complaint alleges that Facebook tracks sensitive and personal information about, for example, "[a]nyone who has used the Internet to seek advice about hemorrhoids, sexually transmitted diseases, abortion, drug rehabilitation, dementia." Compl. ¶ 14. The full extent of personally sensitive web pages that contain Like buttons is a fact question to be ascertained through discovery (indeed, the Facebook Like button is pervasive, and Facebook exercises no control over, and has no approval process for, the websites that contain Like buttons), but by way of example, the websites for Jews for Jesus, the Tea Party, the John Birch Society, RevLeft - the Home of the Revolutionary Left, Americans for Tax Reform, NORML (a drug law reform group), Students for a Sensible Drug Policy, the Human Rights Commission's website promoting gay rights, and Glenn Beck's home page are among the millions of websites that feature the Facebook Like button. A visit to any of these websites will reveal, at the very least, Plaintiffs' interest in potentially highly sensitive material. While Plaintiffs have indeed visited websites regarding medical concerns, politics, and other sensitive topics, the specific websites were not enumerated in the complaint for the same reason that it was a violation of California's constitutional protections when Facebook tracked Plaintiffs' visits to those sites: Plaintiffs have a legally protected privacy interest in that browsing history.[10]

3. Plaintiffs Reasonably Expected That Their Internet Searches Would Remain Private

An Internet user does not expect Facebook to monitor and retain a record of his Internet travel any more than he expects "anyone to monitor and retain a record of every time he drives his car, including his origin, route, destination, and each place he stops and how longs he stays

---

present here, of whether appellant had a privacy interest that precluded prolonged as opposed to short-term surveillance.

[10] Plaintiffs were required to plead their allegations in accordance with Fed. R. Civ. P. 8, which requires only "a short and plain statement of the claim" to put Defendant on notice of the claims against it; Plaintiffs have done so. If Defendant's contentions were accepted as true, *see* Def. Mem. at 8, Plaintiffs would be held to a much higher, inapplicable pleading standard, that would require them to compromise the privacy rights they have asserted.

there," *Maynard*, 615 F.3d at 563—and contrary to Facebook's assertion, Def. Mem. 13, Facebook's privacy policy provides no notice that this is what is going on. Instead, it simply states that Facebook uses cookies "to make Facebook easier to use, to make our advertising better, and to protect both you and Facebook" and "to know when you are interacting with Facebook platform applications and websites, our widgets and Share buttons, and our advertisements." *Id.*

Even if Facebook provided real or even constructive notice generally (which it does not), such notice was wholly ineffective and meaningless with respect to any given website. The millions of sites that host Like buttons all record a user's visit the moment she "arrives" at the website, ***regardless of whether the user clicks on the Like button***. Compl. ¶ 14. There is no way Plaintiffs could have known in advance that the website they were about to visit had a Like button tracking device, and that their visit to that site would be recorded and associated with them and their other website visits.[11] Plaintiffs' only alternative to disclosing private information to Facebook, therefore, would be to avoid using the Internet altogether—a high price to pay in an age in which many people consider the Internet a utility that is no less necessary than electric or phone service, and a price that Facebook has no right to impose.[12]

Defendant argues with regard to the subclass of non-Facebook members, whom Facebook cannot immediately identify, that "[a] person cannot be said to have a reasonable expectation of privacy in anonymous data about the pages he or she has visited on the Internet, particularly because data on the Internet is routinely routed through the multiple third-party

---

[11] For this reason, among others, Defendant's reliance on *Hill* and *Holmes v. Petrovich Development Co.*, 191 Cal. App. 4th 1047, 1068 (2011), are inapt; in both of those cases, plaintiff had ample notice that the matter at issue was public. *Hill*, 7 Cal. 4th at 35-36; *Holmes*, 191 Cal. App. 4th at 1068-72.

[12] Defendant's reliance on *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2008), and *People v. Stipo*, 195 Cal. App. 4th 664 (2011), Def. Mem. 14 n.6, to establish that users of the Internet do not have a reasonable expectation of privacy for similar Internet activity, is misplaced because the Internet activity in both cases was not at all similar. In *Forrester*, the issue was disclosure of email addresses, and in *Stipo*, disclosure of subscriber information. Neither case involved browsing history, and, indeed, *Forrester* recognized that a plaintiff has a reasonable expectation to privacy in the content of web searches. 512 F.3d at 510 n.6 (distinguishing between disclosure of the IP address of the Internet user, on the one hand, and URLs that reveal, *e.g.*, the particular newspaper articles a person viewed, on the other hand).

servers as anonymous data packets." Def. Mem. 14. But it cannot deny that an anonymous user's identity, and dossier of associated information, will be correlated with the user's actual identity, without notice, if she joins Facebook at a later date. The Complaint plainly alleges that, at the time a non-member joins Facebook, "Facebook can associate the previously anonymous 'file' with the member and his or her account information, which includes, at a minimum, the members' names and addresses." Compl. ¶ 15(c). Non-members have a reasonable expectation that their search history is, and *will remain*, anonymous.

B. Plaintiffs Allege Conduct by Defendant that Constitutes a Serious Invasion of Privacy

Defendant tries to trivialize the effects of Facebook's invasion of privacy by suggesting that it is nothing more than "routine commercial behavior" to secretly track Plaintiffs' "website browsing history" and stockpile information about the Plaintiffs. Def. Mem. 14. But Facebook's surveillance *via* the Like button—regardless of whether it is clicked or the Internet user is a Facebook member—is a new technology the impact of which is untested. Therefore, the alleged misconduct cannot be "routine commercial behavior" and will only become so if courts allow it to continue.[13] And courts cannot permit such conduct because it is the very type of "serious" invasion of privacy that the Privacy Initiative was intended to prevent. Pt. II(A)(1), *supra.* The purpose and intent of privacy legislation make clear the seriousness of Facebook's misconduct. For instance, the voters of California intended that the right to privacy protect "our freedom to associate with the people we choose." Official Ballot Pamphlet at 28. The Supreme Court has also "recognized the vital relationship between freedom to associate and privacy in one's associations." *NAACP v. Alabama,* 357 U.S. 449, 462 (1958) ("Inviolability of privacy in group

[13] It clearly is not routine commercial behavior in Germany. Indeed, Thilo Weichert, head of the office for data protection in the German state of Schleswig-Holstein, condemned the Facebook Like button, stating that it violates German and European privacy laws and called "on all institutions in the federal state of Schleswig-Holstein, Germany to shut down their fan pages on Facebook and remove social plug-ins such as the 'like' button from their websites." Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein [The Data Protection Commissioner's Office (Independent Centre for Privacy Protection - ULD)], Press Release, *ULD to website owners*: *"Deactivate Facebook web analytics"* (Aug. 19, 2011), https://www.datenschutzzentrum.de/presse/20110819-facebook-en.htm. *See also* Jeff Jarvis, Buzz Machine, *Disliking "Like" in Germany* (Aug. 19, 2011), http://www.buzzmachine.com/2011/08/19/disliking-like-in-germany/.

association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." *Id.*). Here, Facebook is stockpiling information connected to a web browsing history that discloses information about the users' associations, including membership in, or an interest in, dissident groups—when Plaintiffs and Class members have made no choice to reveal their associations to Facebook, and, in the case of non-members, have made no choice to associate with Facebook itself.

III. PLAINTIFFS HAVE ALLEGED A CLAIM FOR UNJUST ENRICHMENT

Defendant asserts that Plaintiffs' unjust enrichment claim should be dismissed because "there is no such independent cause of action in California." Def. Mem. 15. "[C]ourts have held that unjust enrichment is equivalent to restitution and have allowed litigants to seek restitution using an unjust enrichment claim." *SOAProjects, Inc. v. SCM Microsystems, Inc.*, No. 10-1773, 2010 WL 5069832, at *9 (N.D. Cal. Dec. 7, 2010) (Koh, J.) (internal citations omitted); *see also Matracia v. JP Morgan Chase Bank, NA*, No. 11-190, 2011 WL 3319721, at *4 (E.D. Cal. Aug. 1, 2011) ("A party is required to make restitution if he or she is unjustly enriched at the expense of another. A person is enriched if the person receives a benefit at another's expense." (quotations and citations omitted)). "Given the appropriate facts . . . , a plaintiff advances a basis for obtaining restitution if he or she demonstrates defendant's receipt and unjust retention of a benefit." *Monet v. Chase Home Fin., LLC*, No. 10-0135, 2010 WL 2486376, at *3 (N.D. Cal. June 16, 2010).

In *Monet*, the court discussed three traditional factual scenarios where a theory of unjust enrichment has historically supported a restitution remedy in California: (1) when the parties have a contract that was procured by fraud or is for some reason unenforceable, giving rise to an unjust enrichment claim as an alternative to breach of contract damages; (2) when the plaintiff cannot assert title or right to possession of particular property but nevertheless can show just grounds for recovering money to pay for some benefit the defendant received from him, thus implying a contract at law or a quasi-contract and giving rise to a right to restitution at law through an action derived from the common-law writ of assumpsit; and (3) when money or property identified as belonging in good conscience to the plaintiff could clearly be traced to

particular funds or property in the defendant's possession, giving rise to restitution in equity, ordinarily in the form of a constructive trust or an equitable lien. *Id.* Plaintiffs' allegations most clearly relate to the third scenario. Specifically, Plaintiffs' personal information that Defendant collected and stored, Compl. ¶ 35, is property that belongs to Plaintiffs. *See infra.* In addition, the money allegedly obtained by Defendant from sales of that information to third parties, Compl. ¶ 35, is clearly money that can be traced to that property.

Defendant argues that Plaintiffs have not suffered any detriment to Facebook's benefit because "Plaintiffs [do not] have property rights in their personal information that would be harmed had Facebook collected that information." Def. Mem. 16. This argument is unpersuasive. Plaintiffs have alleged that Defendant has done more than merely collect personal information; Plaintiffs have alleged that Defendant *sold* that information to third parties without Plaintiffs' knowledge. Compl. ¶ 35.[14]

Moreover, the cited precedent is not as supportive as it may seem. The *Facebook Privacy* opinion Defendant relies upon in turn relied on *Thompson v. Home Depot, Inc.*, No. 07-1058, 2007 WL 2746603 (S.D. Cal. Sept. 18, 2007). In *Thompson*, the plaintiff alleged he was required to fill out a form that prompted him to provide personal identification, but he did not allege that "filling out the form caused him to lose any money or property." *Id.* at *3. Similarly, the plaintiffs in the *Facebook Privacy* case did not allege that they lost money as a result of the defendant's conduct. 2011 WL 2039995, at *6. Here, Plaintiffs *have alleged* that Defendant's conduct caused Plaintiffs to lose money. Compl. ¶ 35 ("Facebook has received and retained money *belonging to Plaintiffs and the Class*." (emphasis added)). Additionally, the dismissals of the plaintiffs' unjust enrichment claims in the *Facebook Privacy* case and the *Thompson* case rested on the failure of the plaintiffs to provide *any* support for the contention that personal information constitutes valuable property. *See Thompson*, 2007 WL 2746603, at *3;[15] *Facebook*

---

[14] In its later argument that "Plaintiffs also fail to plead that Facebook's alleged collection of their browsing histories was unjust," Defendant makes the same error of omitting Plaintiff's allegations of selling Plaintiffs' information. Def. Mem. 16.

[15] The *Thompson* court, in turn, cited *In re Jetblue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299, 327 (E.D.N.Y. 2005) ("There is . . . ***no support*** for the proposition that an individual

Privacy Litig., 2011 WL 2039995, at *10 n.10. In contrast, Plaintiffs in this case have provided several sources of scholarly and governmental research discussing the economic value of Plaintiffs' personal information. *See* Compl. ¶¶ 16-18. As a result, Plaintiffs have sufficiently alleged that their personal information is a valuable commodity that was sold by Defendant to the financial detriment of Plaintiffs.

Last, Defendant is incorrect that Plaintiffs have not pleaded that Defendant's conduct was unjust. Def. Mem. 16-17. It is patently unjust to use very private and sensitive information of consumers to make profits without the consumers' knowledge that this private information is being disseminated to complete strangers, and Plaintiffs have adequately pleaded this. *See, e.g.*, Compl. ¶¶ 1, 14, 32, 35. [16]

DATED: September 1, 2011

Respectfully Submitted,

MILBERG LLP
/s/ Anne Marie Vu

Sanford P. Dumain
Peter E. Seidman
Melissa Ryan Clark
Charles Slidders
MILBERG LLP
One Pennsylvania Plaza
New York, NY 10119
Telephone: (212) 594-5300
Facsimile: (212) 868-1229

Michael R. Reese
Kim Richman
REESE RICHMAN LLP
875 Avenue of the Americas
New York, NY 10001
Telephone: (212) 579-4625
Facsimile: (212) 253-4272

Attorneys for Plaintiffs

passenger's personal information has or had any compensable value in the economy at large." (emphasis added)).

[16] Should this Court dismiss any give[n] part of Plaintiffs' case, Plaintiffs respectfully request leave to amend, which should be "freely give[n]" pursuant to Fed. R. Civ. P. 15.