Will Lemkul, Esq. (CA State Bar No. 219061)
Shawn D. Morris, Esq. (CA State Bar No. 134855)
MORRIS SULLIVAN & LEMKUL LLP
9915 Mira Mesa Boulevard, Suite 300
San Diego, CA 92131
Telephone: (858) 566-7600
Facsimile: (858) 566-6602
Email: lemkul@morrissullivanlaw.com

Jodi Westbrook Flowers, *pro hac vice forthcoming*
Ann Ritter, *pro hac vice forthcoming*
Fred Baker, *pro hac vice forthcoming*
Kimberly Barone Baden (207731)
Andrew Arnold, *pro hac vice forthcoming*
Annie Kouba, *pro hac vice forthcoming*
MOTLEY RICE LLC
28 Bridgeside Boulevard
Mount Pleasant, SC 29464
Telephone: (843) 216-9000
Facsimile: (843) 216-9450
Email: kbaden@motleyrice.com

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

Taylor Picha, individually and on behalf of all others similarly situated;

Plaintiffs,

v.

Facebook, Inc., and Cambridge Analytica,

Defendants.

Case No.:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

TABLE OF CONTENTS

I. INTRODUCTION

1. In a keynote speech in San Francisco in 2014, Mark Zuckerberg, CEO of Facebook, vowed, "In every single thing we do, we always put people first;" promising that Facebook would give people control over how they share their information.[1] Zuckerberg continued:

> "And in the past, when one of your friend blogged into an app [sic]... the app could ask him not only to share his data but also data that his friends had shared with him – like photos and friend list here. So now we're going to change this and we're going to make it so that now everyone has to choose to share their own data with an app themselves. So we think that this is a really important step for giving people power and control over how they share their data with the apps. And as developers, this is going to allow you to keep building apps with all the same great social features while also giving people power and control first."[2]

2. Just four years later, on March 21, 2018, Zuckerberg addressed fresh reports of the misappropriation of personal data of 50 million Facebook users by an app made by Global Science Research Ltd. and Cambridge Analytica, admitting: "This was clearly a mistake. We have a basic responsibility to protect people's data, and if we can't do that then we don't deserve to have the opportunity to serve people."[3] Then, on April 4, 2018, Facebook publicly stated that up to ***87 million users*** may have been improperly shared with Cambridge Analytica.[4] He added that he regrets the company waited so long to inform its users of what happened: "I think we got that wrong."[5]

3. This class action lawsuit is about the "wrong" Zuckerberg has admitted.

4. On March 17, 2018 *The Guardian* and *The New York Times* revealed that data

---

[1] https://singjupost.com/facebooks-ceo-mark-zuckerberg-f8-2014-keynote-full-transcript/3/?print=print.
[2] *Id.*
[3] http://money.cnn.com/2018/03/21/technology/mark-zuckerberg-apology/index.html; http://money.cnn.com/2018/03/21/technology/mark-zuckerberg-cnn-interview-transcript/index.html?iid=EL.
[4] https://www.reuters.com/article/us-facebook-privacy/facebook-says-data-leak-hits-87-million-users-widening-privacy-scandal-idUSKCN1HB2CM.
[5] *Id.*

analytics firm, Cambridge Analytica, harvested private information from Facebook users "on an unprecedented scale."[6] Facebook's "platform policy" at the time allowed for the accumulation of Facebook users' "friends'" data for the purpose of improved user experience, but prohibited it from being sold or used for advertising.[7]

5. Although Facebook knew about the misuse of 87 million users' data in 2015, it chose to hide this information from its users until forced to confront the issue on March 17, 2018.[8]

6. Just one month earlier, in February 2018, both Facebook and the CEO of Cambridge Analytica, Alezander Nix, told a U.K. parliamentary inquiry on fake news that the company did not have or use private Facebook data. When asked if Cambridge Analytica had Facebook user data, Simon Milner, Facebook's U.K. policy director, told U.K. officials: "They may have lots of data but it will not be Facebook user data. It may be data about people who are on Facebook that they have gathered themselves, but it is not data that we have provided."[9] Cambridge Analytica's Nix told officials: "We do not work with Facebook data and we do not have Facebook data."[10]

7. In direct contradiction to the actual events stemming from Cambridge Analytica's improper use of Facebook user data, Facebook's applicable Data Use Policy at the time of the activity stated: "Facebook does not share your information with third parties for the third parties' own and independent direct marketing purposes unless we receive your permission."[11] Facebook's current Data Use Policy states: "We do not share information that personally identifies you (personally identifiable information is information like name or email address

---

[6] https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[7] *Id.*

[8] https://www.wsj.com/articles/facebook-scandal-what-to-know-about-cambridge-analytica-and-your-data-1521806400.

[9] https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[10] *Id.*

[11] http://web.archive.org/web/20140103201918/https://www.facebook.com/full_data_use_policy.

that can by itself be used to contact you or identifies who you are) with advertising, measurement or analytics partners unless you give us permission."[12]

8. Plaintiff and potential class representative Taylor Picha, individually and on behalf of all others similarly situated ("Plaintiffs"), by and through the undersigned counsel, alleges the following upon personal knowledge as to her own acts and upon information and belief as to all other matters.

9. Plaintiff brings this class action against defendants Facebook, Inc. (or "Facebook") and Cambridge Analytica (or "CA") (collectively "Defendants") on behalf of all persons who registered for Facebook accounts and whose Personally Identifiable Information was obtained from Facebook by CA or other entities without authorization.

10. Cambridge Analytica is a privately held company that combines data mining and data analysis with strategic communication for use in marketing and other strategies.

11. Facebook is a social networking website. Facebook is in the business of helping people communicate with their family, friends, and coworkers online. Facebook develops technologies that facilitate the sharing of information, photographs, website links, and videos. Facebook users have the ability to share and restrict information based on their own specific criteria. By the end of 2017, Facebook had more than 2.2 billion active users.

12. Facebook's mission is "to give people the power to build community and bring the world closer together. People use Facebook to stay connected with friends and family, to discover what's going on in the world, and to share and express what matters to them."[13]

13. Facebook users "create" profiles containing personal information, including their name, birthdate, hometown, address, location, interests, relationships, email address, photos, and videos, amongst other information, referred to herein as Personally Identifiable Information (or "PII").

14. Facebook captures every IP address a user uses when logging into an account, every friend or connection made with an account (even if deleted), and all user activity (such as

[12] https://www.facebook.com/full_data_use_policy.
[13] https://newsroom.fb.com/company-info/.

any posts, tags in photos, "likes," status changes, and connections with other Facebook account owners).

15. This case involves the absolute disregard with which Facebook has treated Plaintiff's PII. While this information was supposed to be protected, and used for only expressly disclosed and limited purposes, CA and GSR, without authorization, or by exceeding whatever limited authorization it, or its agents, had, improperly collected the PII of nearly 87 million Facebook users.[14]

16. Facebook knew improper data aggregation was occurring and failed to stop it. Plaintiff brings this suit to protect her privacy interests and those of the class.

II. THE PARTIES

17. Plaintiff Taylor Picha (or "Plaintiff") is a resident of Charleston County, South Carolina. Plaintiff has held a Facebook account since 2007. Plaintiff is an active Facebook user and has been at all relevant times. Plaintiff recalls that during the 2016 Presidential election, she frequently saw political advertising for the Trump campaign while using Facebook.

18. Defendant Facebook is incorporated in Delaware, and the company's principal place of business is in Menlo Park, California. Facebook's securities trade on the NASDAQ under the ticker symbol "FB."

19. Defendant Cambridge Analytica is a privately held company that combines data mining and data analysis with strategic communication for the electoral process.

20. Whenever this complaint refers to any act of Defendants, the reference shall mean (1) the acts of the directors, officers, employees, affiliates, or agents of Defendants who authorized such acts while actively engaged in the management, direction, or control of the affairs of Defendants, or at the direction of Defendants, and/or (2) any persons who are the parents or alter egos of Defendants, while acting within the scope of their agency, affiliation, or employment.

[14] https://www.forbes.com/sites/parmyolson/2018/03/20/face-to-face-with-cambridge-analytica-alexander-nix-facebook-trump/#674008da535f.

21. A contract between Cambridge Analytica and GSR describes the objective of the data harvesting as follows: "The ultimate product of the training set is creating a 'gold standard' of understanding personality from Facebook profile information." The contract promises to create a database of 2 million "matched" profiles, identifiable and tied to electoral registers, across 11 states,[15] but with room to expand much further.

III. JURISDICTION AND VENUE

22. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d), the Class Action Fairness Act, because this suit is a class action, the parties are diverse, and the amount in controversy exceeds $5 million, excluding interest and costs. The Court has supplemental jurisdiction over the related state law claims pursuant to 28 U.S.C. § 1367.

23. Venue is proper under 28 U.S.C. §1391(c) because Defendants are corporations that do business in and are subject to personal jurisdiction in this District. Venue is also proper because a substantial part of the events or omissions giving rise to the claims in this action occurred in or emanated from this District, including decisions made by Facebook to permit the information aggregation and CA's collection of the data of personally identifiable information of the class.

IV. FACTUAL ALLEGATIONS

24. On March 17, 2018, both the *New York Times* and *The Guardian* reported on Cambridge Analytica's use of PII obtained from Facebook without permission, and under the pretext of claiming to be collecting and using it for academic purposes. The reports revealed that Cambridge Analytica, a firm hired by the Trump campaign to target voters online, used the data of 87 million people obtained from Facebook without proper disclosures or permission. The reporting also found:

[15] The states are Arkansas, Colorado, Florida, Iowa, Louisiana, Nevada, New Hampshire, North Carolina, Oregon, South Carolina, and West Virginia (*See* https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm).

> [T]he firm harvested private information from the Facebook profiles of more than 50[16] million users without their permission, according to former Cambridge employees, associates and documents, making it one of the largest data leaks in the social network's history. The breach allowed the company to exploit the private social media activity of a huge swath of the American electorate, developing techniques that underpinned its work on President Trump's campaign in 2016.
>
> ***
>
> But the full scale of the data leak involving Americans has not been previously disclosed — and Facebook, until now, has not acknowledged it. Interviews with a half-dozen former employees and contractors, and a review of the firm's emails and documents, have revealed that ***Cambridge not only relied on the private Facebook data but still possesses most or all of the trove.***[17]

(Emphasis added.)

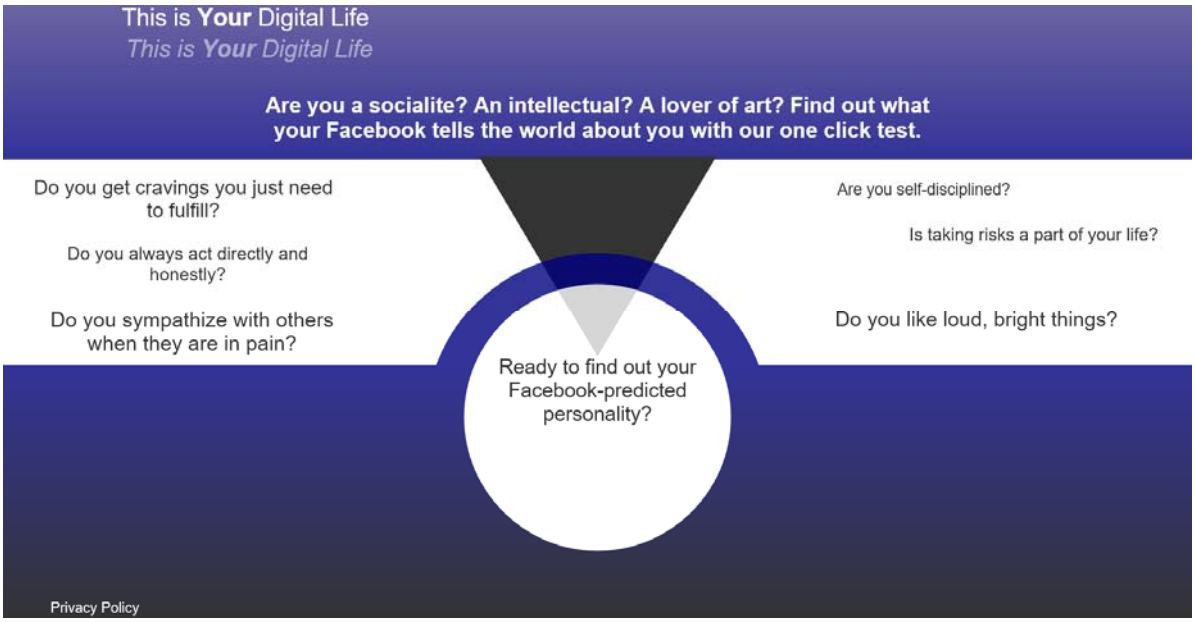
25. In 2014, Cambridge Analytica, through its parent company—Strategic Communications Laboratories (or "SCL"), hired Global Science Research Ltd. to collect Facebook user data for research purposes.[18] SCL agreed to pay GSR's data collection costs "in order to improve 'match rates' against SCL's existing datasets or to enhance GSR's algorithm's 'national capacity to profile American citizens.'"[19]

26. Global Science Research Limited (or "GSR") is a privately held company that "optimizes marketing strategies with the power of big data and psychological sciences."[20] GSR uses "innovative methods [to] produce insight on a revolutionary scale, empowering clients to understand consumers, markets, and competitors more deeply and accurately than ever before."[21] GSR was founded in 2014 by Dr. Aleksandr Kogan (or "Kogan"), a lecturer in Cambridge University's psychology department.

---

[16] Later updated to 87 million users.
[17] https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.
[18] https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data.
[19] *Id.*
[20] https://www.linkedin.com/company/global-science-research/.
[21] *Id.*

27. Global Science Research Ltd. collected this data by "us[ing] Amazon's crowdsourcing marketplace Mechanical Turk (MTurk) to access a large pool of Facebook profiles."[22] GSR offered users one-to-two dollars to download a survey app on Facebook called "ThisIsYourDigitalLife."[23] Billed as a "research app used by psychologists," GSR assured Facebook users that their Personally Identifiable Information would "only be used for research purposes" and remain "anonymous and safe."[24]



28. For every individual recruited on Facebook, CA and GSR not only harvested the Personally Identifiable Information of that individual, but the Personally Identifiable Information of all that individual's friends.[25] In 2014, Facebook users had an average of around 340 friends.[26]

---

[22] *Id.*
[23] https://www.ft.com/content/2034da4e-2988-11e8-b27e-cc62a39d57a0.
[24] https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data.
[25] *Id.*
[26] *Id.*

29. Approximately 270,000 people downloaded "ThisIsYourDigitalLife," giving CA and GSR a backdoor to the personal data of the original user and that of all their friends; ***more than 87 million*** other people.[27]

30. A former contractor with Cambridge Analytica, Christopher Wylie, revealed how the data mining worked: "With their profiles, likes, even private messages, [Cambridge Analytica] could build a personality profile on each person and know how best to target them with messages."[28]

31. Mr. Wylie stated that he had receipts, invoices, emails, legal letters and records that "showed how, between June and August 2014, the profiles of more than 87 million Facebook users had been harvested."[29] These profiles "contained enough information, including places of residence, that [Cambridge Analytica] could match users to other records and build psychographic profiles."[30]

32. In effect, Cambridge Analytica and Global Science Research Ltd. mounted a campaign of psychological warfare on millions of hapless victims, without their knowledge or consent. Indeed, of the 87 million Facebook users victimized by this scheme, "only about 270,000 users – those who had participated in the [thisisyourdigitallife] survey"[31]—had even consented to having their data harvested, and then only for research purposes, and without any authorization to have their data used to promote Cambridge Analytica's political goal to engage in cultural warfare. Mr. Wylie stated that ". . . Facebook data . . . was 'the saving grace' that let his team deliver the models it had promised . . . ."[32]

33. The personal information and data harvested from Facebook was used to "generate sophisticated models of each of [the Facebook users'] personalities using the so-

---

[27] https://www.forbes.com/sites/parmyolson/2018/03/20/face-to-face-with-cambridge-analytica-alexander-nix-facebook-trump/#674008da535f.

[28] https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump.

[29] *Id.* (Facebook later reported that the number of affected users was 87 million).

[30] https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

[31] *Id.*

[32] *Id.*

called 'big five' personality traits and characteristics – openness, conscientiousness, extraversion, agreeableness, neuroticism (known as the OCEAN scale)."[33]

34. None of those 87 million people whose data was harvested – beyond the 270,000 who downloaded the thisisyourdigitallife app, at absolute most – consented to have their data obtained or to have their "psychographic profiles" created.

35. In response to the instant, growing scandal, Facebook initially claimed that users consented to third-party apps being able to collect their data, via their friends' act of downloading the app and nothing more,[34] describing Kogan's and GSR's acquisition of data as having been done "in a legitimate way and through the proper channels that governed all developers on Facebook at that time."[35] This is incorrect, however. Nothing in Facebook's Statement of Rights and Responsibilities ("SRR") or its Privacy Policy (the documents that form the agreement between Facebook and its users) can be read to have obtained users' consent to *any* of Kogan's and GSR's practices. The applicable portions of the SRR are as follows:

> **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:
>
> …
>
> 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.)

[33] https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data.

[34] *See* https://www.nytimes.com/2018/03/19 /technology/facebook-cambridge-analytica-explained.html.

[35] *See* https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/.

36. Indeed, the SRR affirmatively *obligates* parties using the platform to respect the privacy rights of users:

> **5. Protecting Other People's Rights**
>
> We respect other people's rights, and expect you to do the same.
>
> …
>
> *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.*

37. While Facebook's Privacy Policy *does* address the phenomenon of third-party apps being able to acquire user information via that user's friends, Facebook's statement on the matter is patently misleading and describes a scenario entirely different from what Facebook now claims users consented to:

> **Controlling what is shared when the people you share with use applications**
>
> *…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.*
>
> For example, some apps use information such as your friends list, to personalize your experience or show you which of your friends use that particular app.

(italics and underline added)

38. These examples are far afield of the full extent of the "friends permission" functionality – including the use of that functionality that was sanctions by Facebook. Accordingly, Facebook is patently wrong when it suggests that users consented or otherwise authorized *any* of the conduct at issue.

39. The trove of data about a user's friends to developers was exceedingly detailed. The exfiltrated information appears to relate to virtually every aspect of a person's life as embodies on Facebook: their birthday, their hometown, their religious and political

affiliations, their work history, and also highly personal data such as location check-ins, and even the friends' photos and videos.[36]

Facebook's History of Privacy Failures

40. In 2007, Facebook initiated a tracking program called Beacon, which took information from approximately 87 million users' purchases and activities on other websites and posted it to their News Feed, without clearly asking for the user's approval.

41. Weeks after Beacon's introduction, Facebook users responded by signing a petition to drop the feature, citing concerns over privacy. In response, Facebook created an "opt out" from the service. Zuckerberg commented, "[w]e simply did a bad job with this release, and I apologize."[37] In March 2010, Facebook settled a class action for $9.5 million to resolve claims regarding its Beacon feature.

42. In 2008, Facebook introduced "Open ID," which allowed users to log in to other websites with their Facebook credentials. Facebook also made its "like" button available on other websites, further blurring the lines of privacy and allowing for widespread tracking of a person's web browsing history—even non-Facebook users.[38]

43. One year after the initial launch of "Open ID," Facebook changed its default settings to make users' profiles public by default. Users objected to this move, but it took Facebook five years to change the default to be visible to users' friends only.[39]

44. In December 2009, Facebook changed its website so that certain information that users may have designated as private was made public. Facebook didn't warn users of this change or get their prior approval. Facebook represented that third-party apps installed by users would have access only to user information needed to operate, when in fact, the apps (and their developers) could access nearly all of users' Personal Identifiable

[36] *See* http://www.businessinsider.com/what-data-did-cambridge-analytica-have-access-to-from-facebook-2018-3.
[37] https://www.msn.com/en-us/money/companies/facebooks-past-failures/ar-BBKyhST?li=BBnb7Kz.
[38] *Id.*
[39] *Id.*

Information – data the apps didn't need. Facebook users were told they could limit the sharing of their personal data to "Friends Only;" however, selecting "Friends Only" did not prevent users' Personal Identifiable Information from being shared with third-party applications their friends used. Facebook also promised it would not share users' personal data with advertisers; however, it did.

45. Upon receiving a number of complaints, the Federal Trade Commission (or "FTC") investigated Facebook's privacy practices in 2011 which resulted in a consent decree barring Facebook from making any further deceptive privacy claims, required Facebook to obtain consumers' approval before it changed the way it shared users' personal data, and required Facebook to obtain periodic assessments of its privacy practices by independent, third-party auditors for 20 years.[40] In response to the consent decree, Facebook's Zuckeberg stated, "I'm the first to admit that we've made a bunch of mistakes … [w]e can also always do better. I'm committed to making Facebook the leader in transparency and control around privacy."[41]

46. Facebook, Inc. was forewarned of the possible consequences of its privacy practices through its international subsidiary.

47. In August 2011, Facebook user Max Schrems, a German privacy rights lawyer, filed a complaint against Facebook Ireland (Defendant Facebook's Irish subsidiary and the location of its European headquarters) with the Irish-based Office of the Data Protection Commissioner (or "ODPC") concerning the access and use of Facebook users' personal data by developers of third-party applications which "constitute[d] a tremendous threat to data privacy on facebook.com."[42] Schrems went on to state that Facebook Ireland had no way "to ensure compliance with the[] limited contractual measures" it imposed on

[40] https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf; https://www.ftc.gov/sites/default/files/documents/cases/2011/12/111205facebookfrn.pdf.
[41] https://www.msn.com/en-us/money/companies/facebooks-past-failures/ar-BBKyhST?li=BBnb7Kz.
[42] https://noyb.eu/wp-content/uploads/2018/03/Media-Update-Cambridge-Analytica-en.pdf.

developers.[43] Furthermore, while Facebook supposedly requires third-party applications to have a privacy policy, not all apps have one: "[w]hen the user connects to an application that does not have a privacy policy, facebook.com simply hides the link that would usually bring you to the privacy policy, instead of warning the user that there is not even a privacy policy."[44]

48. As a result of Schrems' complaint, the ODPC investigated and issued a "Report of Re-Audit" (or "Report") on September 21, 2012, which noted that Facebook Ireland had failed to adopt complete protection of "sensitive personal data."[45] Specifically, the ODPC recommended to Facebook Ireland that:

- Users must be sufficiently empowered via appropriate information and told to make a fully informed decision when granting access to third party applications;
- It must be easier for users to understand that their activation and use of an app will be visible to their friends as a default setting;
- It should be easier for users to make informed choices about what apps installed by friends can access personal data about them.[46]

49. In June 2013, Facebook notified six million users of a data breach involving that their contact information, including phone numbers and emails. This data breach also revealed that Facebook had been merging users' information with data submitted by their contacts in order to create fuller profiles of its users. Essentially, personal data of non-Facebook users whose information may have been uploaded by friends that are Facebook users was being collected by Facebook and may have been inadvertently exposed in the breach.[47]

---

[43] *Id.*
[44] *Id.*
[45] https://dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf.
[46] *Id.*
[47] https://www.msn.com/en-us/money/companies/facebooks-past-failures/ar-BBKyhST?li=BBnb7Kz.

50. Cambridge Analytica was created in 2013 by its British parent company, Strategy Communications Laboratories Group Limited and Robert Mercer, reported to be a "secretive hedge fund billionaire" participating in American politics. Christopher Wylie stated the company's mission as: "[they] want to fight a culture war in America."[48] The Cambridge Analytica website discloses that it has offices in Washington, DC and in New York,[49] but upon information and belief, it is neither registered to do business nor is licensed to conduct business in either jurisdiction.

51. In 2015, Cambridge Analytica gained recognition as the data analysis company retained by the Ted Cruz presidential primary campaign, but after that campaign faltered in 2016, Cambridge Analytica worked for the Donald Trump presidential campaign.[50] An interview with CA's CEO, Alexander Nix, confirms that the Trump campaign paid for Cambridge Analytica's services and that then-candidate Trump was "a good businessman."[51]

52. During the Ted Cruz presidential campaign of 2015, Global Science Research Ltd. and Cambridge Analytica faced similar allegations of unauthorized use of PII from tens of millions of Facebook users for targeted marketing.[52] At the time, Facebook stated, "misleading people or misusing [users'] information is a direct violation of our policies and we will take swift action against companies that do, including banning those companies from Facebook and requiring them to destroy all improperly collected data."[53]

53. On September 11, 2017, the Spanish Agency for Data Protection (or "AEPD") announced that it had fined Facebook €1.2 million euros for violating data protection regulations following its investigation to determine whether the data processing carried out by the Company complied with the data protection regulations. The AEPD stated that its

---

[48] https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.
[49] https://cambridgeanalytica.org/.
[50] https://en.wikipedia.org/wiki/Cambridge_Analytica.
[51] https://www.forbes.com/sites/parmyolson/2018/03/20/face-to-face-with-cambridge-analytica-alexander-nix-facebook-trump/#674008da535f.
[52] *Id.*
[53] *Id.*

investigation made it possible to verify that Facebook does not inform the users in a comprehensive and clear way about the data that it collects and the treatments it carrie out with them, but that it is limited to giving some examples. In particular, the AEPD found that Facebook collects other data derived from the interaction carried out by users on the platform and on third-party sites without them being able to clearly perceive the information that Facebook collects about them or with what purpose they are going to use it. The AEPD also found that the privacy policy of Facebook contains generic and unclear expressions, and requires access to a multitude of different links to view it. Further, the AEPD concluded that Facebook makes an inaccurate reference to the way it uses the data it collects, so that Facebook users with an average knowledge of new technologies would not become aware of Facebook's data collection, storage, or use policies.[54]

54. In May 2017, the French data protection authority fined Facebook its maximum allowable fine of €150,000 for violations similar to those claimed by the Spanish authorities. "Facebook proceeded to a massive compilation of personal data of internet users in order to display targeted advertising"" complained the Commission Nationale de 'Informatique et des Libertés. "It has also been noticed that Facebook collected data on browsing activity of internet users on third-party websites without their knowledge."[55]

55. More recently, the allegations in a lawsuit filed by the makers of Pikinis, an app that was shut down three years ago when Facebook finally cut off third-party access to a back-door channel to friends' data, also undermine Facebook's suggestion that it has always placed user privacy interests at the forefront of its business. Pikinis alleged that Facebook engaged in "an anti- competitive bait-and-switch scheme" that duped Six4Three and tens of thousands of other developers into making hefty investments to build apps and then decided "it would be in Facebook's best interest to no longer compete with many developers and to shut down their businesses." While Facebook has denied any wrongdoing in the Pikinis lawsuit, its response confirms that Facebook has always had the ability to change its practices

[54] http://fortune.com/2017/09/11/facebook-privacy-fine-spain/.
[55] https://www.nytimes.com/2017/05/16/technology/facebook-privacy-france-netherlands.html.

with respect to third party developers, but did not. "Facebook made -- and must continue to make – important editorial decisions about what third party content is available through its platform to protect its users' privacy and experience," the company argued in a February 2018 court filing.[56]

56. While the plethora of earlier "red flag" warnings should have caused Facebook to seriously address what was a systemic problem with its privacy and data security practices, the so-called "White Paper" that Alex Stamos (Facebook's Chief Information Security Officer) co-authored, entitled "Information Operations and Facebook," unquestionably alerted Defendant that those activities were pervasive and supported by management. The "White Paper" also confirmed that Facebook's public statements were false and misleading. Among other things, the White Paper affirmatively misrepresented that Facebook had "no evidence of any Facebook accounts being compromised" in connection with the 2016 election as of the date it was published on April 27, 2017.

57. Stamos said that he had initially provided a written report to Facebook executives concerning the circumstances which led to the harvest of Facebook users' Personal Identifiable Information by Cambridge Analytica, but instead of taking appropriate action and disclosing the incident, the report was rewritten and presented as a hypothetical scenario; which appeared in the whitewashed "White Paper" that Facebook published to further suppress and conceal its wrongdoing.

Facebook Regarded User Privacy and Data Security as Paramount to Its Business Model, but Failed to Uphold Its Own Policies

58. Maintaining user privacy and data security has long been considered in Facebook's business and growth prospects. A June 21, 2013 blog post entitled, "Important Message from Facebook's White Hat Program" states: "At Facebook, we take people's privacy seriously, and we strive to protect people's information to the very best of our

[56] https://www.bloomberg.com/news/articles/2018-03-21/facebook-is-trying-to-protect-bikini-photos-but-it-s-not-easy.

ability. We implement many safeguards, hire the brightest engineers and train them to ensure we have only high-quality code behind the scenes or your Facebook experiences . . . ***Your trust is the most important asset we have, and we are committed to improving our safety procedures and keeping your information safe and secure.***"[57]

59. However, prior to this blog post, Facebook had experienced at least one major attack to its security systems and represented that it was "working continuously" to prevent similar security threats in the future. A February 15, 2013 post entitled, "Protecting People On Facebook" states:

> Facebook, like every significant internet service, is frequently targeted by those who want to disrupt or access our data and infrastructure. As such, ***we invest heavily in preventing, detecting, and responding to threats that target our infrastructure, and we never stop working to protect the people who use our service.*** The vast majority of the time, we are successful in preventing harm before it happens, and our security team works to quickly and effectively investigate and stop abuse.
>
> Last month, Facebook Security discovered that our systems had been targeted in a sophisticated attack. As soon as we discovered the presence of the malware, we remediated all infected machines, informed law enforcement, and began a significant investigation that continues to this day. We have found no evidence that Facebook user data was compromised.
>
> As part of our ongoing investigation, we are working continuously and closely with our own internal engineering teams, with security teams at other companies, and with law enforcement authorities to learn everything we can about the attack, and how to prevent similar incidents in the future.
>
> ***
>
> We will continue to work with law enforcement and the other organizations and entities affected by this attack. It is in everyone's interests for our industry to work together to prevent attacks such as these in the future.[58]

(Emphasis added.)

60. An October 16, 2015 post by Stamos, stated:

---

[57] https://www.facebook.com/notes/facebook-security/important-message-from-facebooks-white-hat-program/10151437074840766/.

[58] https://es-la.facebook.com/notes/facebook-security/protecting-people-on-facebook/10151249208250766/.

> ***The security of people's accounts is paramount at Facebook, which is why we constantly monitor*** for potentially malicious activity and offer many options to proactively secure your account. Starting today, we will notify you if we believe your account has been targeted or compromised by an attacker suspected of working on behalf of a nation-state.
>
> ***
>
> While we have always taken steps to secure accounts that we believe to have been compromised, we decided to show this additional warning if we have a strong suspicion that an attack could be government-sponsored. We do this because these types of attacks tend to be more advanced and dangerous than others, and we strongly encourage affected people to take the actions necessary to secure all of their online accounts.
>
> It's important to understand that this warning is not related to any compromise of Facebook's platform or systems, and that having an account compromised in this manner may indicate that your computer or mobile device has been infected with malware. Ideally, people who see this message should take care to rebuild or replace these systems if possible.
>
> To protect the integrity of our methods and processes, we often won't be able to explain how we attribute certain attacks to suspected attackers. That said, we plan to use this warning only in situations where the evidence strongly supports our conclusion. We hope that these warnings will assist those people in need of protection, and we will continue to improve our ability to prevent and detect attacks of all kinds against people on Facebook.[59]

(Emphasis added.)

61. Stamos once told his security team that he explained to upper management that Facebook has "the threat profile of a Northrop Grumman or a Raytheon or another defense contractor, but we run our corporate network, for example, like a college campus, almost."[60] Stamos repeatedly butted heads with Facebook executives over the lack of security with their platform. He once had 120 people under his direction in Facebook's security group, but as of earlier this month there are only three.[61]

62. At all relevant times, Facebook has maintained a Data Use Policy on its website. At all relevant times, the Data Use Policy advised Facebook users, in part:

---

[59] https://www.facebook.com/notes/facebook-security/notifications-for-targeted-attacks/10153092994615766/.

[60] https://www.nytimes.com/2018/03/20/technology/alex-stamos-facebook-security.html.

[61] https://www.nytimes.com/2018/03/19/technology/facebook-alex-stamos.html.

> Granting us permission to use your information 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 and any other personally identifying information from it.***[62]

(Emphasis added.)

63. In a post to the Company's website on March 18, 2018, Facebook Vice President Adam Bosworth noted that maintaining user privacy is in the Company's best interests:

> Yes developers can receive data that helps them provide better experiences to people … [we] have this set up in a way so that no one's personal information is sold to businesses.
>
> ***
>
> If people aren't having a positive experience connecting with businesses and apps then it all breaks down. This is specifically what I mean when we say [Facebook's] interests are aligned with users when it comes to protecting data."[63]

64. When Kogan created his app in 2013, Facebook allowed developers to collect information on friends of those who chose to use third-party apps if their privacy settings allowed it. In an email to university colleagues, Kogan said that in 2014, after he founded GSR, he transferred the app to the company and used an official Facebook Inc. platform for developers to change the terms and conditions of his app from "research" to "commercial use," and that at no point then did the social media company object. Kogan's email further stated: "Through the app, we collected public demographic details about each user (name, location, age, gender), and their page likes (e.g., the Lady Gaga page). We collected the same data about their friends whose security settings allowed for their friends

[62] https://www.facebook.com/full_data_use_policy.
[63] https://www.wired.com/story/facebook-privacy-transparency-cambridge-analytica/.

to share their data through apps. Each user who authorized the app was presented with both a list of the exact data we would be collecting, and also a Terms of Service detailing the commercial nature of the project and the rights they gave us as far as the data. Facebook themselves have been on the record saying that the collection was through legitimate means."[64]

65. Kogan's position contradicts Facebook's stance that Kogan violated the company's terms and services and then lied about it. "We clearly stated that the users were granting us the right to use the data in broad scope, including selling and licensing the data," Kogan wrote in a March 18, 2018 email obtained by Bloomberg. "These changes were all made on the Facebook app platform and thus they had full ability to review the nature of the app and raise issues." Facebook's position is suspect given revelations regarding its relationship with Cambridge Analytica and the fact that Facebook researchers co-authored a study with Kogan in 2015 that also used data harvested by a Facebook app.[65]

66. Although Facebook claims it did not receive notice of Cambridge Analytic harvesting users' personal data until 2015, its response to an inquiry from WIRED regarding the incident confirms that Facebook personnel were aware of similar user privacy issues by at least 2014, and knew that updates to Facebook's policies and data security practices were necessary to alleviate concerns that had already expressed by Facebook users. "In 2014, after hearing feedback from the Facebook community, we made an update to ensure that each person decides what information they want to share about themselves, including their friend list," Facebook stated. "Before you decide to use an app, you can review the permissions the developer is requesting and choose which information to share. You can manage or revoke those permissions at any time."[66]

67. Even after Facebook changed its policy in 2014 supposedly to protect user information from being exploited by "bad actors," Facebook gave developers a ***full year***

---

[64] https://www.bloomberg.com/news/articles/2018-03-21/facebook-app-developer-kogan-defends-his-actions-with-user-data.

[65] *Id.*

[66] https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/.

before it ended their access to friends' newsfeeds and photos. Worse, Facebook failed to follow up on suspicious activity when security protocols were triggered, as noted by Wylie.

68. Facebook's failure to detect and prevent the harvesting of Personal Identifiable Information by Cambridge Analytica, or to adequately respond with proper notification and disclosures to Facebook users in accordance with best practices and applicable laws, belies any claim that Facebook's actual "monitoring" practices and internal data security and privacy policies were sufficient. Facebook's user privacy data security practices were woefully inadequate.

69. The incident has violated the privacy of millions of people in every State. The privacy and personal, sensitive information of 87 million people is now at high risk for identity theft and compromise, and will continue to be at risk as a direct result of the acts of Defendants.

Government Investigations and Lawsuits

70. In the days after the breach was publicly revealed, the Attorneys General of New York and Massachusetts announced an investigation into Facebook and Cambridge Analytica.[67] On March 19, 2018, Senator Ron Wyden followed up with a detailed series of questions for Facebook to answer.[68]

71. Senators Amy Klobuchar, Democrat of Minnesota, and John Kennedy, Republican of Louisiana, have asked the chairman of the Judiciary Committee, Charles E. Grassley, Republican of Iowa, to hold a hearing.[69] Republican leaders of the Senate Commerce Committee, organized by John Thune of South Dakota, wrote a letter to Mr. Zuckerberg demanding answers to questions about how the data had been collected and if users were able to control the misuse of data by third parties.[70] "It's time for Mr.

[67] https://ag.ny.gov/press-release/statement-ag-schneiderman-facebookcambridge-analytica.
[68] https://www.wyden.senate.gov/imo/media/doc/wyden-cambridge-analytica-to-facebook.pdf.
[69] https://www.marketwatch.com/story/sens-klobuchar-kennedy-call-for-hearing-on-facebook-google-twitter-2018-03-19.
[70] https://www.commerce.senate.gov/public/_cache/files/6499b47b-05e8-49fc-90c2-6ff56dd9bf65/8D44CEC37FF5FC2C421C71962F62D998.facebook-letter-03.19.2018.pdf.

Zuckerberg and the other C.E.O.s to testify before Congress," Senator Mark Warner, Democrat of Virginia, said on Tuesday. "The American people deserve answers about social media manipulation in the 2016 election."[71]

72. On March 20, 2018, a committee in the British Parliament sent a letter to Defendant Zuckerberg and asked him to appear before the panel to answer questions on the company's connection to Cambridge Analytica. The president of the European Parliament also requested an appearance by Mr. Zuckerberg. "The committee has repeatedly asked Facebook about how companies acquire and hold on to user data from their site, and in particular about whether data had been taken without their consent," wrote Damian Collins, chairman of the British committee. "***Your officials' answers have consistently understated this risk, and have been misleading to the committee.***"[72]

73. On March 21, 2018, a former Facebook employee told British lawmakers that his concerns about lax data protection policies at the Company went ignored by "senior executives." Sandy Parakilas, who worked as a platform operations manager from 2011 to 2012, appeared before the U.K. parliament committee investigating the impact of social media on recent elections. "I made a map of the various data vulnerabilities of the Facebook platform," Parakilas told the committee. "I included lists of bad actors and potential bad actors," he said, "and said here's some of the things these people could be doing and here's what's at risk."[73] When asked by the committee if any of those executives were still at the company, Parakilas said they were, but declined to name them in public. Parakilas previously told *The Guardian* on March 20, 2018 that he had warned senior executives at Facebook about how the Company's data protection policies posed a risk of breach. Parakilas explained, "My concerns were that all of the data that left Facebook servers to developers could not be monitored by Facebook."[74] He also said that Facebook

[71] https://twitter.com/MarkWarner/status/976067286732869632.
[72] http://www.bbc.com/news/uk-43474760.
[73] https://www.bloomberg.com/news/articles/2018-03-21/facebook-ex-employee-tells-u-k-lawmakers-data-warnings-ignored.
[74] https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas.

could have prevented the collection of Personal Identifiable Information by Cambridge Analytica.

74. Parakilas was initially told that any decision to ban an app required the personal approval of the chief executive, Mark Zuckerberg.

75. From 2007 until mid-2014, Facebook allowed developers to access the personal data of friends of people who used apps by the "friends permission" functionality. This allowed tens of thousands of developers to access user data without the consent of those users.

76. Facebook had two incentives to offer up user data for these purposes. First, developers created third party content that was then hosted on Facebook and enticed users to return often. In addition, Facebook took a 30% cut of any payments made to those developers' apps.

77. Parakilas believes that "a majority of Facebook users" have had their data exfiltrated, without their consent, by unknown third parties. The use of the data continues to this day, with no oversight and in direct violation of the most basic autonomy and privacy rights of the individuals who have been – and continue to be – profiled.[75]

78. Parakilas, stated that as many as "[h]undreds of millions of Facebook users are likely to have had their private information harvested by companies that exploited the same terms as the firm that collected data and passed it on to Cambridge Analytica."[76]

79. Incredibly, Facebook's "trust model" was rife with security vulnerabilities and a near total abnegation of its responsibility to audit its own rules limiting use of Facebook data by third parties. Or, in Parakilas' own words, "[Facebook] felt that it was better not to know."[77]

[75] *Id.*
[76] https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas.
[77] *Id.*

80. That company philosophy and practice has continued since Mr. Parakilas' departure from Facebook, as evidenced by the improper harvesting and hijacking of more than 87 million of the company's user profiles by Cambridge Analytica. Facebook's stated position—that "Protecting people's information is at the heart of everything we do"[78]—is in direct contradiction with the truth: That fact, Facebook knew about this security breach for two years, but did little or nothing to protect its users.[79]

81. On March 19, 2018, *Bloomberg* reported "FTC Probing Facebook For Use of Personal Data, Source Says," disclosing that the U.S. Federal Trade Commission (or "FTC") is "probing whether Facebook violated terms of a 2011 consent decree of its handling of user data that was transferred to Cambridge Analytica without [user] knowledge."[80] Under a 2011 settlement with the FTC, Facebook "agreed to get user consent for certain changes to privacy settings as part of a settlement of federal charges that it deceived consumers and forced them to share more personal information than they intended."[81]

82. The current FTC investigation involves similar concerns about Facebook's user privacy practices. In an interview with *The New York Times*, David Vladeck, former director of the FTC's Bureau of Consumer Protection, said the Cambridge Analytica incident may have violated Facebook's 2011 consent decree. "There are all sorts of obligations under the consent decree that may not have been honored here," he said.[82] In another interview, with *The Washington Post*, Vladeck stated, "I will not be surprised if at

---

[78] https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

[79] *Id.*; https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas

[80] https://www.bloomberg.com/news/articles/2018-03-20/ftc-said-to-be-probing-facebook-for-use-of-personal-data

[81] https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf; https://www.ftc.gov/sites/default/files/documents/cases/2011/12/111205facebookfrn.pdf

[82] https://www.nytimes.com/2018/03/20/business/ftc-facebook-privacy-investigation.html.

some point the FTC looks at this. I would expect them to[.]"[83] Jessica Rich, who also served as director of the bureau and was deputy director under Vladeck, said, "Depending on how all the facts shake out, Facebook's actions could violate any of all of these provision, to the tune of many millions of dollars in penalties. They could also constitute violations of both U.S. and EU laws," adding, "Facebook can look forward to multiple investigations and potentially a whole lot of liability here."[84]

83. "We are aware of the issues that have been raised but cannot comment on whether we are investigating," an FTC spokeswoman said in a statement on March 20, 2018. "We take any allegations of violations of our consent decrees very seriously."[85]

84. Concerning the FTC investigation into the potential violations of the 2011 consent decree, Facebook's deputy chief privacy officer, Rob Sherman, stated: "We remain strongly committed to protecting people's information … We appreciate the opportunity to answer questions the FTC may have."[86] If Facebook violated terms of the consent decree, it could face fines of more than $40,000 a day per violation.

V. CLASS ACTION ALLEGATIONS

85. Plaintiff bring this class action claim pursuant to Rule 23 of the Federal Rules of Civil Procedure. The requirements of Rule 23 are met with respect to the class defined below.

86. Plaintiff brings her claims on her own behalf, and on behalf of the following class (the "Class"):

> All persons who registered for a Facebook account in the United States whose Personally Identifiable Information was obtained from Facebook by Cambridge Analytica, or other entities, without authorization or in excess of authorization.

---

[83] https://www.washingtonpost.com/business/economy/us-and-european-officials-question-facebooks-protection-of-personal-data/2018/03/18/562b5b0e-2ae2-11e8-911f-ca7f68bff0fc_story.html?utm_term=.78754f22e61b.

[84] *Id.*

[85] http://money.cnn.com/2018/03/20/technology/ftc-pressure-facebook/.

[86] *Id.*

87. Excluded from the Class are Defendants and any entities in which any Defendant or their subsidiaries or affiliates have a controlling interest, and Defendants' officers, agents, and employees. Also excluded from the Class are the judge assigned to this action, and any member of the judge's immediate family.

88. Plaintiff reserves the right to amend or modify the Class definition in connection with a motion for class certification and/or the result of discovery. This lawsuit is properly brought as a class action for the following reasons.

89. The Class is so numerous that joinder of the individual members of the proposed Class is impracticable. Plaintiff reasonably believes that the Class includes eighty-seven (87) million people or more in the aggregate and well over 1,000 in the smallest of the classes. The precise number and identities of Class members are unknown to Plaintiff, but are known to Defendants and can be ascertained through discovery regarding the information kept by Defendants or their agents.

90. Questions of law or fact common to the Class exist as to Plaintiff and all Class members, and these common questions predominate over any questions affecting only individual members of the Class. The predominant common questions of law and/or fact include the following:

a. Whether Facebook represented that it would safeguard Plaintiff's and Class members' Personally Identifiable Information and not to disclose it without consent;

b. Whether Cambridge Analytica improperly obtained Plaintiff's and Class members' Personally Identifiable Information without authorization or in excess of any authorization;

c. Whether Facebook was aware of the improper collection of Plaintiff's and Class members' Personally Identifiable Information by Cambridge Analytica;

d. Whether Facebook owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, safeguarding, and/or obtaining their Personally Identifiable Information;

e. Whether Facebook breached a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, safeguarding, and/or obtaining their Personally Identifiable Information;

f. Whether Class members' Personally Identifiable Information was obtained by CA and/or other unauthorized third-parties;

g. Whether Defendants' conduct violated Cal. Civ. Code § 1750, *et seq.*;

h. Whether Defendants' conduct was an unlawful or unfair business practice under Cal. Bus. & Prof. Code § 17200, *et seq.*;

i. Whether Defendants' conduct violated § 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, *et seq.*;

j. Whether Facebook breached its promises of privacy to its users;

k. Whether Plaintiff and the Class are entitled to equitable relief, including, but not limited to, injunctive relief and restitution; and

l. Whether Plaintiff and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief.

91. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff and the Class. Individual questions, if any, pale by comparison to the numerous common questions that predominate.

92. Plaintiff's claims are typical of the claims of Class members. The injuries sustained by Plaintiff and the Class flow, in each instance, from a common nucleus of operative facts based on the Defendants' uniform conduct as set forth above. The defenses, if any, that will be asserted against Plaintiff's claims likely will be similar to the defenses that will be asserted, if any, against Class members' claims.

93. Plaintiff will fairly and adequately protect the interests of Class members. Plaintiff has no interests materially adverse to or that irreconcilably conflict with the

interests of Class members and have retained counsel with significant experience in handling class actions and other complex litigation, and who will vigorously prosecute this action.

94. A class action is superior to other available methods for the fair and efficient group-wide adjudication of this controversy, and individual joinder of all Class members is impracticable, if not impossible. The cost to the court system of individualized litigation would be substantial. Individualized litigation would likewise present the potential for inconsistent or contradictory judgments and would result in significant delay and expense to all parties and multiple courts hearing virtually identical lawsuits. By contrast, a class action presents fewer management difficulties, conserves the resources of the parties and the courts and protects the rights of each Class member.

95. Defendants have acted on grounds generally applicable to the entire Class, thereby making injunctive relief or corresponding declaratory relief appropriate with respect to the Class as a whole.

96. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether (and when) Facebook knew about the improper collection of Personally Identifiable Information;

b. Whether Defendants' conduct was an unlawful or unfair business practice under Cal. Bus. & Prof. Code § 17200, *et seq.*;

c. Whether Facebook's representations that they would secure and not disclose without consent the Personally Identifiable Information of Plaintiff and members of the classes were facts that reasonable persons could be expected to rely upon when deciding whether to use Facebook's services;

d. Whether Facebook misrepresented the safety of its many systems and

services, specifically the security thereof, and its ability to safely store Plaintiff's and Class members' Personally Identifiable Information;

e. Whether Facebook failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

f. Whether Defendants' acts, omissions, misrepresentations, and practices were and are likely to deceive consumers;

g. Whether Defendants' conduct violated Cal. Bus. & Prof. Code § 22575, *et seq.*;

h. Whether Facebook breached its promises of privacy to its users;

i. Whether Defendants failed to adhere to their posted privacy policy concerning the care they would take to safeguard Plaintiff's and Class members' Personally Identifiable Information in violation of California Business and Professions Code § 22576;

i. Whether Defendants negligently and materially failed to adhere to their posted privacy policy with respect to the extent of their disclosure of users' data, in violation of California Business and Professions Code § 22576;

COUNT ONE

Negligence as Against Facebook

97. Plaintiff hereby incorporates all the above allegations by reference as if fully set forth herein. Plaintiff asserts this count individually and on behalf of the proposed Class.

98. Defendants owed a duty to Plaintiff and the Class to exercise reasonable care in obtaining and protecting their Personally Identifiable Information, and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties.

99. Defendants knew that the Personally Identifiable Information of Plaintiff and the Class was personal and sensitive information that is valuable.

100. By being entrusted by Plaintiff and the Class to safeguard their Personally Identifiable Information, Facebook had a special relationship with Plaintiff and the Class. Plaintiff and the Class signed up for Facebook's services and agreed to provide their Personally Identifiable Information with the understanding that Facebook would take appropriate measures to protect it, and would inform Plaintiff and the Class of any breaches or other security concerns that might call for action by Plaintiff and the Class. But, Facebook did not. Facebook failed to prevent Cambridge Analytica and Global Science Research Ltd. from improperly obtaining Plaintiff's and the Class Members' Personally Identifiable Information.

101. Defendants breached their duties by failing to adopt, implement, and maintain adequate security measures to safeguard the Personally Identifiable Information, or by obtaining that Personally Identifiable Information without authorization.

102. Facebook breached its duties by allowing a third-party to access and obtain the Personally Identifiable Information of approximately 87 million users that did not consent to provide this information to either Facebook or Cambridge Analytica.

103. Facebook further breached its duties by failing to confirm that Cambridge Analytica had deleted users' Personally Identifiable Information after it became aware of the breach of information.

104. Facebook also breached their duty to timely disclose that Plaintiff's and the other class members' Personally Identifiable Information had been, or was reasonably believed to have been, improperly obtained. Facebook first discovered that its users' information had been improperly obtained in at least 2015, but did not disclose the privacy breach until media pressure forced it to respond on March 22, 2018.

105. Cambridge Analytica had a duty to refrain from obtaining Plaintiff's and the Class Members' Personally Identifiable Information without their consent or authorization.

106. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and the Class, their Personally Identifiable Information would not have been

improperly obtained. Defendants' negligence was a direct and legal cause of the theft of the Personally Identifiable Information of Plaintiff and the Class and all resulting damages.

107. The injury and harm suffered by Plaintiff and the Class members was the reasonably foreseeable result of Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other class members' Personally Identifiable Information.

108. These damages include, but are not limited to, invasion of privacy, theft of PII, increased risk of data breaches, increased risk of identity theft, emotional distress, lost time, effort and money in responding to Facebook's negligence and misuse of their personal data beyond what Facebook promised.

COUNT TWO

Violations of the Stored Communications Act, 18 U.S.C. § 2701, *et seq*.

109. Plaintiff incorporates all of the above allegations by reference as if fully set forth herein.

110. Facebook is an electronic communications provider within the meaning of the Stored Communications Act ("SCA").

111. Under the Stored Communications Act, an entity providing an electronic communication service to the public "shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

112. The servers Facebook uses to provide its electronic communications service to Facebook users are a "facility" within the meaning of the SCA.

113. Facebook and Cambridge Analytica are "persons" within the meaning of the SCA.

114. Section 2701(a)(1) of the Stored Communications Act authorizes a private right of action for damages, injunctive relief and equitable relief against any person who "intentionally exceeds an authorization to access (a facility through which an electronic

communication service is provided] … and thereby obtains … access to wire or electronic communication while it is in electronic storage in such system…"

115. Facebook intentionally exceeded any authorization they may have had to Plaintiff's and other users' stored electronic communications by allowing Global Science Research Limited and Cambridge Analytica to have access to Plaintiff's and other users' stored electronic communications which also contained sensitive personal information.

116. Facebook knowingly allowed Global Science Research Limited and Cambridge Analytica and as yet unknown other possible third parties to intentionally exceed any authorization it may have had to Plaintiff's and other users' stored electronic communications.

117. Facebook's provision of 'users' personal data to third parties and Cambridge Analytica's acquisition of the same as alleged herein exceeded any authorization from any party to the personal data at issue.

118. Because of the architecture of Facebook's servers, the sharing of personal data among Facebook users results in and constitutes interstate data transmissions.

119. Plaintiff and Class members have been harmed by Defendants' misconduct and are entitled to statutory damages, actual damages and reasonable attorneys' fees and costs, as well as declaratory and injunctive relief.

COUNT THREE

Violations of California's Unfair Competition Law ("UCL") – Unlawful Business Practices (Cal. Bus. & Prof. Code § 17200, *et seq.*)

120. Plaintiff incorporates all of the above allegations by reference as if fully set forth herein.

121. By reason of the conduct alleged herein, Defendants engaged in unlawful practices within the meaning of the UCL. The conduct alleged herein is a "business practice" within the meaning of the UCL.

122. Facebook represented that it would not disclose user's Personally Identifiable Information without consent and/or notice. It also required application

developers, like Cambridge Analytica and Global Science Research Ltd., to obtain and utilize users' Personally Identifiable Information in specified, limited ways.

123. Facebook failed to abide by these representations. Facebook did not prevent improper disclosure of Plaintiff's and the Class Members' Personally Identifiable Information.

124. Facebook stored the Personally Identifiable Information of Plaintiff and members of the Class in its electronic and consumer information databases. Defendants represented to Plaintiff and members of the classes that their Personally Identifiable Information would remain private. Defendants engaged in unfair acts and business practices by representing that they would not disclose this Personally Identifiable Information without authorization, and/or by obtaining that Personally Identifiable Information without authorization.

125. Cambridge Analytica obtained Plaintiff's and the Class Members' Personally Identifiable Information either wholly without authorization or in excess of any authorization it—or its agents—may have obtained.

126. Defendants' acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, *inter alia*, Cal. Civ. Code § 1798.81.5(b), Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a), and Cal. Bus. & Prof. Code § 22576 (as a result of Facebook failing to comply with its own posted policies).

127. In Silicon Valley, data is currency. Plaintiff and the Class members suffered injury in fact and lost money or property as the result of Defendants' unlawful business practices. In particular, Plaintiff and Class members Personally Identifiable Information was "harvested" and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the information at issue in this case is of tangible value.

128. In particular, Plaintiff and Class members Personally Identifiable Information was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value.

129. As a result of Defendants' unlawful business practices and violation of the UCL, Plaintiff and the class are entitled to restitution, disgorgement of wrongfully obtained profits and injunctive relief.

COUNT FOUR

Violations of the California Invasion of Privacy Act (Cal. Penal Code §§ 630, *et seq.*)

130. Plaintiff incorporates all of the above allegations by reference as if fully set forth herein.

131. Plaintiff, individually and on behalf of Class Members, asserts violations of the CIPA, Cal. Penal Code § §630, *et seq.*, specifically Cal. Penal Code §§ 631(a), 632, and 637.7(d) for Cambridge Analytica's unlawful interception and use the contents of Facebook users' personal and private communications and for the unlawful acquisition of Plaintiffs and Class members' location data, without consent.

132. Cambridge Analytica used and/or continues to use this information for the purposes of profiling, marketing, and advertising.

133. Facebook was aware that Cambridge Analytica used and/or uses its users' personal and private communications in this inappropriate manner, and took no action to protect or even notify its uses. Additionally, Facebook provided the platform and lack of privacy protections that made Cambridge Analytica's misconduct possible. Facebook profited from Cambridge Analytica's misconduct.

134. Cal. Penal Code § 630 provides that "The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society."

135. Defendants' acts in violation of the CIPA occurred in the State of California because those acts resulted from business decisions, practices, and operating policies that

Facebook developed, implemented, and utilized in the State of California and which are unlawful and constitute criminal conduct in the state of Facebook's residence and principal business operations. Facebook's implementation of its business decisions, practices, and standard ongoing policies that violate the CIPA took place and continue to take place in the State of California. Defendants profited and continue to profit in the State of California as a result of its repeated and systemic violations of the CIPA. Defendants' unlawful conduct, which occurred in the State of California, harmed and continues to harm Plaintiff and Class Members.

136. Plaintiff and Class Members sent and received private messages, private wall posts, status updates, and other private communications via Facebook's services.

137. Defendants are not, and were not at any time, a party of Plaintiff's and Class Members' private messages.

138. The private messages, status updates, wall posts, and other private communications exchanged among Plaintiff and Class Members are messages.

139. These messages are communications among Plaintiff and Class Members.

A. Violations of Cal. Penal Code § 631(a)

140. Pursuant to Cal. Penal Code § 7, Defendants, corporations, are "persons."

141. Defendants use a "machine," "instrument," "contrivance," or "in any other manner" are able to, read or to learn the content or meaning of Plaintiff's and Class Members' private messages.

142. Defendants act willfully when they read, attempt to read, or learn the content or meaning of Plaintiff's and Class Members' private messages.

143. Defendants do not have the consent of any party to the communication, or they act in an unauthorized manner, when they read, attempt to read, or learn the content or meaning of Plaintiff's and Class Members' private messages.

144. Plaintiff's and Class Members' private Facebook communications are "any message, report, or communication."

145. At the time Defendants read, attempt to read, or learn the content or meaning of Plaintiff's and Class Members' private communications, the private communications are in transit.

146. At the time Defendants read, attempt to read, or learn the content or meaning of Plaintiff's and Class Members' private communications, the private communications are passing over any wire, line, or cable.

147. Private Facebook communications – coded, written messages sent electronically to remote locations – are telegraphs within the meaning of the CIPA and this section of CIPA. As such, the wires, lines, cables, and/or instruments which carry and facilitate the transmission of Plaintiff's and Class Members private Facebook communications are telegraph wires, lines, cables and/or instruments within the meaning of the CIPA and CIPA § 631(a).

148. Plaintiff and Class Members do not consent, expressly or impliedly, to Defendants' eavesdropping upon and recording of their private communications. Defendants do not disclose material information to Facebook users relating to their attempts at, among other things, intercepting, storing, and analyzing the contents of users' private communications.

149. There is no knowledge or expectation among Plaintiff and Class Members regarding the extent of Defendants' reading of private communications, learning about the content or meaning of such content, the acquisition of such content, the collection of such content, or the manipulation of such content for pecuniary gain. Each and every one of these actions extends beyond the normal occurrences, requirements, and expectations regarding the facilitation and transmission of Facebook's private communication.

B. Violations of Cal. Penal Code § 632

150. Pursuant to Cal. Penal Code §§ 7 and 632(b), Defendants, corporations, are "persons."

151. Cal. Penal Code § 632 prohibits eavesdropping upon or the recording of any confidential communication, including those occurring by telephone, telegraph, or other device, through the use of an amplification or electronic recording device without the consent of all parties to the communication.

152. Defendants intentionally and without the consent of any party to the communications, eavesdrops upon and/or records and uses the contents of Plaintiff's and Class Members' private communications.

153. Defendants use electronic amplifying or recording devices, including Cambridge Analytica's data gathering technology, to eavesdrop upon and to record Plaintiff's and Class Members' private communications, for purposes independent and unrelated to storage.

154. Plaintiff's and Class Member's private communications are confidential communications with specifically identified and designated recipients.

155. At the time Plaintiff and Class Member transmit private messages, status updates, wall posts, or other private communications through Facebook, their communications are confidential because the communications are confined to those persons specified as recipients in the destination address fields as pertaining to private messages, and are confined to pre-determined "friends" as to other communications on a private profile. There neither would nor could be any expectation that a third party, such as Cambridge Analytica or Facebook, would act in any manner other than to facilitate the communication of the private message between the sender and the intended recipient or recipients. There certainly would not and could not be any expectation that Cambridge Analytica – through Facebook – would be able to access a trove of personal information and private communications without the consent or knowledge of Plaintiff or Class Members with the intent to use such information for profiling, political advertising, and other non-academic and commercial purposes.

156. There is no knowledge or expectation among Plaintiff and Class Members regarding the extent of Defendants' reading and use of users' private communications

content, learning about the content or meaning of those private communications, acquiring and collecting the content of such communications, and manipulating the content of such communications – each action being beyond the normal occurrences, requirements, and expectations regarding the facilitation and transmission of private communications on Facebook.

157. Plaintiff's and Class Members' private communications sent via Facebook are carried on among the parties by means of an electronic device that is not a radio.

158. Plaintiff and Class Members do not consent, expressly or impliedly, to Defendants' eavesdropping upon and recording of their private communications. Neither Facebook nor Cambridge Analytica disclosed material information to Facebook users relating to their attempts to read, scan, acquire, collect, and manipulate the contents of users' private communications.

159. While Plaintiff has identified certain accused devices and/or technology in this Complaint, Plaintiff reserves the right to assert violations of Cal. Penal Code §§ 631 and 632 as to any further devices or technology subsequently discovered or any devices or technology upon which Facebook provides additional information.

C. Violations of Cal. Penal Code § 637.7

160. As defined under CIPA, "'electronic tracking device' means any device attached to a vehicle *or other movable thing that reveals its location or movement by the transmission of electronic signals*." § 637.7(d). CIPA expressly prohibits the use of "an electronic tracking device to determine the location or movement of a person." Cal. Pen. Code § 637.7(a).

161. Among the data points harvested by Facebook and provided to the remaining Defendants (as well as all third-party developers who used the "friends permission" feature) was the location of Plaintiff's and Class Members.

162. Facebook acquired – and Cambridge Analytica exfiltrated and used – Plaintiff's and Class Members' location through, *inter alia*, location data associated with smartphones and other mobile devices running Facebook.

163. Plaintiffs and Class members did not consent to said acquisition of location information by any Defendant.

D. Relief Sought Under Cal. Penal Code § 637.2

164. As a result of Defendants' violations of Cal. Penal Code §§ 631, 632, and 637, Plaintiff and the Class are entitled to:

a. Preliminary and permanent injunctive relief to require Facebook and Cambridge Analytica to fully disclose the extent of their activities, to seek the informed and knowing consent of all Facebook users when gathering private communications data, and to halt their violations;

b. Appropriate declaratory relief;

c. Monetary relief in the amount set forth in Cal. Penal Code § 637.2(a) for each Class Member; and

d. Reasonable attorney's fees and other litigation costs reasonably incurred.

COUNT FIVE

Invasion of Privacy – Intrusion Upon Seclusion

165. Plaintiff incorporates all of the above allegations by reference as if fully set forth herein.

166. Plaintiff and Class Members have reasonable expectations of privacy in their online behavior on Facebook.

167. The reasonableness of such expectations of privacy is supported by Facebook's unique position to monitor Plaintiff's and Class Members' behavior through its access to Plaintiff's and Class members' user data. It is further supported by the surreptitious, highly-technical, and non-intuitive nature of Defendants' collective tracking and exfiltrating of

Plaintiff's and Class Members' personal data, via third party apps that Class members did not download, much less provide authorization for such behavior.

168. Defendants intentionally intruded on and into Plaintiff's and Class Members' solitude, seclusion, or private affairs. Facebook intentionally designed its platform – and established commensurate policies and procedures governing such platform – to enable the exfiltration, without authorization, of Class Members' personal data by third-party apps such as "thisisyourdigitallife." Defendants intentionally availed themselves of Facebook's privacy-invasive measures in order to acquire Class Members' personal data without consent.

169. Defendants intentionally intruded on and into Plaintiff's and Class Members' solitude, seclusion, or private affairs by intentionally facilitating the exfiltration of Class Members' personal data to surreptitiously obtain, improperly gain knowledge of, review, and/or retain Plaintiff's and Class members' personal data and activities through the monitoring technologies and policies described herein.

170. These intrusions are highly offensive to a reasonable person. This is evidenced by, *inter alia*, the immense outcry following the revelation of these acts and practices – not only from the public, but also from regulators and legislators. Further, the extent of the intrusion cannot be fully known, as the nature of privacy invasion involves sharing Plaintiff's and Class members' personal information with potentially countless third-parties, known and unknown, for undisclosed and potentially unknowable purposes, in perpetuity. Also supporting the highly offensive nature of Defendants' conduct is the fact that Defendants' principal goal was to surreptitiously monitor Plaintiff's and Class Members—in one of the most private spaces available to an individual in modern life—and to allow third-parties to do the same.

171. Plaintiff and Class Members were harmed by the intrusion into their private affairs as detailed throughout this Complaint.

172. Defendants' actions and conduct complained of herein were a substantial factor in causing the harm suffered by Plaintiff and Class Members.

173. As a result of Defendants' actions, Plaintiff and Class Members seek injunctive relief, in the form of (1) destruction of all data obtained by Cambridge Analytica; (2)

certification by Facebook that no third parties presently are able to access Plaintiff's and Class Members' user data without first obtaining express consent; (3) audits, by Facebook, of all third parties who obtained user data through the "friends permissions" feature; (4) notification, by Facebook to Plaintiff and Class members, of each instance in which a third party obtained user data – including the type of user data – via the "friends permissions" feature; and (5) destruction of all improperly obtained user data of Plaintiff and Class Members.

174. As a result of Defendants' actions, Plaintiff and Class members seek nominal and punitive damages in an amount to be determined at trial. Plaintiff and Class members seek punitive damages because Defendants' actions – which were malicious, oppressive, willful – were calculated to injure Plaintiff and made in conscious disregard of Plaintiff's rights. Punitive damages are warranted to deter Defendants from engaging in future misconduct.

COUNT SIX

Violation of the California Constitution Article I, Section I

175. Plaintiff incorporates all of the above allegations by reference as if fully set forth herein.

176. Plaintiff and Class Members have reasonable expectations of privacy in their online behavior on Facebook.

177. The reasonableness of such expectations of privacy is supported by Facebook's unique position to monitor Plaintiff's and Class Members' behavior through its access to Plaintiff's and Class Members' user data. It is further supported by the surreptitious, highly technical, and non-intuitive nature of Defendants' collective tracking and exfiltrating of Class Members' personal data, via third party apps that Class Members did not download, much less provide authorization for such behavior.

178. Defendants intentionally intruded on and into Plaintiff's and Class Members' solitude, seclusion, or private affairs. Facebook intentionally designed its platform – and established commensurate policies and procedures governing such platform – to enable the exfiltration, without authorization, of Class Members' personal data by third-party apps such as

"thisisyourdigitallife." Defendants intentionally availed themselves of Facebook's privacy-invasive measures in order to acquire Class Members' personal data without consent.

179. These intrusions are highly offensive to a reasonable person. This is evidenced by, *inter alia*, the immense outcry following the revelation of these acts and practices – not only from the public, but also from regulators and legislators. Further, the extent of the intrusion cannot be fully known, as the nature of privacy invasion involves sharing Plaintiff's and Class Members' personal information with potentially countless third-parties, known and unknown, for undisclosed and potentially unknowable purposes, in perpetuity. Also supporting the highly offensive nature of Defendants' conduct is the fact that Defendants' principal goal was to surreptitiously monitor Plaintiff's and Class Members—in one of the most private spaces available to an individual in modern life—and to allow third-parties to do the same.

180. Plaintiff and Class Members were harmed by the intrusion into their private affairs as detailed throughout this Complaint.

181. Defendants' actions and conduct complained of herein were a substantial factor in causing the harm suffered by Plaintiff and Class Members.

182. As a result of Defendants' actions, Plaintiff and Class Members seek injunctive relief, in the form of (1) destruction of all data obtained by Cambridge Analytica; (2) certification by Facebook that no third parties presently are able to access Plaintiffs' and Class members' user data without first obtaining express consent; (3) audits, by Facebook, of all third parties who obtained user data through the "friends permissions" feature; (4) notification, by Facebook to Plaintiffs and Class members, of each instance in which a third party obtained user data – including the type of user data – via the "friends permissions" feature; and (5) destruction of all improperly obtained user data of Plaintiffs and Class members.

183. As a result of Defendants' actions, Plaintiffs and Class members seek nominal and punitive damages in an amount to be determined at trial. Plaintiffs and Class members seek punitive damages because Defendants' actions – which were malicious, oppressive, willful – were calculated to injure Plaintiffs and made in conscious disregard of Plaintiffs' rights. Punitive damages are warranted to deter Defendants from engaging in future misconduct.

COUNT SEVEN

Declaratory Relief Pursuant to 28 U.S.C. § 2201

184. Plaintiff incorporates all of the above allegations by reference as if fully set forth herein.

185. An actual controversy, over which this Court has jurisdiction, has arisen and now exists between the parties relating to the legal rights and duties of Plaintiff and Defendants for which Plaintiff desires a declaration of rights.

186. Plaintiff contends and Defendants dispute that Defendants, in whole or in part, were authorized by Plaintiff and Class Members to acquire user data via the "friends permissions" functionality without the express consent, from each developer, of all users whose personal data was thereby acquired.

187. Plaintiff, on behalf of himself and the Class is entitled to a declaration that Defendants were *not* so authorized through their contracts with Facebook, and accordingly that Defendants' behavior violated the Stored Communications Act, CIPA, the UCL, and Plaintiff's common law claims.

COUNT EIGHT

Conversion

188. Plaintiff incorporates all of the above allegations by reference as if fully set forth herein.

189. Plaintiff and Class Members were the owners and possessors of their private information. As the result of Defendants' wrongful conduct, Defendants have interfered with the Plaintiff's and Class Members' rights to possess and control such property, to which they had a superior right of possession and control at the time of conversion.

190. As a direct and proximate result of Defendants' conduct, Plaintiff and the Class Members suffered injury, damage, loss or harm and therefore seek compensatory damages.

191. In converting Plaintiff's Private Information, Defendants have acted with malice, oppression and in conscious disregard of the Plaintiff and Class Members' rights. Plaintiff, therefore, seeks an award of punitive damages on behalf of the class.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other Class members, respectfully requests that this Court enter a judgment against Defendants as follows:

(a) Certifying the Nationwide Class and appointing Plaintiff as Class Representative;

(b) Finding that Defendants' conduct was negligent, deceptive, unfair, and unlawful as alleged herein;

(c) Enjoining Defendants from engaging in further negligent, deceptive, unfair, and unlawful business practices alleged herein;

(d) Awarding Plaintiff and the Class members nominal, actual, compensatory, and consequential damages;

(e) Awarding Plaintiff and the Class members statutory damages and penalties, as allowed by law;

(f) Awarding Plaintiff and the Class members restitution and disgorgement;

(g) Awarding Plaintiff and the Class members pre-judgment and post-judgment interest;

(h) Awarding Plaintiff and the Class members reasonable attorneys' fees costs and expenses, and;

(i) Granting such other relief as the Court deems just and proper.

VII. DEMAND FOR JURY TRIAL

Plaintiff, individually and on behalf of all others similarly situated, demands a trial by jury on all issues so triable.

DATED: April 5, 2018

Respectfully Submitted,

/s/ Will Lemkul
Will Lemkul (State Bar No. 219061)
MORRIS SULLIVAN & LEMKUL LLP
9915 Mira Mesa Boulevard
Suite 300
San Diego, CA 92131
Telephone: (858) 566-7600
Facsimile: (858) 566-6602
Email: lemkul@morrissullivanlaw.com

/s/ Jodi Westbrook Flowers
Jodi Westbrook Flowers, *pro hac vice forthcoming*
Ann Ritter, *pro hac vice forthcoming*
Fred Baker, *pro hac vice forthcoming*
Kimberly Barone Baden (207731)
Andrew Arnold, *pro hac vice forthcoming*
Annie Kouba, *pro hac vice forthcoming*
MOTLEY RICE LLC
28 Bridgeside Boulevard
Mount Pleasant, SC 29464
Telephone: (843) 216-9000
Facsimile: (843) 216-9450
Email: jflowers@motleyrice.com
Email: aritter@motleyrice.com
Email: fbaker@motleyrice.com
Email: kbaden@motleyrice.com
Email: aarnold@motleyrice.com
Email: akouba@motleyrice.com

Attorneys for Plaintiff and the proposed class