

1 NICHOLAS A. CARLIN (State Bar No. 112532)  
2 BRIAN S. CONLON (State Bar No. 303456)  
3 PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP  
39 Mesa Street, Suite 201 - The Presidio  
4 San Francisco, CA 94129  
Telephone: 415-398-0900  
5 Fax: 415-398-0911  
Email: nac@phillaw.com  
6 bsc@phillaw.com

7 Attorneys for Plaintiff

8 UNITED STATES DISTRICT COURT  
9 NORTHERN DISTRICT OF CALIFORNIA  
10

11 JONATHAN D. RUBIN, individually and on  
12 behalf of all those similarly situated,  
13  
14 Plaintiffs,  
15  
16 v.  
17 FACEBOOK, INC, a Delaware corporation;  
18 SCL GROUP, a United Kingdom company;  
19 GLOBAL SCIENCE RESEARCH LTD, a  
20 United Kingdom company; and  
CAMBRIDGE ANALYTICA LLC, a  
Delaware limited liability company.  
21  
22 Defendants.

Case No:

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

**SUMMARY OF THE CASE**

1. On March 17, 2018, Christopher Wylie, a whistleblower and co-founder of Defendant CAMBRIDGE ANALYTICA LLC, revealed that his firm, under the direction of its Vice President and Secretary, Stephen Kevin Bannon, had used sensitive and personal information of over 50 million Americans harvested illegally via defendant FACEBOOK to manipulate American elections. The breach began in 2014, but FACEBOOK has still yet to notify its users of the breach in plain violation of California law.

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP  
39 Mesa Street, Suite 201 – The Presidio  
San Francisco, CA 94129  
Telephone: (415) 398-0900

1           2.       Plaintiff JONATHAN D. RUBIN brings this lawsuit against Defendants  
2 individually and on behalf of a class including all other similarly situated users of FACEBOOK.

3                               **PARTIES**

4           3.       Plaintiff Jonathan D. Rubin is a resident of Los Angeles, California and an  
5 individual user of FACEBOOK during the relevant time period.

6           4.       On information and belief, Defendant SCL (Strategic Communication  
7 Laboratories) GROUP (“SCL”) is a private British behavioral research and strategic  
8 communications company which owns and operates Defendant CAMBRIDGE ANALYTICA  
9 LLC. On information and belief, SCL does significant business in California.

10          5.       On information and belief, Defendant CAMBRIDGE ANALYTICA LLC  
11 (“CAMBRIDGE”) is a Delaware limited liability company owned and operated by SCL,  
12 involved in data mining and data analysis. The company maintains offices in New York and  
13 Washington D.C. and does significant business in California. Steven Kevin Bannon (“Bannon”)  
14 was Vice President and Secretary of CAMBRIDGE until he stepped down from that position to  
15 run Donald Trump’s presidential campaign. On information and belief, Bannon had decision-  
16 making authority at CAMBRIDGE and directed and approved every action taken by  
17 CAMBRIDGE as alleged herein.

18          6.       On information and belief, Defendant GLOBAL SCIENCE RESEARCH LTD.  
19 (“GSR”) was a United Kingdom company which harvested and sold the private information of  
20 social media users for profit. On information and belief, GSR did significant business in  
21 California, but has since dissolved and its successors in interest are unknown at this time.

22          7.       On information and belief, defendant FACEBOOK, INC. (“FACEBOOK”) is a  
23 Delaware corporation with its principal place of business and main operations hub located in  
24 Menlo Park, California. FACEBOOK is an omni-present social media company, whose website  
25 was launched in 2004 and that now has more than two billion active users.

26          8.       Unless separately identified, SCL, CAMBRIDGE, and GSR will be referred to  
27 herein as the “Co-Conspirators.”The business association among and between the Co-  
28 Conspirators will be referred to herein as the “Political Deceit and Manipulation Enterprise.”

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP  
39 Mesa Street, Suite 201 – The Presidio  
San Francisco, CA 94129  
Telephone: (415) 398-0900

1 9. Unless separately identified, SCL, CAMBRIDGE, GSR, and FACEBOOK will  
2 be referred to herein as the “Defendants.”  
3

4 **JURISDICTION AND VENUE**

5 10. This Court has original subject matter jurisdiction over this action pursuant to 18  
6 U.S.C. § 1964. The Court has supplemental jurisdiction over the state law claims pursuant to 28  
7 U.S.C. § 1367.

8 11. This Court has original jurisdiction pursuant to the Class Action Fairness Act, 28  
9 U.S.C. § 1332(d), because (a) at least one member of the putative class is a citizen of a state  
10 different from Defendants, (b) the amount in controversy exceeds \$5,000,000, exclusive of  
11 interest and costs, (c) the proposed class consists of more than 100 class members, and (d) none  
12 of the exceptions under the subsection apply to this action.

13 12. This Court has jurisdiction over Defendants because they conduct business in  
14 California, both in connection with the facts giving rise to this lawsuit and during the general  
15 course of their affairs, and have sufficient minimum contacts in California, or otherwise  
16 intentionally avail themselves of the markets within California, through the promotion, sale,  
17 marketing and distribution of their services and products in California, to render the exercise of  
18 jurisdiction by this Court proper and necessary.

19 13. Venue is proper in this District under 28 U.S.C. § 1391 and 18 U.S.C. § 1965  
20 because a substantial part of the events giving rise to Plaintiff’s claims occurred within this  
21 District.

22 **COMMON FACTUAL ALLEGATIONS**

23 14. FACEBOOK is an onmi-present social media company which allows billions of  
24 people, and hundreds of millions of Americans, to connect through its platform. As part of its  
25 services, FACEBOOK asks its users for a plethora of private information, including  
26 biographical information, birthday, family and relationship status, what the user is interested in,  
27 their religious and political views, their websites, whether they are online at any given time,  
28 posts to the user’s timeline or those of their friends, their hometown, their current location, their

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP  
39 Mesa Street, Suite 201 – The Presidio  
San Francisco, CA 94129  
Telephone: (415) 398-0900

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP  
39 Mesa Street, Suite 201 – The Presidio  
San Francisco, CA 94129  
Telephone: (415) 398-0900

1 education and work history, their activities, interests, posts and pages they liked, and their  
2 activity in different FACEBOOK-connected apps (“User Information”). Importantly, users  
3 control – or at least are led to believe they control – with whom they share User Information,  
4 whether it be privately with one or more individuals, to all their friends, their friends of friends,  
5 or the public at large. Users reasonably expect User Information will only be accessible to the  
6 types of people they allow to see it.

7 15. On March 17, 2018, the Guardian reported, based on information provided by  
8 Christopher Wylie, a co-founder of CAMBRIDGE, that dating back to at least 2014, Defendants  
9 SCL, CAMBRIDGE and GSR obtained from FACEBOOK the private information of at least 50  
10 million American FACEBOOK users who did not consent to their information being shared  
11 with SCL, CAMBRIDGE, or any other related companies or individuals.

12 16. In June 2014, SCL entered into a written agreement with GSR. The agreement  
13 provided that GSR would harvest and process Facebook data so that SCL and its American  
14 subsidiary, CAMBRIDGE, could analyze it and use it to manipulate the American public in  
15 upcoming elections, including the 2016 presidential election. On information and belief, SCL  
16 would not have entered into this agreement with GSR without CAMBRIDGE’s direction and  
17 approval, which it gave.

18 17. On information and belief, CAMBRIDGE and SCL spent \$7 million to amass the  
19 data it acquired, and paid about \$1 million to GSR alone.

20 18. On information and belief, these payments were made through wire transfer or  
21 other electronic payment method.

22 19. On information and belief, GSR, at the direction and with the kull knowledge of  
23 SCL and CAMBRIDGE, created a fake online personality quiz and paid a nominal fee to take it.  
24 GSR solicited participants through Amazon’s Mechanical Turk and Qualtrics’ markets. To take  
25 the quiz, users had to use GSR’s app, “thisismydigitallife.” This app enabled GSR to access the  
26 FACEBOOK profile of the person who took the quiz *and the profiles and private information of*  
27 *all their FACEBOOK friends.*  
28

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP  
39 Mesa Street, Suite 201 – The Presidio  
San Francisco, CA 94129  
Telephone: (415) 398-0900

1           20.     On information and belief, CAMBRIDGE wrote the terms of service for the app,  
2 and provided the legal advice guiding its creation.

3           21.     On information and belief, the terms of service of GRS’s app falsely represented  
4 to users that it was collecting information for academic purposes.

5           22.     On information and belief, the nominal fees paid to quiz participants were made  
6 via transfer or other electronic means via the internet.

7           23.     The result was that around 320,000 FACEBOOK users took these fake quizzes,  
8 resulting in 50 million people having their private User Information harvested for use by SCL  
9 and CAMBRIDGE, without their consent. These entities and individuals later used the data to  
10 manipulate and attempt to manipulate the voting of the American public.

11           24.     On information and belief, FACEBOOK knew or should have known of GSR,  
12 SCL, and CAMBRIDGE’s illegal scheme to obtain the User Information of its users in 2014  
13 when it was happening, but did nothing to stop it.

14           25.     Sandy Paraklias, a former Facebook operations manager responsible for policing  
15 data breaches by third-party software developers in 2011 and 2012, has stated that FACEBOOK  
16 was aware of the problem of third-party apps obtaining information from FACEBOOK users  
17 who had not authorized the apps themselves, but were relying on terms of service and settings  
18 that people didn’t read or understand, instead of fixing the problem. See  
19 [https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-](https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas)  
20 [parakilas](https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas).

21           26.     Paraklias stated that GSR’s app was “one of the very last to have access to friend  
22 permissions,” meaning that FACEBOOK was well-aware of the problem by the time GSR, SCL  
23 and CAMBRIDGE used it to acquire User Information of 50 million FACEBOOK users without  
24 their permission.

25           27.     It was not until August 2016 when FACEBOOK wrote a letter to Wylie, stating  
26 that the data must be deleted immediately, that FACEBOOK did anything to address GSR, SCL,  
27 and CAMBRIDGE’s data theft. But this was two years after the data was harvested, and had  
28 already been used and weaponized against the American public by SCL and CAMBRIDGE at

1 Bannon’s direction. Deleting the data at that point was meaningless; indeed, Wylie stated that  
2 he had already deleted the data by that point and that FACEBOOK made “zero effort to get the  
3 data back.”

4 28. FACEBOOK never notified the 50 million users that their User Information had  
5 been compromised.

6 **FACEBOOK’s Security Practices are Inadequate**  
7 **and Their Representations to Their Users are Misleading**

8 29. Despite growing efforts by hackers and others to illegally access personal  
9 information maintained by social media companies and the emphasis on data security in social  
10 media companies, FACEBOOK (1) failed to implement security measures and technological  
11 safeguards designed to prevent this type of attack even though social media is particularly  
12 vulnerable to this type of data theft; (2) failed to employ security protocols to detect the  
13 unauthorized network activity (or if it did, to sufficiently act on the breach), and (3) failed to  
14 maintain basic security measures.

15 30. This despite FACEBOOK stating publicly that “Protecting people’s information  
16 is at the heart of everything we do.” See  
17 <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>.

18 31. On March 19, 2018, *Bloomberg* published an article entitled “FTC Probing  
19 Facebook For Use of Personal Data, Source Says,” disclosing that the U.S. Federal Trade  
20 Commission (“FTC”) was “probing whether Facebook violated terms of a 2011 consent decree  
21 of its handling of user data that was transferred to [CAMBRIDGE] without [user] knowledge.”  
22 Under the 2011 settlement with the FTC, FACEBOOK “agreed to get user consent for certain  
23 changes to privacy settings as part of a settlement of federal charges that it deceived consumers  
24 and forced them to share more Personal Information than they intended.” The article further  
25 stated that “if the FTC finds Facebook violated terms of the consent decree, it has the power to  
26 fine the company more than \$40,000 a day per violation.”

27 32. At all relevant times, FACEBOOK has maintained a Data Use Policy on its  
28 website, which advised FACEBOOK users, in part: “While you are allowing us to use the

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP  
39 Mesa Street, Suite 201 – The Presidio  
San Francisco, CA 94129  
Telephone: (415) 398-0900

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP  
39 Mesa Street, Suite 201 – The Presidio  
San Francisco, CA 94129  
Telephone: (415) 398-0900

1 information we receive about you, **you always own all of your information. Your trust is**  
2 **important to us, which is why we don't share information we receive about you with others**  
3 **unless we have: [1] received your permission; [2] given you notice**, such as by telling you  
4 about in this policy; or [3] removed your name and any other personally identifying information  
5 from it.” [https://www.facebook.com/full\\_data\\_use\\_policy](https://www.facebook.com/full_data_use_policy) (emphasis added).

6 33. On information and belief, none of the friends of the individuals who took GSR's  
7 quiz gave FACEBOOK permission to share their personal and private User Information with  
8 any other Co-Conspirator, FACEBOOK did not give any of the 50 million Americans notice  
9 that their User Information was taken by the other Co-Conspirators, and FACEBOOK did not  
10 remove the name and other personally identifying information from those 50 million Americans'  
11 information before the other Co-Conspirators took it.

### 12 **Over 50 Million Americans are Victims of the Breach**

13 34. As a result of FACEBOOK's negligent security practices, misrepresentations to  
14 its users, and delay in notifying affected consumers, these users are subject to an increased and  
15 real risk of identity theft based on the breach of their personal FACEBOOK information.

16 35. Affected users will have to spend time and money securing their User  
17 Information and protecting their identities. They will need to monitor their accounts and credit,  
18 and will have to pay for further identity theft protection services in the wake of the data breach,  
19 to make sure their identities were not stolen.

20 36. Now that their private User Information has been sold on the open market,  
21 consumers also face a real and immediate risk of identity theft and other problems associated  
22 with disclosure of this private information, and will need to monitor their credit and tax filings  
23 for an indefinite duration.

### 24 **PLAINTIFF'S EXPERIENCE**

25 37. At relevant times hereto, FACEBOOK collected and stored User Information  
26 from Plaintiff, including his biographical information, birthday, family and relationship status,  
27 what he was interested in, his religious and political views, his websites, whether he was online  
28 at any given time, any posts to his timeline, his hometown, his current location, his education



PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP  
39 Mesa Street, Suite 201 – The Presidio  
San Francisco, CA 94129  
Telephone: (415) 398-0900

1 and work history, his activities, interests, and posts and pages he liked, and his activity in  
2 different apps.

3 38. Plaintiff has been a regular FACEBOOK user at all relevant times and has 1,050  
4 Facebook friends. Plaintiff did not take the above-referenced fake personality quiz and did not  
5 ever consent to allowing GSR, SCL, or CAMBRIDGE to have access to his User Information.  
6 On information and belief, Plaintiff is one of the more than fifty (50) million Americans whose  
7 private User Information has been compromised by Co-Conspirator’s actions.

8 39. Plaintiff did not know and could not know of the conduct alleged in this  
9 complaint until March 17, 2018, because Co-Conspirators, including FACEBOOK, never  
10 disclosed the breach to their victims.

11 40. As a result of the disclosure of his User Information to GSR, SCL and  
12 CAMBRIDGE and unknown others, Plaintiff has spent time and money securing his personal  
13 information and protecting his identity, by, for instance, purchasing identity theft protection. In  
14 addition, now that Plaintiff’s information has been sold on the open market, Plaintiff faces a real  
15 and imminent risk of identity theft and other problems associated with disclosure of his private  
16 information, and will need to monitor his credit and tax filings for an indefinite duration.

17 **CLASS ACTION ALLEGATIONS**

18 41. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 on  
19 behalf of himself and the following class:

20 All persons in the United States whose personal data was stored by FACEBOOK  
21 and who had such data accessed by GSR, SCL, or CAMBRIDGE without  
authorization or in excess of authorization.

22 Excluded from the proposed class are anyone employed by counsel for Plaintiff in this action  
23 and any Judge to whom this case is assigned, as well as his or her staff and immediate family.

24 42. Plaintiff satisfies the numerosity, commonality, typicality, and adequacy  
25 prerequisites for suing as a representative party pursuant to Rule 23.

26 43. Numerosity. The proposed class consists of over 50 million American consumers  
27 who had their data stolen by GSR, SCL and CAMBRIDGE through FACEBOOK making  
28 joinder of each individual class member impracticable.



1           44.    Commonality. Common questions of law and fact exist for the proposed class’  
2 claims and predominate over questions affecting only individual class members.

3           Common questions include:

- 4           a.       Whether FACEBOOK violated California Civil Code section 1798.81.5 by  
5 failing to implement reasonable security procedures and practices;
- 6           b.       Whether FACEBOOK violated California Civil Code section 1798.82 by failing  
7 to promptly notify class members that their personal information had been compromised;
- 8           c.       Whether FACEBOOK acted negligently in failing to maintain adequate security  
9 procedures and practices;
- 10          d.       Whether FACEBOOK breached its contractual promises to adequately protect  
11 class members’ personal information;
- 12          e.       Whether FACEBOOK’s failure to implement adequate security constitutes an  
13 unfair, unlawful, or deceptive practice under state consumer protection law;
- 14          f.       Whether class members may obtain damages, restitution, declaratory and  
15 injunctive relief against FACEBOOK;
- 16          g.       Whether class members had a reasonable expectation of privacy in the personal  
17 data and information they provided to FACEBOOK;
- 18          h.       Whether GSR, SCL and CAMBRIDGE, by their actions, intentionally intruded  
19 into the class members’ private and personal FACEBOOK data by mining it without their  
20 permission;
- 21          i.       Whether GSR, SCL and CAMBRIDGE’s intrusion was highly offensive to a  
22 reasonable person;
- 23          j.       Whether class members were harmed;
- 24          k.       Whether Co-Conspirator’s conduct was a substantial factor in causing class  
25 members’ harm;
- 26          l.       Whether Co-Conspirators acts constitute a pattern of racketeering activity  
27 pursuant to 18 U.S.C. § 1961(5); and
- 28

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP  
39 Mesa Street, Suite 201 – The Presidio  
San Francisco, CA 94129  
Telephone: (415) 398-0900

1 m. What security procedures and data-breach notification procedure FACEBOOK  
2 should be required to implement as part of any injunctive relief ordered by the Court.

3 45. Typicality. Plaintiff's claims are typical of the claims of the proposed class  
4 because, among other things, Plaintiff and class members sustained similar injuries as a result of  
5 Defendants' uniform wrongful conduct and their legal claims all arise from the same core  
6 Defendants' practices.

7 46. Adequacy. Plaintiff will fairly and adequately protect the interests of the class.  
8 His interests do not conflict with class members' interests and he has retained counsel  
9 experienced in complex class action and data privacy litigation to vigorously prosecute this  
10 action on behalf of the class.

11 47. In addition to satisfying the prerequisites of Rule 23(a), Plaintiff satisfies the  
12 requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and  
13 fact predominate over any questions affecting only individual class members and a class action  
14 is superior to individual litigation. The amount of damages available to individual plaintiffs is  
15 insufficient to make litigation addressing Defendants' conduct economically feasible in the  
16 absence of the class action procedure. Individualized litigation also presents a potential for  
17 inconsistent or contradictory judgments, and increases the delay and expense to all parties and  
18 the court system presented by the legal and factual issues of the case. By contrast, the class  
19 action device presents far fewer management difficulties and provides the benefits of a single  
20 adjudication, economy of scale, and comprehensive supervision by a single court.

21 48. In addition, class certification is appropriate under Rule 23(b)(1) and/or (b)(2)  
22 because:

23 a. the prosecution of separate actions by the individual members of the proposed  
24 class would create a risk of inconsistent or varying adjudications which would establish  
25 incompatible standards of conduct for Defendants;

26 b. the prosecution of separate actions by individual class members would create a  
27 risk of adjudications with respect to them which would, as a practical matter, be dispositive of  
28

1 the interests of other class members not parties to the adjudications, or substantially impair or  
2 impede their ability to protect their interests; and

3 c. Defendants have acted or refused to act on grounds that apply generally to the  
4 proposed class, thereby making final injunctive relief or declaratory relief described herein  
5 appropriate with respect to the proposed class as a whole.

6 **FIRST CLAIM FOR RELIEF**

7 **For Violations of Racketeer Influenced and Corrupt Organizations Act,**

8 **18 U.S.C. § 1962(c)**

9 **(Against Co-Conspirators)**

10 49. Plaintiff incorporates the above allegations by reference.

11 50. The Political Deceit and Manipulation Enterprise is an enterprise engaged in, and  
12 whose activities affect, interstate commerce. This enterprise has been in operation since at least  
13 2014.

14 51. On information and belief, Co-Conspirators agreed to and did conduct and  
15 participate, directly and indirectly, in the conduct of the Political Deceit and Manipulation  
16 Enterprise's affairs in a pattern of racketeering activity targeted at intentionally defrauding  
17 FACEBOOK users including, without limitation, via nominal payments and numerous  
18 intentionally false representations averred herein with the specific intent of inducing  
19 FACEBOOK users to unwittingly share other users' private User Information.

20 52. Pursuant to and in furtherance of their corrupt scheme, Co-Conspirators did in  
21 fact induce FACEBOOK users to unwittingly share other FACEBOOK users' User Information  
22 via hundreds of thousands of separate electronic monetary transfers.

23 53. Co-Conspirators willfully and knowingly devised a scheme with artifice to  
24 defraud FACEBOOK users and to obtain, sell, and use personal User Information by false  
25 pretenses and representations, including but not limited to the representation that the data would  
26 only be used for academic purposes.

27 54. The payments made or directed by CAMBRIDGE or SCL to GSR or any other  
28 entity to obtain FACEBOOK data were in furtherance of the fraudulent scheme. On information

1 and belief, those payments were made by wire transfer or other electronic means through  
2 interstate or foreign commerce.

3 55. The payments made from any Co-Conspirator or directed by any Co-Conspirator  
4 to takers of GSR's quiz were in furtherance of the fraudulent scheme. On information and  
5 belief, those payments were made by wire transfer or other electronic means through interstate  
6 or foreign commerce.

7 56. The acts of wire fraud averred herein constitute a pattern of racketeering activity  
8 pursuant to 18 U.S.C. § 1961(5).

9 57. The Co-Conspirators have directly and indirectly participated in the conduct of  
10 the Political Deceit and Manipulation Enterprise's affairs through the pattern of racketeering and  
11 activity alleged herein, in violation of 18 U.S.C. 1962(c). FACEBOOK aided and abetted the  
12 Co-Conspirators by misleading its users to believe that their data was safe, while permitting  
13 third-party apps like GSR's to access and use the data of non-consenting users without their  
14 permission and knowledge, and the other Co-Conspirators directly participated in the conspiracy  
15 by misleading quiz-takers that they were allowing Co-Conspirators' access to only their personal  
16 data for academic purposes, when in fact they were allowing access to their friends' data, and by  
17 fraudulently obtaining the data, selling it in interstate and foreign commerce, and using it to  
18 influence elections.

19 58. Plaintiff and class members were harmed by Co-Conspirators' conduct because  
20 the private information they did not intend to become public or disclose to third parties was  
21 acquired by companies who intended to and did use it illicitly for manipulating elections and  
22 other as yet unknown purposes. Furthermore, the security breach put Plaintiff and class  
23 members in imminent and real danger of having their identities stolen by anyone willing to pay  
24 these unscrupulous companies for the data. In addition, Plaintiff and class members spent time  
25 and money securing their personal information and protecting their identities, by, for instance,  
26 purchasing identity theft protection. The harm and value of the User Information is made plain  
27 by the fact that CAMBRIDGE paid \$7 million to acquire the information.  
28

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP  
39 Mesa Street, Suite 201 – The Presidio  
San Francisco, CA 94129  
Telephone: (415) 398-0900



1           66.     The breach of the personal User Information of tens of millions of FACEBOOK  
2 customers constituted a “breach of the security system” of FACEBOOK pursuant to Civil Code  
3 § 1798.82(g).

4           67.     By failing to implement reasonable measures to protect its customers’ personal  
5 User Information, FACEBOOK violated Civil Code § 1798.81.5.

6           68.     In addition, by failing to promptly notify all affected customers that their  
7 personal User Information had been acquired (or was reasonably believed to have been  
8 acquired) by unauthorized persons, like GSR, SCL and CAMBRIDGE in the data breach,  
9 FACEBOOK violated Civil Code § 1798.82. FACEBOOK’s failure to timely notify users of the  
10 breach has caused damage to class members who have had to buy identity protection services or  
11 take other measures to remediate the breach caused by FACEBOOK’s negligence.

12           69.     By violating Civil Code §§ 1798.81.5 and 1798.82, FACEBOOK “may be  
13 enjoined” under Civil Code § 1798.84(e).

14           70.     Accordingly, Plaintiff requests that the Court enter an injunction requiring  
15 FACEBOOK to implement and maintain reasonable security procedures to protect customers’  
16 User Information in compliance with the California Customer Records Act, including, but not  
17 limited to: (1) ordering that FACEBOOK, consistent with industry standard practices, engage  
18 third party security auditors/penetration testers as well as internal security personnel to conduct  
19 testing, including simulated attacks, penetration tests, and audits on FACEBOOK’s systems on a  
20 periodic basis; (2) ordering that FACEBOOK engage third party security auditors and internal  
21 personnel, consistent with industry standard practices, to run automated security monitoring; (3)  
22 ordering that FACEBOOK audit, test, and train its security personnel regarding any new or  
23 modified procedures; (4) ordering that FACEBOOK, consistent with industry standard practices,  
24 conduct regular database scanning and securing checks; (5) ordering that FACEBOOK,  
25 consistent with industry standard practices, periodically conduct internal training and education  
26 to inform internal security personnel how to identify and contain a breach when it occurs and  
27 what to do in response to a breach; (6) ordering FACEBOOK to meaningfully educate its former  
28 and current users and employees about the threats they face as a result of the loss of their

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP  
39 Mesa Street, Suite 201 – The Presidio  
San Francisco, CA 94129  
Telephone: (415) 398-0900

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP  
39 Mesa Street, Suite 201 – The Presidio  
San Francisco, CA 94129  
Telephone: (415) 398-0900

1 personal User Information to third parties, as well as the steps they must take to protect  
2 themselves; and (7) ordering FACEBOOK to encrypt sensitive personal information.

3 71. Plaintiff further requests that the Court require FACEBOOK to (1) identify and  
4 notify all members of the class who have not yet been informed of the data breach; and (2) to  
5 notify affected former and current users and employees of any future data breaches by email  
6 within 24 hours of FACEBOOK’s discovery of a breach or possible breach and by mail within  
7 72 hours.

8 72. As a result of FACEBOOK’s violation of Civil Code §§ 1798.81.5, and 1798.82,  
9 Plaintiff and members of the class have and will incur economic damages relating to time and  
10 money spent remedying the breach, including, but not limited to, monitoring their online  
11 presence to ensure that their identity has not been stolen or coopted for an illicit purpose, any  
12 unauthorized charges made on financial accounts, lack of access to funds while banks issue new  
13 cards, tax fraud, as well as the costs of credit monitoring and purchasing credit reports.

14 73. Plaintiff, individually and on behalf of the members of the Class, seeks all  
15 remedies available under Civil Code § 1798.84, including, but not limited to: (a) damages  
16 suffered by members of the class; and (b) equitable relief.

17 74. Plaintiff, individually and on behalf of the members of the Class, also seek  
18 reasonable attorneys’ fees and costs under applicable law including Federal Rule of Civil  
19 Procedure 23 and California Code of Civil Procedure § 1021.5.

20 **THIRD CLAIM FOR RELIEF**

21 **Intrusion Upon Seclusion**

22 **(Against All Defendants)**

23 75. Plaintiff incorporates the above allegations by reference.

24 76. Plaintiff and class members put User Information on their FACEBOOK profiles,  
25 including biographical information, birthdays, family and relationship status, their interests,  
26 religious and political views, websites, any posts on their or their friend’s timelines, their  
27 hometown, their current location, their education and work history, their activities, interests, and  
28 posts and pages they liked, and their activity in different apps.



1           77.     Importantly, Plaintiff and class members control – or at least were led to believe  
2 they control – via FACEBOOK’s privacy settings, who has access to what information, be it  
3 private individuals, their FACEBOOK friends, the friends of their FACEBOOK friends, or the  
4 public at large. By putting their information on FACEBOOK, Plaintiff and class members  
5 expect to be able to control who may access that information and expect that only those  
6 individuals who they allow access to that information will be able to see it. As FACEBOOK  
7 puts it, Plaintiff and class members expect to “own all of [their] information.” With respect to  
8 everyone else in the world, besides those who Plaintiff and class members give permission to  
9 see that information, their reasonable expectation is for that information to remain private.

10           78.     By acquiring and using Plaintiff’s and class members’ data from their  
11 FACEBOOK accounts without their permission as alleged above, GSR, SCL and CAMBRIDGE  
12 intentionally intruded upon Plaintiff’s and class members’ private information.

13           79.     FACEBOOK aided and abetted GSR, SCL and CAMBRIDGE’s intrusion upon  
14 Plaintiff and class members’ seclusion because it (1) knew or should have known about this  
15 intrusion; (2) gave substantial assistance to GSR, SCL and CAMBRIDGE by allowing apps like  
16 those used by GSR to access user’s friends’ User Information without their consent and not  
17 notifying their users of the breach or otherwise attempting to stop the breach or control the User  
18 Information leaked as a result of the breach for at least two years; (3) FACEBOOK’s actions and  
19 failure to act was a substantial factor in causing harm to Plaintiff and class members because it  
20 had the capability of stopping the intrusion at any time, but knowingly failed to do so.

21           80.     Defendants’ intrusion and theft of Plaintiff’s and class members’ personal User  
22 Information from their FACEBOOK accounts was highly offensive to a reasonable person in  
23 that (1) GSR, SCL and CAMBRIDGE stole a huge amount of personal and private information  
24 about each person in order to effectively control and alter the votes of the American public; (2)  
25 GSR, SCL and CAMBRIDGE were motivated by profit and political ambition and their goal  
26 was to serve their owners’ purposes of manipulating the American political process and preying  
27 on people’s biases and tendencies to distort their beliefs and ultimately undermine American  
28 democracy; and (3) the intrusion occurred in the setting of FACEBOOK, a social media

1 company Americans trust – because of FACEBOOK’s own representations – to take care of the  
 2 data they share with their friends and family (and not with corporations attempting to fix  
 3 elections through the use of misinformation).

4 81. Plaintiff and class members were harmed by Defendants’ conduct because the  
 5 private information they did not intend to become public was acquired by companies who  
 6 intended to use it for the illicit purpose of manipulating elections. Furthermore, the security  
 7 breach put Plaintiff and class members in imminent and real danger of having their identities  
 8 stolen by anyone willing to pay these unscrupulous companies for the data. The harm and value  
 9 of Plaintiff’s and class members’ User Information is also made plain by the fact that  
 10 CAMBRIDGE paid \$7 million to acquire the User Information. Plaintiff and members of the  
 11 class have and will incur economic damages relating to time and money spent remedying the  
 12 breach, including, but not limited to, monitoring their online presence to ensure that their  
 13 identity has not been stolen or coopted for an illicit purpose, any unauthorized charges made on  
 14 financial accounts, lack of access to funds while banks issue new cards, tax fraud, as well as the  
 15 costs of credit monitoring and purchasing credit reports.

16 82. Defendants’ acts as alleged herein were despicable and were carried out  
 17 intentionally, with willful and conscious disregard of the rights or safety of Plaintiff and class  
 18 members, subjecting them to cruel and unjust hardship. Defendants’ conduct constitutes malice,  
 19 fraud, and/or oppression, and Plaintiff and class members are therefore entitled to recover  
 20 punitive and exemplary damages in an amount according to proof.

21 **FOURTH CLAIM FOR RELIEF**

22 **For Unlawful and Unfair Business Practices Under**  
 23 **California Business and Professions Code § 17200, *et seq.***  
 24 **(Against FACEBOOK)**

25 83. Plaintiff incorporates the above allegations by reference.

26 84. FACEBOOK’s acts and practices, as alleged in this complaint, constitute  
 27 unlawful and unfair business practices, in violation of the Unfair Competition Law (“UCL”),  
 28 Cal. Bus. & Prof. Code § 17200, *et seq.*

1           85.     The acts, omissions, and conduct of FACEBOOK also constitute a violation of  
2 the unlawful prong of the UCL because it failed to comport with a reasonable standard of care  
3 and public policy as reflected in statutes such as the Information Practices Act of 1977 and  
4 California Customer Records Act, which seek to protect individuals' data and ensure that  
5 entities who solicit or are entrusted with personal data utilize reasonable security measures.

6           86.     In failing to protect consumers' User Information and unduly delaying informing  
7 them of the data breach, while simultaneously misrepresenting to its consumers that the data was  
8 safe and would not be shared without their permission, FACEBOOK has engaged in unfair  
9 business practices by engaging in conduct that undermines or violates the stated policies  
10 underlying the California Customer Records Act and the Information Practices Act of 1977. In  
11 enacting the California Customer Records Act, the Legislature stated that: "[i]dentity theft is  
12 costly to the marketplace and to consumers" and that "victims of identity theft must act quickly  
13 to minimize the damage; therefore expeditious notification of possible misuse of a person's  
14 personal information is imperative." 2002 Cal. Legis. Serv. Ch. 1054 (A.B. 700).

15 FACEBOOK's conduct also undermines California public policy as reflected in other statutes  
16 such as the Information Practices Act of 1977, Cal. Civ. Code § 1798, et seq., which seeks to  
17 protect individuals' data and ensure that entities who solicit or are entrusted with personal data  
18 utilize reasonable security measures.

19           87.     As a direct and proximate result of FACEBOOK's unlawful and unfair business  
20 practices as alleged herein, Plaintiff and members of the class have suffered injury in fact.  
21 Plaintiff and the class have been injured in that their personal information has been  
22 compromised and they are at an imminent risk for future identity theft and fraudulent activity.  
23 Plaintiff and class members have also lost money and property by purchasing credit monitoring  
24 services they would not otherwise had to but for FACEBOOK's unlawful and unfair conduct.

25           88.     As a direct and proximate result of FACEBOOK's unlawful and unfair business  
26 practices as alleged herein, Plaintiff and class members face an increased risk of identity theft  
27 and medical fraud, based on the theft and disclosure of their personal User Information.

28           89.     Because of FACEBOOK's unfair and unlawful business practices, Plaintiff and

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP  
39 Mesa Street, Suite 201 – The Presidio  
San Francisco, CA 94129  
Telephone: (415) 398-0900

1 the class are entitled to relief, including restitution to Plaintiff and class members for costs  
2 incurred associated with the data breach and disgorgement of all profits accruing to  
3 FACEBOOK because of its unlawful and unfair business practices, declaratory relief, and a  
4 permanent injunction enjoining FACEBOOK from its unlawful and unfair practices.

5 90. The injunctive relief that Plaintiff and members of the class are entitled to  
6 includes, but is not limited to: (1) ordering that FACEBOOK, consistent with industry standard  
7 practices, engage third party security auditors/penetration testers as well as internal security  
8 personnel to conduct testing, including simulated attacks, penetration tests, and audits on  
9 FACEBOOK’s systems on a periodic basis; (2) ordering that FACEBOOK engage third party  
10 security auditors and internal personnel, consistent with industry standard practices, to run  
11 automated security monitoring; (3) ordering that FACEBOOK audit, test, and train its security  
12 personnel regarding any new or modified procedures; (4) ordering that FACEBOOK, consistent  
13 with industry standard practices, conduct regular database scanning and securing checks; (5)  
14 ordering that FACEBOOK, consistent with industry standard practices, periodically conduct  
15 internal training and education to inform internal security personnel how to identify and contain  
16 a breach when it occurs and what to do in response to a breach; (6) ordering FACEBOOK to  
17 meaningfully educate its former and current users and employees about the threats they face as a  
18 result of the loss of their personal information to third parties, as well as the steps they must take  
19 to protect themselves; and (7) ordering FACEBOOK to encrypt sensitive personal information.

20 91. Plaintiff, individually and on behalf of the members of the class, also seeks  
21 reasonable attorneys’ fees and costs under applicable law including Federal Rule of Civil  
22 Procedure 23 and California Code of Civil Procedure § 1021.5.

23 **FIFTH CLAIM FOR RELIEF**

24 **Negligence**

25 **(Against FACEBOOK)**

26 92. Plaintiff incorporates the above allegations by reference.

27 93. In collecting the User Information of its users, FACEBOOK owed Plaintiff and  
28 members of the class a duty to exercise reasonable care in safeguarding and protecting that User

1 Information. This duty included, among other things, maintaining and testing FACEBOOK's  
2 security systems and taking other reasonable security measures to protect and adequately secure  
3 the personal data of Plaintiff and the class from unauthorized access and use. FACEBOOK's  
4 security system and procedures for handling the personal User Information were intended to  
5 affect Plaintiff and the class. FACEBOOK was aware that by taking such sensitive information  
6 of users, it had a responsibility to take reasonable security measures to protect the data from  
7 being stolen and, in the event of theft, easily accessed.

8 94. The duty FACEBOOK owed to Plaintiff and members of the class to protect  
9 their personal User Information is also underscored by the California Customer Records Act.

10 95. Additionally, FACEBOOK had a duty to timely disclose to Plaintiff and  
11 members of the class that their personal User Information had been or was reasonably believed  
12 to have been compromised and made accessible to unauthorized third parties, like SCL and  
13 CAMBRIDGE. Timely disclosure is appropriate so that Plaintiff and members of the class  
14 could, among other things, monitor their online presence to ensure it has not been coopted for an  
15 illicit purpose, undertake appropriate measures to avoid unauthorized charges on their debit card  
16 or credit card accounts, purchase credit monitoring services, and change or cancel their debit or  
17 credit card PINs (personal identification numbers) to prevent or mitigate the risk of fraudulent  
18 cash withdrawals or unauthorized transactions.

19 96. There is a very close connection between FACEBOOK's failure to take  
20 reasonable security standards to protect its users' data and the injury to Plaintiff and the class. If  
21 not for FACEBOOK's negligence, GSR, SCL, and CAMBRIDGE would not have been able to  
22 steal Plaintiff's and the class's information and use it for their own political purposes.

23 97. FACEBOOK is morally to blame for not protecting the User Information,  
24 misrepresenting to its users how secure their User Information was, and by failing to take  
25 reasonable security measures. If FACEBOOK had taken reasonable security measures, data  
26 thieves, like GSR, SCL, and CAMBRIDGE would not have been able to take the personal User  
27 Information of over 50 million Americans and use it to manipulate the American people and  
28 undermine American democracy.

1           98.     The policy of preventing future harm weighs in favor of finding a special  
2 relationship between FACEBOOK and the class. FACEBOOK's users count on FACEBOOK  
3 to keep their User Information safe and in fact are encouraged to share sensitive personal data  
4 with FACEBOOK. If companies are not held accountable for failing to take reasonable security  
5 measures to protect their customers' personal information, they will not take the steps that are  
6 necessary to protect against future data breaches.

7           99.     It was foreseeable that if FACEBOOK did not take reasonable security measures,  
8 the User Information of Plaintiff and members of the class would be stolen. In fact, on  
9 information and belief, FACEBOOK was well aware that third-party apps like the one created  
10 by GSR could and did steal the User Information users who never consented to give those apps  
11 access to their information. Major corporations, particularly those in the social media industry,  
12 like FACEBOOK, face a higher threat of security breaches than other companies due in part to  
13 the large amounts and type of data they possess. FACEBOOK should have known to take  
14 precautions to secure its users' User Information, especially in light of the sheer volume of data  
15 accumulated by FACEBOOK from its users.

16           100.    FACEBOOK breached its duty to exercise reasonable care in protecting the User  
17 Information of Plaintiff and the class by failing to implement and maintain adequate security  
18 measures to safeguard its users' User Information, failing to monitor its systems to identify  
19 suspicious activity or act on identified suspicious activity, allowing unauthorized access to the  
20 personal information of Plaintiff and the class, and failing to encrypt or otherwise prevent  
21 unauthorized reading of such User Information.

22           101.    FACEBOOK breached its duty to timely notify Plaintiff and the class about the  
23 data breach. Additionally, FACEBOOK was, or should have been, aware of unauthorized  
24 access to its users' User Information as early as 2014.

25           102.    But for FACEBOOK's failure to implement and maintain adequate security  
26 measures to protect its users' personal User Information and failure to monitor its systems to  
27 identify suspicious activity or act on identified suspicious activity, the User Information of  
28

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP  
39 Mesa Street, Suite 201 – The Presidio  
San Francisco, CA 94129  
Telephone: (415) 398-0900

1 Plaintiff and members of the class would not have been stolen, and they would not be at a  
2 heightened risk of identity theft in the future.

3 103. FACEBOOK’s negligence was a substantial factor in causing harm to Plaintiff  
4 and members of the class.

5 104. As a direct and proximate result of FACEBOOK’s failure to exercise reasonable  
6 care and use commercially reasonable security measures, the User Information of current and  
7 former FACEBOOK users was accessed by unauthorized individuals who could use the  
8 information to commit identity fraud, medical fraud, or debit and credit card fraud. Plaintiff and  
9 the class face a heightened risk of identity theft in the future.

10 105. Plaintiff and members of the class have also suffered economic damages,  
11 including the purchase of credit monitoring services they would not have otherwise purchased.

12 106. Neither Plaintiff nor other members of the class contributed to the security  
13 breach, nor did they contribute to FACEBOOK’s employment of insufficient security measures  
14 to safeguard User Information.

15 107. Plaintiff and the class seek compensatory damages and punitive damages with  
16 interest, the costs of suit and attorneys’ fees, and other and further relief as this Court deems just  
17 and proper.

18 **PRAYER FOR RELIEF**

19 WHEREFORE, Plaintiff, individually and on behalf of the proposed class, requests that  
20 the Court:

21 1. Certify this case as a class action on behalf of the class defined above, appoint  
22 Jonathan D. Rubin as class representative, and appoint Phillips, Erlewine, Given & Carlin LLP  
23 and Nicholas A. Carlin as class counsel;

24 2. Award declaratory, injunctive and other equitable relief as is necessary to protect  
25 the interests of Plaintiff and other class members;

26 3. Award restitution and damages to Plaintiff and class members in an amount to be  
27 determined at trial;

28



- 1           4.       Award Plaintiff and class members their reasonable litigation expenses, costs,
- 2 and attorneys' fees;
- 3           5.       Award Plaintiff and class members treble damages under 18 U.S.C. § 1964(c);
- 4           6.       Award Plaintiff and class members pre- and post-judgment interest, to the extent
- 5 allowable; and
- 6           7.       Award such other and further relief as equity and justice may require.

8 Dated: March 26, 2018

PHILLIPS, ERLEWIN, GIVEN & CARLIN LLP

10 By: /s/ Nicholas A. Carlin  
 11       Nicholas A. Carlin  
 12       Brian S. Conlon  
 13       Attorneys for Plaintiff

14 **JURY DEMAND**

15 Plaintiff hereby demands a jury trial on all issues so triable.

17 Dated: March 26, 2018

PHILLIPS, ERLEWIN, GIVEN & CARLIN LLP

19 By: /s/ Nicholas A. Carlin  
 20       Nicholas A. Carlin  
 21       Brian S. Conlon  
 22       Attorneys for Plaintiff

PHILLIPS, ERLEWIN, GIVEN & CARLIN LLP  
 39 Mesa Street, Suite 201 – The Presidio  
 San Francisco, CA 94129  
 Telephone: (415) 398-0900