EFiled: Apr 25 2018 12:41PM EDT
Transaction ID 61956909
Case No. 2018-0307-

IN THE COURT OF CHANCERY OF THE STATE OF DELAWARE

KAREN SBRIGLIO, derivatively on behalf of Nominal Defendant FACEBOOK, INC.,	:	
Plaintiff,	:	
v.	:	C. A. No.
MARK ZUCKERBERG, SHERYL SANDBERG, MARC ANDREESSEN, ERSKINE B. BOWLES, SUSAN DESMOND-HELLMANN, REED HASTINGS, JAN KOUM, PETER A. THIEL,	:	
Defendants,	:	
- and –	:	
FACEBOOK, INC.,	:	
Nominal Defendant.	:	

VERIFIED STOCKHOLDER DERIVATIVE COMPLAINT

Of Counsel:

Catherine Pratsinakis (Del. Id. 4820)
DILWORTH PAXSON LLP
1500 Market Street, Suite 3500E
Philadelphia, PA 19102
(215) 575-7013 (telephone)
cpratsinakis@dilworthlaw.com

Thaddeus J. Weaver (Del. Id. 2790)
DILWORTH PAXSON LLP
One Customs House
704 King Street, Suite 500
Wilmington, DE 19801
(302) 571-8867 (telephone)
tweaver@dilworthlaw.com

Counsel for Plaintiff Karen Sbriglio

TABLE OF CONTENTS

Plaintiff Karen Sbriglio (the "Plaintiff") derivatively on behalf of nominal defendant Facebook, Inc. ("Facebook" or the "Company"), brings the following Verified Derivative Complaint against Facebook's Chief Executive Officer ("CEO") and Chairman of its board Mark Zuckerberg ("Zuckerberg"), Chief Operating Officer ("COO") and director Sheryl Sandberg ("Sandberg"), and directors Marc Andreessen ("Andreesen"), Erskine S. Bowles ("Bowles"), Susan Desmond-Hellmann ("Desmond"), Reed Hastings ("Hastings"), Jan Koum ("Koum"), and Peter Thiel ("Thiel"), for breaching fiduciary duties that they owed to the Company and its shareholders. Except for the allegations specifically pertaining to Plaintiff and Plaintiff's own acts, the allegations in this Complaint are based on information and belief, which include but are not limited to the Company's public filings with the United States Securities and Exchange Commission ("SEC"), media reports, and other public sources.

SUMMARY OF THE ACTION

1. This is a derivative suit brought on behalf of Facebook to address the outrageous realization that for over a decade Facebook, under Zuckerberg's control, did not regard users' rights to privacy or Facebook's legal obligations when it allowed third parties repeated unauthorized access to tens of millions of Facebook users' private data. This complete and utter failure of leadership and governance left Facebook subject to public scrutiny, billions of dollars in lost

market value, millions of dollars in foreseeable fines and costs, and inquiries by governments worldwide. Zuckerberg's initial response to these revelations was to hide.

2. Facebook controls and is legally obligated to protect the personal data of over 2.2 billion people worldwide. Facebook's legal obligation to protect billions of users' data arises in part from (a) consumer and privacy laws in the United States, the European Union and other countries around the world; (b) its certification to comply with the Privacy Shield Frameworks (defined below); (c) its Facebook user agreements; (d) its policies on data security and user privacy; and (e) a consent decree that Facebook entered with the U.S. Federal Trade Commission ("FTC") in November 2011 (the "Consent Decree") (1) identifying the weaknesses in Facebook's data security infrastructure, (2) requiring Facebook to monitor third parties granted access to Facebook users' data and how that data is used, (3) requiring Facebook to obtain informed consent from users regarding what entities Facebook allows to access user data and for what purposes such data may be used, and (4) notifying the FTC of any violation of the Consent Decree.

3. From 2007 to present, certain officers and directors, *i.e.*, Defendants in this case, allowed Facebook to adopt an aggressive, high-speed growth and business model without the appropriate data security infrastructure in place to ensure that the Company complied with its legal obligations and the terms of its

user agreements. Employing lax controls and providing open access to thousands of third parties willing to pay for data led to what has quickly become one of the most infamous social media security breaches in history.

4. Specifically, on March 17, 2018, news reporting revealed that a firm called Cambridge Analytica had illegally harvested and improperly retained the personal data of 50 million Facebook users without meaningful disclosures to or permissions from these users. Facebook later determined that another 37 million Facebook user accounts were harvested for a total of 87 million users impacted.

5. The sheer size of the data breach was significant, but the more striking (and horrifying) aspect was how Cambridge Analytica used the data obtained illegally to manipulate users and influence both voter behavior and elections around the world.

6. In 2014, Cambridge Analytica used data obtained from Facebook users' accounts and activities to build a system that could profile U.S. voters and then target those individuals with personalized political advertisements.

7. Defendants knew about this improper access and use of Facebook users' data in 2015, if not earlier, but their response was a clear abrogation of their duties to the Company and its shareholders. Defendants failed to notify the FTC though they were required to do so, took nearly no action to protect or retrieve the illegally harvested data of millions of Facebook users and decided *not* to notify

impacted users in hopes of avoiding public ire and accountability. Informing users about the size and scope of the Cambridge Analytica problem would have been tantamount to admitting that Facebook's policies and infrastructure with respect to user privacy and data security were woefully deficient and that the Company had breached laws and legal obligations in various jurisdictions. To avoid exposure of its failed processes, Defendants quietly asked Cambridge Analytica to certify in writing that it had destroyed the illegally harvested data.

8. In the days following the revelation of the Cambridge Analytica data breach in March 2018, the public learned about the scope of the breach, the shocking manner in which user data was employed for the purpose of manipulating election results, the material weaknesses in Facebook's infrastructure and laxness in its oversight policies, and the hard reality that the problem did not begin nor end with Cambridge Analytica.

9. Since at least 2007, Facebook has allowed thousands of third party developers to access millions of users' data and to use this highly personal and private data for purposes not disclosed to users or monitored by Facebook. It is clear that for over a decade Facebook, under Zuckerberg's leadership and control, did not prioritize its users' privacy and did not prevent developers and marketers from accessing and using sensitive, personal data.

10. As the nuances of this scandal unfolded, Facebook lost ***over $100 billion in market capitalization*** in a period of days. Facebook's data security infrastructure and business practices are now under scrutiny by government regulators in the United States, the United Kingdom, the European Union, Canada, and Israel, all seeking information and/or testimony from Zuckerberg. To date, New York, New Jersey, Massachusetts, and Oregon also have launched investigations into Facebook's conduct.

11. Significantly, on March 19, 2018, the FTC announced that it would investigate whether and how often Facebook violated the November 2011 Consent Decree governing privacy issues related to the Cambridge Analytica data breach. The Consent Decree provides for a penalty of $40,000 per day per violation. Depending on the outcome of the FTC's investigation, Facebook faces astronomical fines based on the scope, length, and number of violations.

12. Defendants, as Facebook's officers and/or directors, breached their fiduciary duties when they consciously disregarded the known and systemic weaknesses in their infrastructure and systems which, by their design, were geared towards violating Facebook's legal obligation to protect and secure user privacy and data. Defendants failed to ensure the implementation of a reasonable monitoring system required by the FTC's Consent Decree to monitor developers' and other third parties' access to and use of Facebook users' data. Moreover, the

Board consciously disregard the Company's legal obligation to advise the impacted users of the breaches in how their data was obtained and used.

13. Facebook's data security systems were so weak that one Facebook operations manager described the "main enforcement mechanism" employed with respect to vendors and developers who accessed user data as to "call them and yell at them," and only when someone complained.

14. Defendants did not devise or design a secure infrastructure to control which entities accessed Facebook users' data and how they used the data, and to meaningfully provide users with that information. Now that the Cambridge Analytica data breach is public, the Board is contemplating enforcement protocols, as well as strategies for retrieving illegally harvested data from Cambridge Analytica and the thousands of other developers who had open access for a decade. Only now, with the world watching, will Defendants identify and inform impacted Facebook users.

15. Defendants knew through multiple privacy and data incidences, well-documented internal and external reports, and the result of an FTC investigation, that: (a) third parties illegally accessed more data than what was consented to or allowed contractually; (b) Facebook had no enforcement mechanism in place to monitor the use of that data; and (c) Facebook users did not give informed consent to such use because they did not appreciate the number of developers accessing

their data, the scope of the data they were accessing (*i.e.*, their friends' data), or how their data would be used. Facebook users were also misled into believing that privacy and data security were priorities at Facebook, which was patently false.

16. Defendants are under a substantial threat of personal liability on the breach of fiduciary duty claims raised herein given (a) the gravity, frequency, and scope of the repeated data breaches (Cambridge Analytica and many others); (b) the number of users impacted (likely all individuals who have had a Facebook account at any time since 2007); (c) the lack of sufficient infrastructure to monitor and enforce Facebook's policies and terms of its agreements with third-party developers; (d) the failure to sufficiently monitor and enforce Facebook's compliance with its legal obligations for a period of ten years; (e) numerous instances where Facebook failed to comply with laws and its obligations to protect data and how it was used; and (f) the failure to provide users meaningful disclosures so that they could provide informed consent.

17. Moreover, demand is excused because Facebook is controlled and dominated by Zuckerberg who, as of the end of 2017, controlled 60% of the shareholder vote, though he owned only 16% of outstanding shares. Zuckerberg personally selects and may remove any director on Facebook's Board. He sets the business strategy and makes all key business decisions including his philosophy over the last ten years to "Move fast and break things." Additionally, Zuckerberg

provides members of the Board (*i.e.*, Defendants) access to investment opportunities that have made some of them among the wealthiest individuals in the world.

18. The majority of the Board is also incapable of exercising impartial judgment as several Board members face a substantial threat of personal liability. Members of the Board had detailed knowledge through multiple well-publicized reports of data security problems and misappropriation of Facebook's user data. Defendants knew of the Company's obligations under the Consent Decree and knew in 2015 about the Cambridge Analytica debacle, among many other data breaches. Yet, they disregarded the fact that Facebook did not have the infrastructure in place to secure user privacy or data, and they consciously disregarded the fact that Facebook was not monitoring data use, nor giving users sufficient information so that they could provide informed consent. Then, instead of notifying the impacted users of the Cambridge Analytica data breach, they concealed it. Plaintiff, therefore, respectfully requests that the Court excuse demand.

JURISDICTION AND VENUE

19. This Court has jurisdiction over this action pursuant to 10 Del. C. § 341 and 8 Del. C. § 111.

20. As directors of a Delaware corporation, Defendants have consented to the jurisdiction of this Court pursuant to 10 Del. C. § 3114.

21. This Court has jurisdiction over Facebook pursuant to 10 Del. C. § 3111.

22. The proper venue for this action is in the Court of Chancery pursuant to Article IX of Facebook's Restated Certificate of Incorporation, which states in relevant part as follows:

> Unless the corporation consents in writing to the selection of an alternative forum, the Court of Chancery of the State of Delaware shall, to the fullest extent permitted by law, be the sole and exclusive forum for (1) any derivative action or proceeding brought on behalf of the corporation, (2) any action asserting a claim of breach of a fiduciary duty owed by, or other wrongdoing by, any director, officer, employee or agent of the corporation to the corporation or the corporation's stockholders, ….

PARTIES

23. Plaintiff Karen Sbriglio owns and has owned shares of Facebook, Inc. common stock throughout the relevant period.

24. Nominal Defendant Facebook, Inc. is a corporation organized and existing under the laws of the State of Delaware, with its principal place of business at 1601 Willow Road, Menlo Park, California 94025, and its registered agent, pursuant to 8 Del. C. § 131- *et al.*, at Corporation Service Company located at 251 Little Falls Drive, Wilmington, DE 19808. Facebook operates a social networking website that allows people to communicate with their family, friends,

and coworkers. Facebook develops technologies that facilitate the sharing of information, photographs, website links, and videos. At the end of 2017, Facebook had more than 2.2 billion active users. The Company's stated 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." Facebook's securities trade on the NASDAQ under the ticker symbol "FB."

25. Defendant Zuckerberg is the founder of the Company and has served as the Company's CEO and as a member of the Board since July 2004, and as Chairman of the Board since January 2012. Zuckerberg is responsible for Facebook's day-to-day operations, as well as the overall direction and product strategy of the Company. He is also the Company's controlling stockholder with ownership of stock and proxies for stock representing more than 60% of Facebook's voting power, though he owns only 16% of Facebook's total equity.

26. Defendant Sheryl Sandberg ("Sandberg") has been the Company's Chief Operating Officer ("COO") since March 2008 and a member of the Board since June 2012. Sandberg served in various positions at Google, Inc. (now known as Alphabet, Inc.) from November 2001 to March 2008, most recently as Vice President, Global Online Sales & Operations. Sandberg has been a director of

online survey development cloud-based software company SurveyMonkey since July 2015.

27. Defendant Marc Andreessen has been a member of the Board since June 2008. Andreessen is a general partner of venture capital firm Andreessen Horowitz, which he co-founded in July 2009. Andreessen also co-founded, and was chairman of the board of software company Opsware, Inc. (formerly known as Loudcloud Inc.). He also served as Chief Technology Officer of America Online, Inc., an Internet services company. Andreessen was co-founder of Netscape Communications Corporation, a software company, serving in various positions, including Chief Technology Officer and Executive Vice President of Products. Andreessen also serves on the boards of Hewlett-Packard Enterprise Company and several private companies. Andreessen previously served as a member of the board of eBay Inc.

28. Defendant Erskine B. Bowles ("Bowles") has been a member of the Board since September 2011. Bowles is a politician who, among other appointments, served as President Bill Clinton's Chief of Staff from 1996 to 1998. In addition to Facebook's Board, Bowles currently serves on the board of Norfolk Southern Corporation, a position he has held since February 2011. Bowles also served on the board of General Motors Company from June 2005 to April 2009, Cousins Properties Incorporated from August 2003 to May 2012, Belk, Inc. from

May 2011 to November 2015, and Morgan Stanley from December 2005 to February 2018. Bowles has also been associated with a series of venture capital firms. He been a Senior Advisor and non-executive vice chairman of BDT Capital Partners, LLC, a private investment firm, since January 2012. Bowles was Managing Director of Carousel Capital LLC, a private investment firm, from 1999 to 2001, and was a Senior Advisor for the firm from 2001 to 2015. He was also a partner of Forstmann Little & Co., an investment firm, from 1999 to 2001. He also founded venture capital firm Kitty Hawk Capital.

29. Defendant Susan Desmond-Hellmann ("Desmond-Hellman") has been a member of the Board since March 2013. Desmond-Hellmann is currently the CEO of the Bill & Melinda Gates Foundation, the largest private foundation in the world, with aims to enhance healthcare and reduce extreme poverty, and in America, to expand educational opportunities and access to information technology.

30. Defendant Reed Hastings ("Hastings") has been a member of the Board since June 2011. Hastings has served as CEO and Chairman of Netflix, Inc., a provider of Internet subscription service for movies and television shows, since 1999. Hastings previously served on the board of Microsoft Corporation.

31. Defendant Jan Koum ("Koum") has been a member of the Board since October 2014. Since February 2009, Koum has served as co-founder and

CEO of WhatsApp Inc. ("WhatsApp"), a cross-platform mobile messaging application company and Facebook's wholly-owned subsidiary.

32. Defendant Peter A. Thiel ("Thiel") has been a member of the Board since April 2005. Thiel has served as President of Thiel Capital, an investment firm, since 2011, has been a partner of Founders Fund, a venture capital firm, since 2005, and has served as President of Clarium Capital Management, a global macro investment manager, since 2002. Thiel was one of Facebook's, and Zuckerberg's, early venture capital backers. In 1998, Thiel co-founded PayPal, Inc., an online payment company, where he served as CEO, President and Chairman from 2000 until its acquisition by eBay in 2002.

33. As directors and/or officers of the Company, Defendants Zuckerberg, Sandberg, Andreessen, Bowles, Desmond-Hellmann, Hastings, Koum and Thiel (collectively, "Defendants"), are in a fiduciary relationship with the Company, Plaintiff, and the public stockholders of Facebook, and owe the highest obligations of due care, loyalty, and good faith and fair dealing.

34. Non-party Kenneth I. Chenault ("Chenault") joined Facebook's Board in February 2018 and is not a party to this action. Mr. Chenault is Chairman and a Managing Director at General Catalyst, a venture capital firm, that makes early-stage and growth equity investments in technology companies such as AirBnB, Stripe, and Snapchat. Prior to joining General Catalyst, Mr. Chenault was

Chairman and Chief Executive Officer of American Express Company, a position he held from 2001 to 2018.

35. Non-party Cambridge Analytica is a British political consulting firm which combines data mining, data brokerage, and data analysis with strategic communication to influence voter behavior. It was incorporated in Canary Wharf, London as "SCL USA Limited" in January 2015, as a subsidiary of its American parent company SCL Group. In April 2016, it changed its name to Cambridge Analytica (UK) Limited. Cambridge Analytica maintains offices in London, New York City, and Washington, D.C.

DEFENDANTS' OBLIGATIONS AS OFFICERS AND DIRECTORS OF FACEBOOK

36. By reason of their positions as officers and directors of Facebook and because of their ability to control the business, corporate, and financial affairs of the Company, Defendants owed Facebook and its shareholders the duty to exercise due care and diligence in the management and administration of the affairs of the Company, including taking appropriate, affirmative measures to halt practices that they knew were illegal and/or noncompliant with the Consent Decree, and to ensure that all policies and practices complied with applicable federal and state laws, rules and regulations.

37. Defendants were and are required to act in furtherance of the best interests of Facebook and its stockholders so as to benefit all stockholders equally and not in furtherance of Defendants' personal interest or benefit.

38. Each Director and officer owes Facebook and its stockholders the fiduciary duty to exercise good faith and diligence in the use and preservation of the Company's property and assets, and act in compliance with the highest obligations of fair dealing.

39. Because of their positions of control and authority as directors and officers of Facebook, Defendants were able to and did, directly and indirectly, exercise control over the wrongful acts detailed in the Complaint. By virtue of such duties, the officers and directors of Facebook were required to, among other things:

(a) manage, conduct, supervise, and direct the employees, businesses, and affairs of Facebook in accordance with laws, rules, and regulations, as well as the charter and bylaws of Facebook;

(b) ensure that Facebook did not engage in imprudent or unlawful practices and that the Company complied with all applicable laws and regulations;

(c) remain informed as to how Facebook was, in fact, operating, and, upon receiving notice or information of imprudent or unsound practices, to take reasonable corrective and preventative actions, including maintaining and implementing adequate financial and operational controls;

(d) supervise the preparation, filing, or dissemination of any SEC filings, press releases, audits, reports, or other information disseminated by Facebook, and to examine and evaluate any reports of examinations or investigations concerning the practices, products, or conduct of officers of the Company;

(e) preserve and enhance Facebook's reputation as befits a public corporation; and

(f) exercise good faith to ensure that the affairs of the Company were conducted in an efficient, business-like manner so as to make it possible to provide the highest quality performance of its business.

40. Because of their advisory, executive, managerial, and directorial positions with the Company, Defendants had access to adverse, non-public information about the Company.

41. Defendants, because of their positions of control and authority, were able to and did, directly or indirectly, exercise control over the wrongful acts complained of herein, as well as the contents of the various public statements issued by Facebook.

42. In addition, the Board was solely responsible for risk management of known risks and compliance issues (such as privacy and data security). According to Facebook's preliminary proxy statement, filed with the Securities and Exchange Commission ("SEC") on or about April 14, 2017 (the "2017 Proxy Statement"):

> Our board of directors as a whole has responsibility for overseeing our risk management. The board of directors exercises this oversight responsibility directly and through its committees. The oversight responsibility of the board of directors and its committees is informed by reports from our management team and from our internal audit department that are designed to provide visibility to the board of directors about the identification and assessment of key risks and our risk mitigation strategies.
>
> The full board of directors has primary responsibility for evaluating strategic and operational risk management, and for CEO succession planning. Our audit committee has the responsibility for overseeing our major financial and accounting risk exposures as well as legal and regulatory risk exposures. Our audit committee also oversees the steps our management has taken to monitor and control these exposures, including policies and procedures for assessing and managing risk and related compliance efforts. Finally, our audit committee oversees our internal audit function. Our compensation & governance committee evaluates risks arising from our compensation policies and practices, as more fully described in "Executive Compensation—Compensation Discussion and Analysis— Compensation Risk Assessment." The audit committee and the compensation & governance committee provide reports to the full board of directors regarding these and other matters.

FACEBOOK'S LEGAL OBLIGATIONS TO PROTECT USER PRIVACY AND DATA SECURITY

43. Facebook's users are located all over the world, and, as such, Facebook operates in every country and must comply or, at a minimum, attempt to comply with the consumer and privacy laws and regulations around the globe.

44. According to Facebook's Form 10-K for the period ending December 31, 2017, filed on February 1, 2018 ("2017 Form 10-K"):

> We are subject to a number of U.S. federal and state and foreign laws and regulations that affect companies conducting business on the Internet. Many of these laws and regulations are still evolving and being tested in courts, and could be interpreted in ways that could harm our business. These may involve ***user privacy, data protection and personal information***, rights of publicity, content, intellectual property, advertising, marketing, distribution, ***data security, data retention and deletion***, electronic contracts and other communications, competition, protection of minors, consumer protection, telecommunications, product liability, taxation, economic or other trade prohibitions or sanctions, securities law compliance, and online payment services. ***In particular, we are subject to federal, state, and foreign laws regarding privacy and protection of people's data. Foreign data protection, privacy, content, competition, and other laws and regulations can be more restrictive than those in the United States.*** (Emphasis added.)

45. Facebook also made numerous privacy and data security commitments to abide with its certification to the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework (collectively, "Privacy Shield Frameworks") with the U.S. Department of Commerce regarding the collection and processing of personal data.

46. For example, the Privacy Shield Principles which were updated by the European Union in April 2016, provide in part:

> Informed consent means that you must be given information about the processing of your personal data, including at least:

> the identity of the organisation processing data;
>
> the purposes for which the data is being processed;
>
> the type of data that will be processed;
>
> the possibility to withdraw consent (for example by sending an email to withdraw consent);
>
> where applicable, the fact that the data will be used solely for automated-based decision-making, including profiling; . . . .

47. As noted in Facebook's 2017 Form 10-K:

> Facebook is ***liable for any processing of personal data by such third parties that is inconsistent with the Privacy Shield Principles*** unless Facebook was not responsible for the event giving rise to any alleged damage. (Emphasis added.)

48. In addition, Facebook's 2017 Form 10-K provides:

> We are currently, and may in the future be, subject to regulatory orders or consent decrees. Violation of existing or future regulatory orders or consent decrees could subject us to substantial monetary fines and other penalties that could negatively affect our financial condition and results of operations.

49. One such consent decree involves the consent decree reached between Facebook and the FTC in November 2011 in settlement of a multi-count complaint that Facebook was mishandling its users' data, committing privacy violations, and failing to secure its data ("Consent Decree"). *See infra,* Section VIII.B. As part of the Consent Decree, Facebook promised to end existing practices relating to

controls over data access and the transfer of information to third parties without Facebook users' consent.

50. In addition to its obligations under the Privacy Shield Principles and the Consent Decree, and other privacy and consumer laws around the world, Facebook also had obligations to its users *vis-a-vis* its user agreements, which states in relevant part:

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

51. Facebook's Privacy Policy states that its users "have control over who sees what you share on Facebook" and sets forth the following privacy tenets:

a. We give you control of your privacy.

b. We help people understand how their data is used.

c. We design privacy into our products from the outset.

d. We work hard to keep your information secure.

e. We work around the clock to help protect people's accounts, and we build security into every Facebook product.

f. You own and can delete your information.

g. Improvement is constant.

h. We are accountable.

52. Moreover, Facebook's Data Use Policy, last revised in 2013, states in part as follows:

> 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.

See Facebook's website, https://www.facebook.com/full_data_use_policy (last visited 3/21/2018).

53. As a result of the above, Facebook had and continues to have numerous legal obligations to: (a) protect users' privacy, (b) secure users' data, (c) secure users' permission before sharing data, and (d) monitor third parties' access and use of data.

FACTUAL ALLEGATIONS

A. The Cambridge Analytica Scandal Exposes Facebook's Weak Infrastructure, Lack of Monitoring and Enforcement and Failure To Comply With Legal Obligations Related to User Privacy, Data Security and Data Use

54. In December 2015, *The Guardian* revealed that Cambridge Analytica illegally harvested Facebook user data to aid Senator Ted Cruz in his bid for president. Cambridge Analytica, a political consulting firm, used Facebook's data to impact the electoral process and outcome of elections of high-paying political candidates.

55. A Facebook representative claimed that the Company was "carefully investigating this situation" and that "misleading people or misusing their 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."

56. Yet, after the Company's investigation into Cambridge Analytica's misappropriation of Facebook's user data, Defendants did not report the scope of the illegal harvesting to the victimized Facebook users. Instead, they asked Cambridge Analytica to sign a legal certification promising that it had destroyed the misappropriated user data. But, they did nothing to verify Cambridge Analytica's compliance with that certification.

57. Despite this and other warnings, Facebook did not materially change its standard business practices. Even after Defendants discovered Cambridge Analytica's misconduct, Defendants continued to allow third parties to access Facebook's servers and disregarded what data was being mined and how it would be used.

58. On March 17, 2018, *The New York Times* and the *Observer* revealed that Cambridge Analytica illegally harvested the private information of tens of millions of Facebook users without notice to the Company or consent of Facebook users. According to *The New York Times*:

> [T]he firm harvested private information from the Facebook profiles of more than 50 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.

59. It was discovered that, as of the latest count, Cambridge Analytica had illegally accessed and retained information of 87 million user accounts without informed consent.

60. According to *The Observer*, a whistleblower had revealed that Cambridge Analytica relied on Facebook users' personal information in early 2014 to build a system that could profile U.S. voters and target those individuals with personalized political advertisements.

61. Whistleblower Christopher Wylie ("Wylie"), a Canadian data analytics expert, worked with Cambridge Analytica and Cambridge research professor Dr. Aleksandr Kogan ("Kogan") to devise and implement their political motives. Wylie told The Observer:

> We exploited Facebook to harvest millions of people's profiles. And built models to exploit what we knew about them and target their inner demons. That was the basis the entire company was built on.

62. The user data was collected through an application ("app") called "thisismydigitallife" designed by Kogan and his company, Global Science Research ("GSR").

63. GSR, in collaboration with Cambridge Analytica, convinced Facebook users to open the "thisismydigitallife" app and take a personality test under the guise that GSR was collecting the data for academic purposes.

64. The app's disclosures informed users that it was a "research app used by psychologists," designed by a Cambridge academic, and would give users a better understanding of their own personalities. Based on these false and misleading disclosures, an estimated 270,000 Facebook users downloaded the app

using their Facebook login credentials, which, under Facebook's developer platform, allowed Kogan and Cambridge Analytica access backdoor access to these users' personal data and the data of their friends.

65. According to *The New York Times*, Wylie's access to this volume of data was "the saving grace" that allowed his team to develop statistical models to predict and influence political views and behavior. Facebook "contained enough information, including places of residence, that [Cambridge Analytica] could match users to other records and build psychographic profiles." According to Wylie:

> 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.

66. According to *The New York Times*, Wylie claimed to have receipts, invoices, emails, legal letters and records that showed how, between June and August 2014, the profiles of more than 50 million Facebook users had been illegally harvested. And, of the 50 million Facebook users victimized by this scheme, "[o]nly about 270,000 users — those who participated in the survey — had consented to having their data harvested."

67. None of the Facebook users whose data had been collected by Cambridge Analytica consented to having their personal data used for political or commercial purposes.

68. Despite this lack of consent, Cambridge Analytica used this data obtained under false pretense to provide strategic advice to 44 political campaigns in 2014, including Senator Ted Cruz's presidential campaign in 2015, Donald Trump's presidential campaign in 2016, and the 2016 Leave.EU-campaign (known as "Brexit") related to a referendum on the United Kingdom's withdrawal from the European Union.

69. As reported by *The Observer* and confirmed by Facebook in recent statements, the Company's management learned as early as 2015 that Kogan violated Facebook's platform policies, including those relating to its developer application programming interface ("API"), but did not inform the millions of affected users or make any reasonable and meaningful effort to recover and secure the private information of the impacted users.

70. Instead, Facebook's management asked Cambridge Analytica to sign a certification stating that it had destroyed Facebook users' data. Meanwhile, copies of the data harvested by Cambridge Analytica were still circulating and located online as recently as 2017.

71. The problem, however, is much larger than one third-party developer, like Cambridge Analytica. According to Zuckerberg, Facebook is now auditing tens of thousands similar app developers who likely also exploited Facebook's lax

oversight of user privacy and data security in these app developers collection and use of Facebook's user data.

72. In the wake of the Cambridge Analytica scandal, Facebook's policies and practices with respect to privacy and data security are under investigation in the United States, the United Kingdom, the European Union, Canada, and Israel. Most if not all of these governments have expressed their intentions to interrogate Zuckerberg. State governments, including New York, New Jersey, Massachusetts, and Oregon, have also launched probes into Facebook's conduct.

73. On March 19, 2018, the FTC launched an investigation into whether Facebook violated terms of the Consent Decree that the agency entered into with the Company in 2011. Evidently, Facebook failed to adhere to a key term in the Consent Decree - that it "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." If the FTC finds that Facebook violated terms of the Consent Decree, the FTC will have the power to fine Facebook more than "$40,000 a day per violation," or trillions of dollars in fines given the number of user accounts impacted.

B. Defendants Knew Facebook Had Violated the Law and Consciously Disregarded their Duty to (A) Monitor User Privacy and Data Security; (B) Enforce Data Use Policy; and (C) Notify Users of Known Data Breaches and Data Misuse

74. Throughout its history, Facebook has been embroiled in controversy over data security concerns and its failure to protect users' information.

75. Defendants knew through numerous red flags, including lawsuits, internal and external reports, and by their own admission that Facebook was not complying with laws, the FTC Consent Decree, nor its legal obligations to users to ensure their privacy and the security of their data.

76. Facebook's controls and systems were woefully inadequate to monitor and enforce its policies and legal obligations relating to user privacy, data security and data use because:

(a) ***first***, until just recently, Facebook did not review or audit third parties to determine what data they were collecting and how they were using the data, essentially running a multibillion company on the honor system;

(b) ***second***, Defendants knew that Facebook users were not aware of the scope or amount of personal data being collected on each them (such as "scraping" information, *i.e.*, data extraction using software, about users' friends or private direct messages sent in between users), nor were they advised of who was accessing their data, for what purpose and how their data would be used.

(c) ***third***, Defendants had a policy and/or practice of not notifying impacted users of known privacy breaches or data misuse, which again highlights the flippant view Defendants had towards protecting users and their data.

77. For far too long the misappropriation and exploitation by third parties of user data entrusted to Facebook had been met with negligible response.

1. Defendants Were on Notice of Facebook's Failure to Protect User Privacy, Secure Data and Monitor Data Use

78. In 2009, Facebook began making users' posts, which had previously been private, public by default. That incident triggered anger, confusion, an investigation that ultimately led to the FTC action and Consent Decree described herein.

79. In 2009, the Canadian Internet Policy and Public Interest Clinic ("CIPPIC") filed a complaint against Facebook alleging 12 distinct data privacy issues, including default privacy settings, collection and use of users' personal information for advertising purposes, disclosure of users' personal information to third-party application developers, and collection and use of non-users' personal information. In August 2009, the Office of the Privacy Commissioner of Canada which had addressed the CIPPIC's complaint reached a resolution with Facebook. In particular, with respect to third-party application developers, the resolution was as follows:

> I am pleased that Facebook reconsidered my recommendations with respect to improving consent and safeguards around third-party application developers' access to users' personal information. I was concerned about open access by developers to users' personal information and recommended that Facebook introduce technical measures to limit access.
>
> Facebook has agreed to adopt such measures and will be implementing significant changes to its site (namely, retrofitting its API) in order to give its users granular control over what personal information developers may access and for what purposes. Facebook plans to introduce a permissions-based model whereby the user can choose what information she wants to share with that particular application. There will also be a link to a statement by the developer explaining how it will use the data. Currently, other than a user choosing to opt out of the Facebook API altogether, there is no way a user can choose what information is shared with all applications.
>
> As for friends' data, a user can now choose if they want to share their friends' data with a particular application. The application will only be able to access the information the friend is already sharing with the user. Friends can limit the information they share with their friends, de-friend someone, block all applications, block specific applications or block certain information through their application privacy settings. Facebook has also agreed to add information to explain the new permissions model so that users will know what happens when their friends add applications and can take steps to limit their data should they wish to.
>
> * * *
>
> Facebook has committed to using its best efforts to roll out the permissions model by September 1, 2010. In the meantime, Facebook will oversee the applications developers' compliance with contractual obligations.

80. In March 2010, Facebook settled a class action for $9.5 million to resolve claims regarding its Beacon feature, which tracked what users buy online

and shared the information with their friends. Reflecting on Beacon, Zuckerberg attributed part of Facebook's success to giving "people control over what and how they share information." He said that he regretted making Beacon an "opt-out system instead of opt-in ... if someone forgot to decline to share something, Beacon went ahead and still shared it with their friends."

81. In 2010, the *Wall Street Journal* reported that online tracking firm RapLeaf Inc. used Facebook data to build databases of personal user information and sold the data to political advertisers and other commercial entities.

82. In 2011, Facebook users complained to the Company that some of their old profile data was inexplicably posted for anyone to view on a site called Profile Engine. The developer of that site had illegally collected 420 million user profiles, prompting another lawsuit against the Company.

83. In 2011, a social-media startup, Klout Inc., reportedly created profiles for minors using Facebook data, without the minors' knowledge.

84. In December 2012, Facebook settled a class action for $20 million over claims it used subscribers' names without their permission to advertise products in its "Sponsored Stories."

85. According to *The Irish Times* in an article dated November 14, 2017, Max Schrems, an Austrian lawyer and privacy activist, reportedly told Ireland's data protection authority of loopholes in Facebook's policy that allowed apps to

"harvest" data about their friends without consent some time ago. "We flagged it in 2011," Schrems said. "Now it emerges that in 2014 Cambridge Analytica started doing precisely what we warned about three years earlier."

86. By 2013, 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 on the Company's website, 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.

87. On September 11, 2017, the Spanish government's Agency for Data Protection ("AEPD") announced that it was imposing a €1.2 million fine on

Facebook for violating data protection regulations following an agency investigation.

88. The AEPD stated that its investigation verified that Facebook does not disclose to users in a comprehensive and clear way the data that it collects and how that data is treated. Instead, Facebook's disclosures are limited to examples. In particular, the AEPD found that Facebook collects data derived from interaction by users on Facebook's platform and on third-party sites without users knowing exactly *what* information Facebook collects and for what purpose.

89. The AEPD also found that Facebook's privacy policy contains generic and unclear expressions, and requires users to access a multitude of different links to fully review. Further, the AEPD concluded that a Facebook user with an average working knowledge of modern technology and social media will not get an accurate understanding of how data is collected, stored, and treated from reading the Company's privacy policy.

90. In May 2017, the French data protection authority imposed the maximum allowable fine of €150,000 on Facebook for similar violations uncovered 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 l'Informatique et des

Libertés. “[Facebook] collected data on the browsing activity of internet users on third-party websites, via the ‘data’ cookie, without their knowledge.”

2. The FTC Complaint and Consent Decree

91. By the end of 2011, in an administrative action initiated before the Federal Trade Commission, the FTC alleged in an eight-count complaint that Facebook had violated the Federal Trade Commission Act (“FTC Act”) by engaging in unfair and deceptive practices over the collection and use of user data.

92. Specifically, the FTC alleged that in December 2009, Facebook changed its website so certain information that users may have designated as private – such as their Friends List – was made public. The Company did not warn users that this change was coming, or get their approval in advance.

93. The FTC alleged that Facebook represented to its users that third-party apps installed by users would have access only to user information that they needed to operate, when in fact “the apps could access nearly all of users’ personal data,” including data the apps did not need.

94. The FTC alleged that Facebook misrepresented to users that users could restrict sharing of data to limited audiences – for example, selecting “Friends Only” on a post did not prevent users’ information from being shared with third-party applications that their “friends” downloaded.

95. The FTC alleged that Facebook falsely claimed that it had a "Verified Apps" program and that Facebook certified the security of participating apps when it did not.

96. Facebook promised users that it would not share their personal information with advertisers when, according to the FTC, it did.

97. The FTC alleged that Facebook misrepresented that when users deactivated or deleted their accounts, their photos and videos would be inaccessible. Facebook continued to have access to the content, even after users deactivated or deleted their accounts.

98. The FTC alleged that Facebook failed to comply with the U.S.- EU Safe Harbor Framework that governs data transfer between the U.S. and the European Union.

99. In November 2011, Facebook settled the FTC's charges by entering into a Consent Decree that barred Facebook from making deceptive privacy claims, required Facebook to obtain users' approval before it changed its data sharing policies, and required Facebook to have its privacy practices reviewed periodically by independent, third-party auditors for twenty (20) years following its entry.

100. Specifically, under the Consent Decree, Facebook is:

a. barred from making misrepresentations about the privacy or security of users' personal information, including, the extent to which third parties collect and access user information, steps taken by Facebook to verify privacy or security protections of third parties and the extent to which information is available after users delete their accounts;

b. required to obtain a user's affirmative express consent before sharing private data and enacting changes that override his or her privacy preferences;

c. required to prevent anyone from accessing a user's material more than 30 days after the user has deleted his or her account;

d. required to establish and maintain a comprehensive privacy program designed to address privacy risks associated with the development and management of new and existing products and services and protect the privacy and confidentiality of consumers' information; and

e. design and implementation of reasonable controls and procedures to address the risks identified through a privacy risk assessment, and regular testing or monitoring of the effectiveness of those controls and procedures.

f. required, every two years for the next 20 years after entry of the consent order, to obtain independent, third-party audits certifying that it has a privacy program in place that meets or exceeds the requirements of the FTC order, and to ensure that the privacy of users' information is protected.

101. In the FTC's press release announcing the settlement and terms of the Consent Decree, issued November 29, 2011, then-FTC Chairman Jon Leibowitz stated that "Facebook is obligated to keep the promises about privacy that it makes to its hundreds of millions of users" and "Facebook's innovation does not have to come at the expense of consumer privacy." As officers and/or members of Facebook's Board, Defendants were aware of the Consent Decree and Facebook's obligations thereunder.

3. Reports from Facebook's Security and Operations Managers

102. In June 2015, Alex Stamos joined Facebook as its Chief Security Officer ("CSO"), and reported directly to Zuckerberg. According to reporting by *The New York Times*, Stamos got off on the wrong foot with some executives, including defendant Sandberg, over how best to police the platform. Stamos reportedly argued to management that Facebook needed to act more like a defense contractor in dealing with security, given that the social network was becoming a similar target for nation states.

103. In an audio recording leaked to ZDNet, a technology news site, in October 2017, Stamos told his team that he explained to Facebook management "that we have 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." The tape infuriated Zuckerberg and Sandberg, according to reports, and the Company's internal leak investigation is ongoing.

104. In early 2017, Stamos co-authored a "White Paper" titled "Information Operations and Facebook," which alerted readers, including Defendants, that Facebook's lax data security practices were pervasive and supported by management. The "White Paper" also confirmed that Defendants' public statements about its business practices, infrastructure and systems were false and misleading.

105. Upon information and belief, Stamos had initially provided a written report to Facebook executives concerning the circumstances which led to the Cambridge Analytica leak. Instead of disclosing the leak, the report was rewritten and presented as a hypothetical scenario, which appeared in the whitewashed "White Paper" that Facebook published on April 27, 2017, further suppressing and concealing the wrongdoing at the Company .

106. Stamos shared his concerns over Facebook's lack of user privacy vulnerabilities with Zuckerberg, but by December 2017, Stamos was reportedly relieved of his duties as CSO, though he was permitted to stay through August 2017 to avoid negative publicity.

107. According to *The Guardian* in a March 20, 2018 news article, Sandy Parakilas, a Facebook operations manager who policed data breaches by third party software developers between 2011 and 2012, also expressed his concerns.

108. Parakilas concluded that developers were collecting and exploiting the private information of hundreds of millions of Facebook users and warned senior executives at the Company that its lax approach to data protection risked a major breach.

109. "[Parakilas's] concerns were that all of the data that left Facebook servers to developers could not be monitored by Facebook, so [Facebook] had no idea what developers were doing with the data" and that the Company did not use enforcement mechanisms, including audits of third-party developers and their apps, to ensure data was not being misused.

110. Parakilas told *The Guardian* that 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. In Parakilas' own words, "***[Facebook] felt that it was better not to know,***" which he found to be "utterly shocking and horrifying."

111. On March 21, 2018, Parakilas 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.” 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.

4. Zuckerberg’s and Sandberg’s Apologies For Facebook’s Repeated Lapses in User Privacy and Data Security

112. The *Washington Post’s* article, “14 years of Mark Zuckerberg Saying Sorry, Not Sorry,” published on April 9, 2018, chronicled the Zuckerberg-Sandberg apology tour, in part, as follows:

113. As early as 2006, users protested that Facebook’s news feed feature was making public information that users had intended to keep private, exposing updates to friends in one central place. In response, Zuckerberg stated:

> “We really messed this one up. ... We did a bad job of explaining what the new features were and an even worse job of giving you control of them.”

114. In December 2007, after launching Beacon, which opted-in everyone to sharing with advertisers what they were doing in outside websites and apps**,** Zuckerberg stated:

> " We simply did a bad job with this release, and I apologize for it. ... People need to be able to explicitly choose what they share. "

115. In February 2009, after unveiling new terms of service that angered users, Zuckerberg stated:

> " Over the past couple of days, we received a lot of questions and comments. ... Based on this feedback, we have decided to return to our previous terms of use while we resolve the issues. "

116. In May 2010, after reporters found a privacy loophole allowing advertisers to access user identification, Zuckerberg stated:

> " Sometimes we move too fast. ... We will add privacy controls that are much simpler to use. We will also give you an easy way to turn off all third-party services. "

117. In November 2011, after Facebook reached a consent decree with the Federal Trade Commission for deceiving consumers about privacy, Zuckerberg stated:

> “ I’m the first to admit that we’ve made a bunch of mistakes. ... Facebook has always been committed to being transparent about the information you have stored with us – and we have led the internet in building tools to give people the ability to see and control what they share . ”

118. In July 2014, after an academic paper exposed that Facebook conducted psychological tests on nearly 700,000 users without their knowledge, Defendant Sandberg stated:

> “ It was poorly communicated. ... And for that communication we apologize . We never meant to upset you. ”

---

119. In December 2016, after criticism of the role of Facebook in spreading fake news about Republic and Democrat political candidates, Zuckerberg stated:

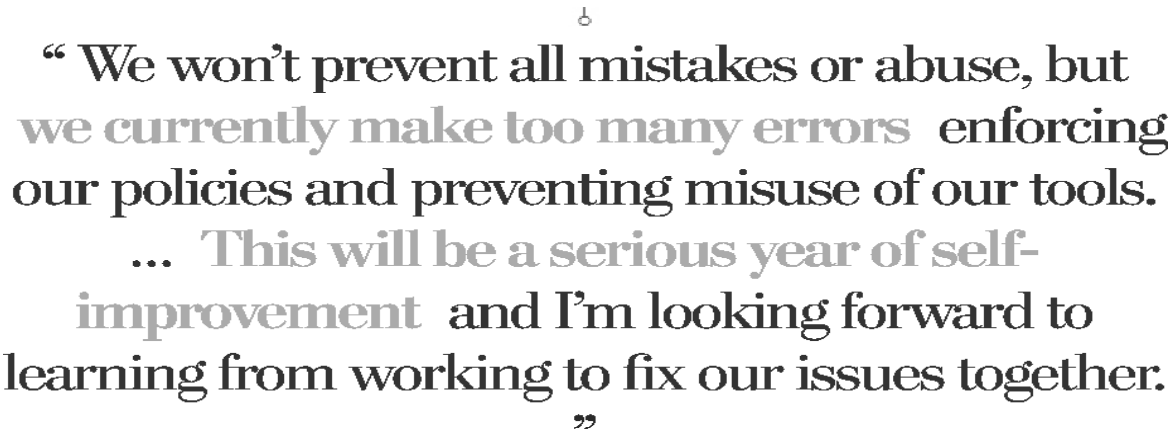
> " I think of Facebook as a technology company, but I recognize we have a greater responsibility than just building technology that information flows through. ... Today we're making it easier to report hoaxes. "

120. In September 2017, while revealing a nine-step plan to stop nations from using Facebook to interfere in one another's elections, noting that the amount of "problematic content" found so far is "relatively small."

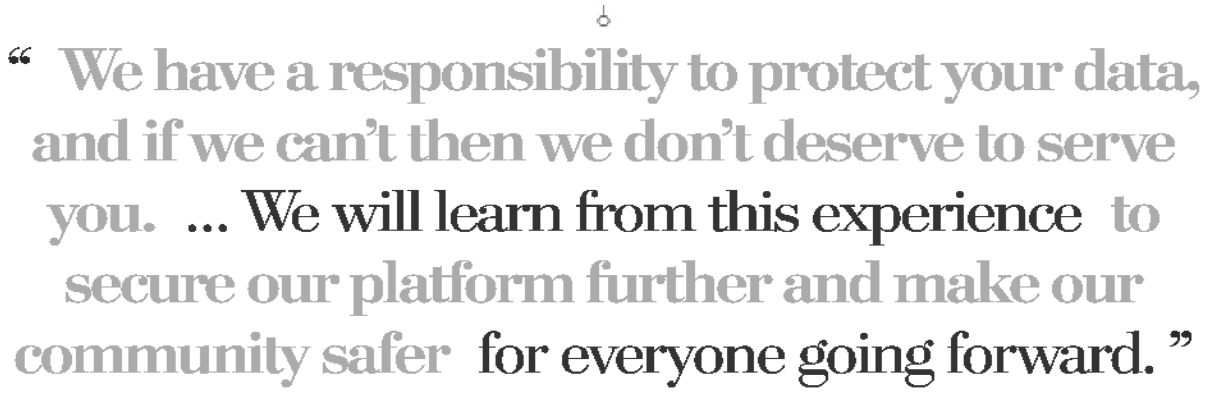
121. Then in September 2017, after continued criticism about the role of Facebook in Russian manipulation of the 2016 election, Zuckerberg stated:

> " For the ways my work has been used to divide rather than to bring us together, I ask for forgiveness and I will work to do better. "

122. In January 2018, announcing his personal challenge for the year is to fix Facebook, Zuckerberg stated:



123. In March 2018, after details emerged about Cambridge Analytica taking user data.



---

124. According to *The New York Times* article, “Mark Zuckerberg’s Reckoning: “‘This Is a Major Trust Issue,’” dated March 21, 2018, Zuckerberg stated in reaction to the breach of trust:

> One of our biggest responsibilities is to protect data. If you think about what our services are, at their most basic level, you put some content into a service, whether it’s a photo or a video or a text message - whether it’s Facebook or WhatsApp or Instagram - and you're trusting that that content is going to be shared with the people you want to share it with. Whenever there’s an issue where someone’s data gets passed to someone who the rules of

> the system shouldn't have allowed it to, that's rightfully a big issue and deserves to be a big uproar.

125. In April 2018, after revealing Cambridge Analytica got unauthorized data on up to 87 million Facebook members — and that nearly all Facebook users may have had their public profile scraped, Zuckerberg stated:

> " We're an idealistic and optimistic company. ... But it's clear now that we didn't do enough. We didn't focus enough on preventing abuse and thinking through how people could use these tools to do harm as well. ... [We are] going to do a full investigation of every app that had a large amount of people's data. "

126. In April 2018, in prepared comments for his congressional testimony, Zuckerberg stated:

> " It was my mistake, and I'm sorry. ... There's more we can do here to limit the information developers can access and put more safeguards in place to prevent abuse. "

127. During the hearing on April 18, 2018, Senator Bill Nelson warned Zuckerberg that "Facebook has a responsibility to protect this personal

information... You [Zuckerberg] told me that the company had failed to do so. It's not the first time that Facebook has mishandled its users' information… did Facebook watch over its operations?"

128. In response to these and other comments by Congressional leaders, Zuckerberg apologized, stating:

> We didn't take a broad enough view of our responsibility, and that was a big mistake. And it was my mistake. And I'm sorry. I started Facebook, I run it, and I'm responsible for happens here.

C. Defendants Consciously Disregarded Their Duties

129. As set forth above, Defendants had at all relevant times duties and obligations as members of the Board and/or officers of Facebook to oversee Facebook's legal compliance, risk exposure, corporate governance, and other critical aspects of the Company's business and operations. In addition, Facebook had legal obligations to protect user privacy and secure its data.

130. Defendants knew from the above incidences, the FTC regulatory investigation and well-documented internal and external reports that: (a) third parties had illegally accessed more data than what was consented to or allowed contractually; (b) Facebook had no enforcement mechanism in place to monitor the collection or use of user data; and (c) Facebook users did not understand or appreciate the number of developers accessing their data, the scope of the data

being collected (i.e., their friends' data and private messages between users), or how their data would be used.

131. Defendants consciously opted out of effective monitoring of data mining activities of third-party app developers and applied lax monitoring policies. They also pursued broad, unclear user permissions that failed to give users adequate notice of the scope and use of the data being collected.

132. Defendants adopted a culture of "move fast and break things." Indeed, Defendant Desmond-Hellmann acknowledge this as Facebook's decade-old motto in speeches she delivered in Seattle and at Cambridge University in the United Kingdom in June 2017.

133. Put differently, Zuckerberg made a strategic choice to *not* prioritize user privacy because it would have impeded Facebook's growth. The other Defendants knew about, and acquiesced in, Zuckerberg's strategy. The unfettered mining of Facebook's user data by third-party developers was Facebook's ethos and business model.

134. Thus, Defendants believed that implementing a meaningful infrastructure with checks, controls, and oversight of third parties' access to and use of Facebook user data would be an impediment to Zuckerberg's vision for the Company.

135. Instead, Defendants maintained business practices that allowed third-party app developers to obtain massive amounts of Facebook user information without verifying the nature and extent of its use. Third parties paid for access to this data and while Facebook had written policies governing that access, it did not enforce the Company's policies or otherwise monitor third parties' compliance with those policies.

136. Defendants knew and consciously disregarded the fact that Facebook was violating various laws and consent decrees (including the FTC Consent Decree), as well as its own policies and the Facebook user agreements by giving app developers nearly unfettered access coupled with no monitoring or oversight.

137. Even though Defendants knew of this type of illegal data collection and data misuse by third party app developers, like Cambridge Analytica, as early as 2015, Defendants took minimal action to strengthen Facebook's data security.

138. Rather, Defendant enforced its policies with respect to third party developers, like Cambridge Analytica, on an *ad hoc* basis. Meaning, that the Company only sought to enforce its policies in specific cases where they were notified of a data breach by an outside party. They took no proactive measures to ensure that third parties' access and user of user data complied with Facebook's terms.

139. For this reason, after learning that 50 million user accounts had been misappropriated, Defendants engaged in an active cover-up and consciously decided not to notify (despite Facebook's Policies described herein) any of the users whose private data had been improperly harvested or the FTC to whom Facebook owed audit and reporting obligations.

140. Now that the Cambridge Analytica data breach is public, Defendants are contemplating enforcement protocols, as well as strategies for retrieving illegally harvested data from Cambridge Analytica and the thousands of other developers who had open access for over a decade. Only now, with the world watching, will Defendants identify and inform impacted Facebook users and audit third party developers.

141. Defendants should be found personally liable for breaching their fiduciary duties given: (a) the gravity, frequency, and scope of the repeated data breaches (Cambridge Analytica and many others); (b) the number of users impacted (likely all individuals who have had a Facebook account at any time since 2007); (c) the lack of sufficient infrastructure to monitor and enforce Facebook's policies and terms of its agreements with third-party developers; (d) the failure to sufficiently monitor and enforce Facebook's compliance with its legal obligations for a period of ten years; (e) the numerous instances where Facebook failed to comply with laws and its obligations to protect data and how it was used;

and (f) the failure to provide users meaningful disclosures so that they could provide informed consent.

D. Defendants' Misconduct Has Harmed Facebook

142. The recent revelations regarding Facebook's actual practices with respect to user privacy and data security have severely damaged the Company's reputation and imposed significant costs on it, including government and regulatory scrutiny, loss of user engagement, and exposure to consumer and shareholder class litigation. Facebook lost an estimated $100 billion in market value following news reports about Cambridge Analytica and the material weaknesses in Facebook's data security systems and controls, as well as the substantial liability stemming from violations of its user privacy obligations.

143. In the days after the breach was publicly revealed, the United States, the United Kingdom, the European Union, Canada, and Israel, have initiated investigations into Facebook's conduct. At the moment, the Attorneys General of the New York, New Jersey, Massachusetts, and Oregon have all launched probes into Defendants' conduct.

144. The Chairman of the Senate Judiciary Committee, Senator Charles E. Grassley of Iowa, has stated that he intends to hold a hearing on the data breach. Members of the Senate Committee on Commerce, Justice, and Science wrote an open letter to Zuckerberg demanding information about how Facebook allowed

third party developers to collect and misuse data. “It’s time for Mr. Zuckerberg and the other C.E.O.s to testify before Congress,” said Senator Mark Warner of Virginia.

145. On March 20, 2018, a committee in the British Parliament sent a letter to Zuckerberg asking him to appear before the panel to answer questions related to Cambridge Analytica. The President of the European Union Parliament also requested an appearance by 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.”

146. On March 19, 2018, Bloomberg reported that the FTC is investigating Facebook’s use of personal user data, specifically “whether Facebook violated terms of a 2011 consent decree of its handling of user data that was transferred to Cambridge Analytica without [user] knowledge.”

147. According to Bloomberg, “if the FTC finds Facebook violated terms of the consent decree, it has the power to fine the company more than $40,000 a day per violation,” or trillions of dollars. An FTC spokeswoman said in a statement on March 20, 2018: “We are aware of the issues that have been raised but cannot

comment on whether we are investigating. We take any allegations of violations of our consent decrees very seriously."

148. In addition to government investigations and regulatory problems, Defendants' misconduct has harmed Facebook's reputation.

149. Defendants breached their obligations to its 2.2 billion users and acted in direct contravention of its own policies on data security and privacy.

150. The illegal practices and Defendants' gross failures to timely address, remedy, or disclose them severely damaged Facebook's reputation within the business community and in the capital markets, as evidenced by, for example, the more than $80 billion loss in market capitalization after the Cambridge Analytica incident and Defendants' related conduct were revealed.

151. Defendants' conduct has harmed Facebook by impairing its ability to attract customers and investors. Users are more likely to delete their Facebook accounts or less likely to sign up for an account knowing their personal data will be compromised. Investors likely will be skeptical of Facebook due to its lack of internal controls and failure to timely disclose material information. Further, as a direct and proximate result of Defendants' actions, Facebook has expended and will continue to expend significant funds, including costs incurred in defending against, and the potential settlement of, civil and criminal legal proceedings brought against the Company related to the unauthorized sharing and use of users'

personal information; and costs incurred from the substantial compensation and benefits paid to Defendants, who are responsible for the scheme.

DERIVATIVE ALLEGATIONS

152. Plaintiff brings this action derivatively in the right and for the benefit of Facebook to redress the breaches of fiduciary duty and other violations of law by Defendants as alleged herein. Plaintiff is a current stockholder of the Company and was a stockholder during misconduct alleged herein, holding Facebook stock continuously. Plaintiff will continue to hold Facebook stock through the resolution of this action.

153. Plaintiff will adequately and fairly represent the interests of Facebook and its stockholders in enforcing and prosecuting the Company's rights, and Plaintiff has retained counsel experienced in prosecuting this type of derivative action.

DEMAND ON FACEBOOK'S BOARD WOULD HAVE BEEN FUTILE

154. At the time this action was filed, Facebook's Board consisted of nine members, defendants Zuckerberg, Sandberg, Andreessen, Thiel, Hastings, Bowles, Koum, Desmond-Hellman, and Kenneth Chenault.

155. Plaintiff did not make a demand to institute this action on this Board because such demand would have been futile.

A. The Board Lacks Independence

156. This Board is incapable of making an independent and disinterested decision to institute and vigorously prosecute this action. With the exception of Chenault, each of the other members of the Board are Defendants to this and other actions and have disabling personal conflicts of interest that render them incapable of exercising independent judgment.

157. By late 2017, Zuckerberg held only 16% of the Company's total outstanding shares, yet he controlled ***60% of the shareholder vote.*** As a result, Zuckerberg exercises absolute control over the Company, its directors and officers, and all key decisions. As such, the Company concedes in its public filings that it is a "Controlled Company"[1] under the corporate governance rules of the NASDAQ Stock Market. *See* Facebook's Definitive Proxy Statement, dated April 14, 2017 ("2017 Proxy").

158. According to the 2017 Proxy:

> Because Mr. Zuckerberg controls a majority of our outstanding voting power, we are a "controlled company" under the corporate governance rules of the NASDAQ Stock Market LLC (NASDAQ). Therefore, we are not required to have a majority of our board of directors be independent, nor are we required to have a

[1] Defined as "any company of which more than 50% of the voting power for the election of directors is held by an individual. . . ." *See http://nasdaq.cchwallstreet.com/nasdaq/main/nasdaq-equityrules/chp_1_1/chp_1_1_4/chp_1_1_4_3/chp_1_1_4_3_8/default.asp.*

> compensation committee or an independent nominating function. In light of our status as a controlled company, our board of directors has determined not to have an independent nominating function and to have the full board of directors be directly responsible for nominating members of our board.

159. As a result of his voting power, Zuckerberg has the power to unseat Defendants from the Board.

160. Andreessen, Thiel, Hastings, Bowles, Koum, and Desmond-Hellman have each proven their unyielding loyalty to Zuckerberg when in 2016 they approved the introduction of a new class of zero-voting shares that would have permitted Zuckerberg to give away a substantial portion of his Facebook shares but continue to maintain control over the Company by eliminating other shareholders' voting rights.

161. Andreessen coached Zuckerberg through the process of pushing the proposed plan to the rest of the Board, even though Andreessen served on the special committee that was supposed to evaluate the proposal independently.

162. Andreessen, Thiel, Hastings, Bowles, Koum, and Desmond-Hellman's willingness to abdicate their duties and approve a plan that would have ensured Zuckerberg's perpetual control over the Company while stripping away shareholder voter rights strongly demonstrates that the Board is loyal to Zuckerberg, and not to the Company and its shareholders.

163. Moreover, Andreessen, Thiel, Hastings, Bowles, and Koum lack independence because they are beholden to Zuckerberg for the prestige of being associated with Facebook and because each has been substantially enriched by their business relationship with Zuckerberg through investment opportunities with and outside of Facebook.

164. Defendant Koum was the controlling shareholder and co-founder of WhatsApp which was acquired by Facebook in 2014 for $22 billion in consideration. Koum owned 45% of WhatApp and therefore, received $10 billion dollars in consideration.

165. Defendants Andreesen and Thiel have also demonstrated a personal bias in favor of keeping founders in control of the companies they fund.

166. Andreesen is one of the founders and principals of Andreessen Horowitz, a venture capital firm that provides seed, venture and growth stage funding to the "best new technology companies." One of Andreesen Horowitz's philosophies is to "enable founders to run their own companies" without interference from financial backers.

167. Andreessen also lacks independence from Zuckerberg as a result of several highly lucrative deals that Andreessen Horowitz has made with Zuckerberg in the past few years, including Facebook's purchase of two of its portfolio companies, Instagram and Oculus VR. Andreessen turned his firm's $250,000

investment in Instagram into $78 million when the $1 billion acquisition by Facebook closed.

168. Andreessen would not have even been able to invest in Oculus VR without Zuckerberg. Andreessen had declined to invest in the company previously, but desperately wanted to invest by the fall of 2013, according to an October 2015 *Vanity Fair* article. When Oculus VR's CEO seemed reluctant to allow the investment, Andreessen reportedly had Zuckerberg talk to the CEO about Andreessen. Andreessen Horowitz got the deal and Andreessen became one of four board members. Not long after, Zuckerberg offered $2 billion for Facebook to acquire Oculus VR.

169. Andreessen Horowitz's access to the best investments relies heavily on Andreessen's relationship with Zuckerberg and Facebook. In a May 18, 2015, *New Yorker* article titled "Tomorrow's Advance Man," Andreessen reportedly explained: "Deal flow is everything. If you're in a second-tier firm, you never get a chance at that great company." Andreessen Horowitz saw its biggest successes after "logo shopping" to add Facebook to the firm's portfolio in 2010. Within two years of that investment, "Andreessen Horowitz was the talk of the town."

170. Defendant Thiel was one of the early investors in Facebook. He co-founded PayPal, Inc., and in 2005 he founded and has since been a partner of The Founders Fund, a venture capital firm that strives to keep founders in control of the

companies they have created. The Founders Fund is marketed on the principle that company founders should have long-term control of the companies they create. In fact, The Founders Fund's website touts Facebook as a primary example of that *maxim*, stating that "we have often tried to ensure that founders can continue to run their businesses through voting control mechanisms, as Peter Thiel did with Mark Zuckerberg and Facebook."

171. Thiel, like Andreessen, has greatly benefited by his relationship with Zuckerberg and his seat on the Facebook Board. The Founders Fund gets "good deal flow" from this high profile association.

172. Defendant Bowles has a history of bowing to the financial interests of CEOs. Over the last decade, Bowles has collected tens of millions of dollars in director compensation for his services on Facebook and other high-profile corporate boards. During his tenures on these various boards, the companies underperformed against the market while he consistently approved lavish (and excessive) payouts to CEOs. For example, in 2012, he and the other board members increased the Norfolk CEOs compensation by 16% while the stock fell below the S&P 500 average. During his time on the Cousins board, the company underperformed, and yet Bowles and the other directors increased the CEO's pay by 73% in 2011 and 276% in 2012. Similarly, during Bowles' tenure on Morgan Stanley's board, the CEO pay went from less than $1.3 million annually in 2008

and 2009 to $38.8 million in 2010 through 2012, though Morgan Stanley's stock price was in decline. Bowles personally received over $3.8 million from Morgan Stanley for his services as a director from 2007 to 2017. Bowles was also member of the General Motors board from June 2005 until April 2009, when the auto giant filed for bankruptcy. Bowles also served on the board of the embattled doughnut maker Krispy Kreme. Ironically, during his tenure on many of these boards, he served as the Co-Chair of the National Commission on Fiscal Responsibility and Reform and preached against reckless government spending. Yet he has consistently voted in favor of excessive compensation increases for CEOs despite poor performance as measured by the market.

173. Defendant Hastings also lacks independence from Zuckerberg. Defendant Hastings is a co-founder of Netflix, and currently serves as its CEO and Chairman of its Board of Directors. In addition to being sympathetic to Zuckerberg's desire to maintain founder's control due to his own founder role at Netflix, Hastings has every incentive to cater to Zuckerberg's desires at Facebook due to Facebook's business relationship with Netflix.

174. Through the "Friends and Community" initiative launched in March 2013, Netflix enjoyed valuable word-of-mouth type marketing because the initiative allows Facebook users to share data about their Netflix viewing habits

with their Facebook friends. Hastings would not want to risk losing this relationship, as the initiative's launch caused Netflix's share price to climb 6%.

175. Defendant Desmond-Hellmann lacks independence from defendant Zuckerberg due to their close business and personal relationships. As Lead Independent Director, Desmond-Hellmann serves as a liaison between Zuckerberg and the Board's independent directors.

B. The Majority of The Board Is Subject to Substantial Risk of Personal Liability

176. Demand is also excused because Defendants face a substantial likelihood of liability for the claims alleged against them in this Complaint. The facts detailed in this Complaint demonstrate that they: (1) affirmatively adopted, implemented, and condoned a business strategy based on deliberate and widespread violations of policies, applicable law and the Consent Decree, which is not a legally protected business decision and cannot be considered a valid exercise of business judgment; and/or (2) consciously disregarded numerous red flags of misconduct throughout the relevant period, subjecting them to a substantial likelihood of liability as to Plaintiff's claims against them in this action. Accordingly, demand on the Board is excused.

177. Defendants were aware of the weaknesses of Facebook's user privacy and data security controls and failed to address and repair them. They were also

and disregarded their affirmative obligations to oversee Facebook's compliance with the Consent Decree.

178. Section VII of the Consent Decrees states that: "[Facebook] shall deliver a copy of this order to all current and future principals, officers, directors, and managers;…." Thus, each of Defendants received the Consent Decree, had knowledge and understood the issues addressed therein and the Company's affirmative obligations under the Decree. Yet, Defendants failed to act to ensure the Company complied with the Consent Decree.

179. The entire Board had a duty to ensure Facebook's systems were sufficiently well-designed to protect user information and detect suspicious activity at the developer level with respect to same. The Board's duty was heightened by the fact that the FTC imposed affirmative obligations with respect to the Company's user privacy practices in the 2011 Consent Order.

180. The Board failed to fulfill that duty, and its failure is even more egregious in light of the many blatant warnings both before and during the relevant period that Facebook's systems were not sufficient to address the misconduct at issue in this Complaint.

181. Given the Board's awareness and deliberate concealment of the breach from the public, and Facebook's failure to notify affected users in accordance with applicable statutes—wrongful actions that resulted in the retention

and unauthorized use of millions of users' personal information for over several years—it is clear the Board either deliberately or recklessly failed to take remedial action to stop the practices that allowed the illicit scheme to continue.

182. For these reasons, the Board is incapable or unwilling to take the actions required to seek the relief requested in this Complaint. Because a majority of the Board faces a substantial risk of liability, demand is futile.

LEGAL COUNTS

COUNT I – BREACH OF FIDUCIARY DUTY
(Against Defendant Zuckerberg)

183. Plaintiff incorporates by reference each and every allegation set forth above, as though fully set forth herein.

184. Defendant Zuckerberg is the Company's controlling shareholder and, as such, owed and continues to owe the Company the highest obligation of due care, loyalty, and good faith.

185. Defendant Zuckerberg breached his fiduciary duties and abused his control over the Company when he allowed the Company to disregard the law and its legal obligations.

186. Zuckerberg failed to monitor and enforce Facebook's compliance with the FTC Consent Decree.

187. Zuckerberg knew that Facebook lacked the infrastructure to monitor and enforce Facebook's policies and terms of its agreements with developers, advertisers, and other third parties.

188. Zuckerberg knew that Facebook was not providing users meaningful disclosures so that they could provide informed consent on who was accessing their data and for what purpose.

189. As a direct and proximate cause of Zuckerberg's conscious inaction and failure to perform his fiduciary duties, the Company has sustained, and will continue to sustain, significant damages, both financially and to its reputation.

COUNT II – BREACH OF FIDUCIARY DUTY
(Against All Defendants Other Than Defendant Zuckerberg)

190. Plaintiff incorporates by reference each and every allegation set forth above, as though fully set forth herein.

191. Defendants owed and owe fiduciary duties to the Company and its shareholders. By reason of their fiduciary relationships, Defendants specifically owed and owe Plaintiff and the Company the highest obligation of good faith and loyalty in the administration of the affairs of the Company, including, without limitation, the oversight of the Company's compliance with laws, regulations, and the FTC Consent Decree.

192. Defendants consciously breached their fiduciary duties and violated their corporate responsibilities by willfully abdicating their roles as fiduciaries by

failing to monitor the Company's compliance with the law and the FTC Consent Decree, failing to monitor the Company's compliance with its own terms of service and with applicable laws regarding data privacy.

193. As a direct and proximate cause of Defendants' conscious failure to perform their fiduciary duties, the Company has sustained, and will continue to sustain, significant damages, both financially and to its corporate image and goodwill.

COUNT III – BREACH OF FIDUCIARY DUTY
(Against Defendants Zuckerberg And Sandberg)

194. Plaintiff incorporates by reference each and every allegation set forth above, as though fully set forth herein.

195. Defendants Zuckerberg and Sandberg owed the Company and its shareholders fiduciary duties by virtue of their positions as CEO and COO, respectively.

196. By reason of their fiduciary relationships, Zuckerberg and Sandberg specifically owed and owe Plaintiff and the Company the highest obligation of good faith and loyalty in the administration of the affairs of the Company, including, without limitation, the oversight of the Company's compliance with laws, regulations, and the FTC Consent Decree.

197. Defendants Zuckerberg and Sandberg consciously breached their fiduciary duties and violated their corporate responsibilities by willfully abdicating

their roles as fiduciaries by failing to monitor the Company's compliance with the FTC Consent Decree and by failing to monitor the Company's compliance with its own terms of service and with applicable laws regarding data privacy.

198. As a direct and proximate cause of Defendants Zuckerberg and Sandberg's conscious failure to perform their fiduciary duties, the Company has sustained, and will continue to sustain, significant damages, both financially and to its corporate image and goodwill.

COUNT IV – CONTRIBUTION OR INDEMNIFICATION
(Against All Defendants)

199. Plaintiff incorporates by reference each and every allegation set forth above, as though fully set forth herein.

200. This claim is brought derivatively on behalf of the Company against Defendants for contribution or indemnification.

201. Facebook is being investigated by the FTC to determine the extent to which Facebook violated its Consent Decree and is a named defendant in various putative consumer class actions filed in the United States District Courts for the North District of California and District of Delaware. The focus of the FTC investigation and the private consumer class actions are Facebook's violations of its legal obligations related to user privacy, data security and data use.

202. If and when the Company is found liable for violating the FTC's Consent Decree and/or consumer laws, the Company's liability will arise in whole

or in part as a result of the intentional, knowing, or reckless acts or omissions of some or all of Defendants as alleged herein.

203. The Company, therefore, is entitled to receive contribution and/or indemnification from Defendants in connection with liabilities that will stem from the FTC investigation and the consumer class actions pending against the Company.

204. Accordingly, the Company is entitled to all appropriate contribution and/or indemnification from Defendants.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff demands judgment as follows:

A. Determining that this action is a proper derivative action maintainable under the law and demand was excused;

B. Finding that the members of the Board breached their fiduciary duties;

C. Finding that Mark Zuckerberg breached his fiduciary duty as controlling shareholder;

D. Finding that Mark Zuckerberg and Sheryl Sandberg breached their fiduciary duties as officers;

E. Against all Defendants and in favor of the Company for extraordinary equitable and injunctive relief as permitted by law and/or equity;

F. Directing the Company to take all necessary actions to reform and improve its corporate governance and internal controls and Board oversight of user privacy, data security and use of data, compliance with various legal obligations including under the Facebook user agreement, the FTC Consent Decree, and any other court or administrative orders;

G. Against all Defendants and in favor of the Company for the amount of any and all damages sustained by the Company as a result of Defendants' breaches of their fiduciary duties;

H. Requiring Defendants to contribute towards any third party liability or judgment against Facebook and/or indemnify Facebook for any losses, fines and legal expenses that resulted from, in whole or in part, by Defendants' misconduct;

I. Awarding Plaintiff the costs and disbursements of this action, including reasonable attorneys' fees and experts' fees; and

J. Granting such other relief as the Court deems just and proper.

Respectfully submitted,

OF COUNSEL:

Catherine Pratsinakis (Del. Id. 4820)
DILWORTH PAXSON LLP
1500 Market Street, Suite 3500E
Philadelphia, PA 19102
(215) 575-7013 (telephone)
cpratsinakis@dilworthlaw.com

DILWORTH PAXSON LLP

By: */s/ Thaddeus J. Weaver*

Thaddeus J. Weaver (Id. No. 2790)
One Customs House
704 King Street, Suite 500
P.O. Box 1031
Wilmington, DE 19899
(302) 571-8867 (telephone)

(302) 655-1480 (facsimile)
tweaver@dilworthlaw.com

Dated: April 25, 2018

Counsel for Plaintiff Karen Sbriglio