EFiled: May 01 2019 01:57AM EDT
Transaction ID 63214436
Case No. 2019-0324-

IN THE COURT OF CHANCERY OF THE STATE OF DELAWARE

ROBERT A. FEUER, Plaintiff, v. MARK ZUCKERBERG; SHERYL K. SANDBERG; PETER A. THIEL; REED HASTINGS; SUSAN D. DESMOND-HELLMAN; MARC L. ANDREESSEN; JAN KOUM; and ERSKINE B. BOWLES, Defendants, and FACEBOOK, INC., Nominal Defendant.	Civil Action No.

VERIFIED COMPLAINT

Plaintiff Robert A. Feuer ("Plaintiff"), a shareholder of Facebook, Inc. ("Facebook" or the "Company"), brings this action on Facebook's behalf seeking relief for the misconduct perpetrated against Facebook by its current and former directors and officers identified below (collectively, "Individual Defendants"). Plaintiff, through his counsel, conducted an investigation of the facts supporting the allegations in this Complaint and believes discovery will elicit further

evidentiary support for the allegations herein. As indicated below, Plaintiff has made a pre-suit demand on Facebook's Board of Directors (the "Board") to, *inter alia*, pursue the claims set forth herein on behalf of Facebook. It has wrongfully failed to do so and, by extension, has *de facto* rejected such demand.

PARTIES

Plaintiff

1. Plaintiff is a current holder of shares of Facebook common stock who has continuously held his Facebook stock since May 18, 2012.

Nominal Defendant Facebook

2. Nominal Defendant Facebook is a Delaware corporation headquartered at 1601 Willow Road, Menlo Park, CA 94025. Facebook's common stock trades on the NASDAQ under the ticker symbol "FB."

3. No claims are alleged herein against Facebook; this litigation is brought on Facebook's behalf. The claims against the Individual Defendants are based on their actions and inactions while serving as directors and/or officers of Facebook.

4. Facebook operates what it has described as a digital "town square" pursuant to which it has obtained more than two billion "subscribers" (users) through, *inter alia*, its Instagram, What's App and Messenger platforms. These users are encouraged to share photos and messages publicly through use of such

platforms. Facebook has made its un-protected user identities and related data available to advertisers (who generate ninety-eight percent (98%) of Facebook's revenues) and other Facebook customers.[1] As Defendant Mark Zuckerberg ("Zuckerberg") has acknowledged, …"we don't currently have a strong reputation for building privacy protective services, and we've historically focused on tools for more open sharing."[2] Although Zuckerberg has maintained that Facebook would focus on private and encrypted communications (by integrating its Instagram, WhatsApp and Messenger platforms) so that users could easily and confidentially message with one another, Facebook has yet to do so. Further, in speaking of Facebook's control over users' confidential data, according to *The New York Times* of April 14, 2019, Zuckerberg maintains that "Every piece of content that you share on Facebook, you own and have complete control over."

Individual Defendants

5. Defendant Zuckerberg is Facebook's Founder, Chairman and Chief Executive Officer. Zuckerberg is responsible for Facebook's day-to-day operations as well as the overall direction and product strategy of Facebook.

[1] Facebook has left millions of user passwords accessible by its employees in readable plain text format, thereby violating fundamental computer security practices. The Company revealed in March, 2019 that hundreds of millions of user passwords had been stored in a format accessible to its employees.

[2] Youn, Soo, *Facebook to Rebrand as 'Privacy-Focused Messaging and Social Networking Platform'* (2019), https://abcnews.go.com/Business/facebook-rebrand-privacy-focused-messaging-social-networking platform/story?id=61510020 (last visited Apr. 30, 2019).

Zuckerberg is Facebook's controlling stockholder with ownership of stock/proxies for stock representing more than 53.3% of Facebook's voting power, though he owns approximately 16% of Facebook's total equity value.

6. Defendant Sheryl K. Sandberg ("Sandberg") has been Facebook's Chief Operating Officer ("COO") since 2008. As COO, Sandberg oversees Facebook's business operations. Additionally, Sandberg has been a Facebook director since 2012.

7. Defendant Marc L. Andreessen ("Andreessen") has been a Facebook director since June 2008. Andreessen is also a member of the Board's Audit Committee and was a member of the Board's Compensation & Governance Committee until May 2018. Andreessen is a close personal friend of Zuckerberg and has conspired with him in connection with previous shareholder litigation and coached him in his testimony by means of text messages and otherwise.

8. Defendant Peter Thiel ("Thiel") is a Facebook director and has been since April 2005. Thiel is also a member of the Board's Compensation & Governance Committee.

9. Thiel was one of the early investors in Facebook and is its second longest-standing Board member behind Zuckerberg. Thiel co-founded PayPal, Inc. and has been a partner of the Founders Fund, a venture capital firm that strives to keep company founders (such as Zuckerberg) in control of the companies they

have created, since 2005. Defendant Thiel also co-founded Palantir in 2003.

10. *The New York Times* reported on Thiel's connections to Palantir and Cambridge Analytica in an article published on January 11, 2017.

11. Defendant Reed Hastings ("Hastings") is a Facebook director and has been since June 2011. Hastings is also the Chair of the Board's Compensation & Governance Committee.

12. Defendant Hastings is a co-founder of Netflix and currently serves as Netflix's CEO and Chairman of its Board of Directors. Netflix is one of Facebook's largest advertisers. Facebook disclosed that Netflix purchased ads from Facebook during the relevant period through Facebook's usual procedures, "including a competitive bid auction." (*See* Facebook 2018 Proxy Statement at 13).

13. As its founder, Zuckerberg desires to maintain control of Facebook. In addition to being sympathetic to Zuckerberg's desire to maintain control of Facebook, Hastings (as Netflix's founder) has every incentive to cater to Zuckerberg's desire to maintain control at Facebook due to Facebook's business relationship with Netflix. Through the "Friends and Community" initiative launched in March 2013, Netflix enjoys 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 Netflix's relationship with Facebook, as the "Friends and Community"

initiative's launch caused Netflix's share price to climb six percent (6%). If Hastings displeased Zuckerberg, such displeasure could potentially jeopardize Netflix's access to valuable Facebook data.

14. Hastings does not want to risk losing his relationship with Facebook or with Zuckerberg, given how lucrative those relationships are for Netflix and for Hastings personally.

15. Defendant Erskine B. Bowles ("Bowles") has been a Facebook director since September 2011. Bowles also chairs the Board's Audit Committee.

16. The Board granted Bowles a waiver of the mandatory retirement age for directors set forth in Facebook's *Corporate Governance Guidelines* (the "*Guidelines*") so that he could stand for re-election to the Board despite having attained the age of 70 years before the date of the Company's annual stockholder meeting on May 31, 2018.

17. Section IX of the *Guidelines* ("Retirement Age") states: "It is the general policy of the company that no director having attained the age of 70 years (as of the date of Facebook's annual stockholder meeting for such year), shall be nominated for re-election or reappointment to the Board. However, the Board may determine to waive this policy in individual cases." Section XXIV of the *Guidelines* ("Review, Amendment and Waiver of Guidelines") provides that "[t]he Board may amend these Corporate Governance Guidelines, *or grant waivers in*

exceptional circumstances, provided that any such modification or waiver may not be a violation of any applicable law, rule or regulation, and, provided further, that any such modification or waiver is appropriately disclosed." (Emphasis added).

18. According to Facebook's 2018 Proxy Statement, the Board granted Bowles a waiver to permit his re-election at the 2018 stockholder meeting despite Bowles having reached the mandatory retirement age for directors in 2019. Individual Defendants did not disclose any reason for the waiver granted to Bowles, let alone identify any "exceptional circumstances" warranting the waiver, in the 2018 Proxy Statement.

19. Defendant Susan D. Desmond-Hellmann ("Desmond-Hellmann") has been a Facebook director since March 2013 and is the designated "Lead Independent Director" of the Board. Desmond-Hellmann is also a member of the Board's Compensation & Governance Committee and was a member of the Board's Audit Committee until May 2018.

20. Desmond-Hellman has demonstrated that she will not take any action to oppose Zuckerberg's wishes or those of the other directors. In April 2016, Desmond-Hellmann initially objected to Zuckerberg's plan to issue new "Class C" shares with no voting rights, a plan that would allow him to sell the majority of his shares for billions of dollars, all while simultaneously retaining total control over decision-making for Facebook. However, Zuckerberg eventually swayed her to

vote in his favor on the plan, highlighting her willingness to cede to his views even when they conflict with her own views of what is best for the Company and its shareholders.

21. As the designated Lead Independent Director of the Board, Desmond-Hellman made a public statement following the break of the Cambridge Analytica scandal described herein, saying that the Board supported Zuckerberg and Sandberg. It was the Board's only comment about the revelations, confirming (once again) that Desmond-Hellman will not take any position against Zuckerberg, even in a statement, let alone commence litigation against him.

22. Defendant Jan Koum ("Koum") was a Facebook Director from October 2014 until April 2018. Koum is a co-founder and former Chief Executive Officer of Facebook's WhatsApp subsidiary until April 2018, when he resigned from the Board and from his role at WhatsApp. According to Facebook's website, Koum was "responsible for the design and interface of WhatsApp's service and the development of its core technology and infrastructure."

NATURE OF THE ACTION

23. The claims herein are based upon, *inter alia,* pervasive breaches of fiduciary duty, misrepresentations, and omissions of material facts by the Individual Defendants, directors and officers of Facebook relating to the Company's mishandling of the confidential and private data of tens of millions of

users of Facebook's social media platforms. The allegations contained herein, taken together, represent one of the worst examples of privacy abuse in the age of social media. The pervasive breaches of fiduciary duty, misrepresentations, and omissions of material facts described herein have caused damage in the name of short-term profit. In addition, while concealing the Individual Defendants' wrongdoing from Facebook shareholders, the investing public and government regulators, three of the Individual Defendants Zuckerberg, Sandberg and Koum, liquidated massive amounts of their personal holdings in breach of their fiduciary duties owed to Facebook and in violation of federal securities laws. Moreover, the Individual Defendants caused Facebook to further violate the federal disclosure laws and rules by misrepresenting material facts regarding the Company, causing massive investor losses resulting in, *inter alia*, class actions against the Company which will cost it massive amounts to defend against and, ultimately, resolve.

JURISDICTION AND VENUE

24. This Court has jurisdiction over the subject matter of this action pursuant to 10 *Del. C.* §341. As officers and directors of a Delaware corporation, the Individual Defendants are deemed to have consented to the jurisdiction of this Court pursuant to 10 *Del. C.* §3114. This Court has jurisdiction over Nominal Defendant, Facebook, a Delaware corporation, pursuant to 10 *Del. C.* §3111.

25. Venue is proper in this forum because this action involves significant issues of Delaware corporate law relating to corporate governance, including the fiduciary duties of loyalty, good faith and oversight that are owed by corporate officers and directors to the Company that they are entrusted to serve, and aiding and abetting the breach of such duties, and is therefore suitable for adjudication before the Delaware Court of Chancery. Venue is also appropriate in this Court by virtue of the provisions of Facebook's corporate bylaws relating to venue in actions asserting claims such as those asserted in this action.

PRE-SUIT DEMAND UPON THE BOARD

26. The claims asserted herein are brought by Plaintiff derivatively on behalf of Facebook. Plaintiff, through his counsel, will fairly and adequately represent Facebook's interests in connection with this action.

27. On June 27, 2018, before asserting these claims, Plaintiff (through his counsel) made a written demand upon the Board for appropriate action by the Board pursuant to Chancery Rule 23.1, a copy of which is attached hereto as **Exhibit A** and is incorporated herein by reference as though set forth in full (the "Demand Letter"). In the more than ten months since the Demand Letter was sent, Plaintiff has not received a response to the Demand Letter.

28. After more than forty-five (45) days lapsed without response to the Demand Letter, on August 15, 2018 Plaintiff's counsel wrote a separate letter to

Zuckerberg, a copy of which is attached hereto as **Exhibit B** and is incorporated herein by reference as though set forth in full (the "Zuckerberg Letter"). The Zuckerberg letter provides, *inter alia*, as follows:

> On June 27, 2018, I sent the enclosed letter to you and your fellow Directors on behalf of Mr. Feuer. FedEx has confirmed that it was received and signed for by "A. Garcia" on June 29, 2018. As of this date, I have not received a response from any member of the Board or legal counsel. As such, I trust that the Board has *de facto* rejected the demands set forth in my June 27 letter. If I am incorrect, please have legal counsel for the Board get back to me promptly.

29. The Zuckerberg Letter was, according to FedEx records, received and signed for by "Z. Helmer" on August 21, 2018. Plaintiff did not receive a response to the Zuckerberg Letter.

30. While most of the facts and circumstances alleged in this Complaint relating to the Individual Defendants' wrongdoing have been shielded from public view, such facts and circumstances have existed, have been perpetrated and known by the Individual Defendants over an extended period of time, during which period there has been substantial, ongoing and escalating harm to Facebook. In addition to the Board's failure to respond to the Demand Letter or the Zuckerberg Letter, the Board has not commenced litigation against the Individual Defendants as demanded by Plaintiff.

31. The Board's failure to respond to the Demand Letter after the expiration of more than ten months since the Demand Letter was received, a more

than reasonable amount of time, confers standing upon Plaintiff to assert the claims alleged in this Complaint on behalf of Facebook.

THE INDIVIDUAL DEFENDANTS' OBLIGATIONS TO FACEBOOK

32. The Individual Defendants owed the Company and its shareholders the fiduciary obligations of good faith, loyalty, prudence, due care, candor and diligence because of (i) their positions as directors and/or officers of Facebook, (ii) their ability to control the business and corporate affairs of Facebook, and (iii) their positions of oversight over the Company's operations. The Individual Defendants were required to exercise reasonable and prudent supervision over the affairs of Facebook in a loyal, diligent, informed, fair, just, competent, ethical and legal manner. All Individual Defendants had an obligation to act at all times in the best interests of Facebook, and to subordinate their individual self-interest to the paramount interests of Facebook. Each Individual Defendant failed to do so.

33. Each Individual Defendant, as a director and/or officer of Facebook, had/has an obligation to take reasonable steps to ensure that the Company is operated in an honest and prudent manner, complying with all applicable federal and state laws, rules, regulations, and requirements as well as agreed-upon consent decrees. Compliance with these requirements was/is required to prevent significant financial and other harm to the Company in the form of fines, penalties,

regulatory sanctions, and (potentially) criminal prosecution for transgressions of applicable law. Each Individual Defendant failed to do so.

34. Each Individual Defendant, as a director and/or officer of Facebook, had an obligation to take reasonable steps to investigate and, if appropriate, assert any and all valid claims and causes of action the Company may have (or may have had) against persons and entities on account of the breaches of fiduciary duty, misrepresentations, and omissions of material facts alleged in this Complaint. The Individual Defendants also have/had an obligation to take reasonable and prudent steps to preserve the Company's ability to assert potential claims as they were being evaluated and considered so that any such claims (or potential claims) do not /did not lapse, or become stale, due to the passage of time. Each Individual Defendant failed to do so.

35. In addition to their obligations as set forth above and pursuant to applicable Delaware corporate law, each Individual Defendant was bound to implement, enforce and execute corporate policies and rules of corporate governance applicable to him or her, including the obligations set forth in the *Guidelines*.[3]

The *Guidelines* state:

[3] While the *Guidelines* purport to be "not…binding legal obligations," they nevertheless serve as the standard by which the conduct of officers and directors should be evaluated.

> Facebook's Board of Directors has adopted these Corporate Governance Guidelines to reflect the Board's strong commitment to sound corporate governance practices and to encourage effective policy and decision making at both the Board and management level, with a view to enhancing long-term value for Facebook stockholders. These guidelines are intended to assist the Board in the exercise of its governance responsibilities and serve as a flexible framework within which the Board may conduct its business, not as a set of binding legal obligations.

36. Each Individual Defendant failed to act pursuant to, and consistent with, the standards established by the *Guidelines*.

37. The *Guidelines* enumerate the primary responsibilities of the members of the Board:

> The Board acts as the management team's adviser and monitors management's performance. The Board also reviews and, if appropriate, approves significant transactions and develops standards to be utilized by management in determining the types of transactions that should be submitted to the Board for review and approval or notification.
>
> * * *
>
> Each member of the Board (each, a "director" and collectively, the "directors") is expected to spend the time and effort necessary to properly discharge such director's responsibilities. Accordingly, a director is expected to regularly attend meetings of the Board and Board committees on which such director sits, and review prior to each meeting the material distributed in advance for such meeting.

38. As set forth herein, each Individual Defendant failed to fulfill the *Guidelines'* responsibilities identified in the preceding paragraph.

39. The Individual Defendants' obligations are also described in Facebook's *Code of Conduct* (the "*Code*"), which provides in relevant part:

> Employees of Facebook … and others performing work for Facebook or on its behalf, collectively referred to in this code as 'Facebook Personnel,' are expected to act lawfully, honestly, ethically, and in the best interests of the company while performing duties on behalf of Facebook.

40. As set forth herein, each Individual Defendant failed to act consistent with the *Code* responsibilities identified in the preceding paragraph.

THE CONSENT DECREE

41. Among other obligations, the Individual Defendants are bound by agreements made on behalf of Facebook with the Federal Trade Commission ("FTC"). In particular, the FTC found that Facebook had deceived its users by representing that said users could control access to the information which they provided to Facebook. The Company, through the Board, was forced to adhere to strict user data protection measures as part of a Consent Decree (as hereinafter defined) with the FTC that was agreed to on November 29, 2011.[4]

42. The Consent Decree required Facebook to, among other things, give users clear and prominent notice and obtain express consent before allowing user

[4] *See* Agreement Containing Consent Order, Fed. Trade Comm'n, *In the Matter of Facebook, Inc.*, File No. 092 3184 (Nov. 29, 2011) (the "Consent Decree"), https://www.ftc.gov/sites/default/files/documents /cases/2011/11/ 111129facebookagree.pdf (last visited Apr. 30, 2019); Decision and Order, Fed. Trade Comm'n, *In the Matter of Facebook, Inc.*, File No. 092 3184 (July 27, 2012) (available at same link).

information to be shared with other applications. In addition, the Consent Decree required Facebook to establish and implement a comprehensive privacy program to protect the privacy and confidentiality of user information. The Consent Decree includes a fine of $40,000 per day for each violation of the Consent Decree. Upon information and belief, the Individual Defendants have acquiesced in Facebook's continuing breach of its obligations under the Consent Decree.

43. The Consent Decree also required Facebook to:

> establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to address … privacy risks related to the development and management of new and existing products and services for consumers ….

44. As described herein, Facebook failed to comply with its obligations pursuant to the Consent Decree.

45. Such breaches of the Consent Decree and other, related misconduct have resulted in the re-opening of an investigation by the FTC and parallel investigations by the Federal Bureau of Investigation, the Department of Justice and the Securities and Exchange Commission. These widening federal investigations have created severe and imminent risks to Facebook, including the likelihood that substantial financial and other sanctions will be imposed. Indeed, on April 24, 2019, Facebook disclosed that it expected that the FTC would impose a

fine against the Company of $3 billion to $5 billion for violation of the Consent Decree, a sum that would be "symbolic of the gravity"[5] of the violation.

CAMBRIDGE ANALYTICA

46. On December 11, 2015, *The Guardian* reported that an English company, Cambridge Analytica, was paying researchers at Cambridge University to gather detailed personal data from a massive pool of unwitting Facebook users in order to create psychological profiles of U.S. voters for the purpose of influencing elections. Facebook immediately assured shareholders that misusing user data would be met with strict consequences and that Facebook was in full compliance with the Consent Decree.

47. On March 17, 2018, a pair of exposés published by *The New York Times* and *The Observer of London* revealed that private information from as many as 87 million Facebook users' profiles had been harvested and purchased by the business and political consulting firm Cambridge Analytica without the users' knowledge or consent after initially having been provided to Alexandr Kogan, a Cambridge University professor and/or its related Psychometrics Centre.[6]

[5] Warzel, Charlie, *When $5 Million Is a Slap on the Wrist*, A18, THE NEW YORK TIMES (Apr. 26, 2019).

[6] Prof. Kogan used a quiz app to gather data on those who took a survey and their friends. The Facebook data-gathering feature, called an API, was a common technique at the time in assembling massive data troves for analysis, including names, hometowns, work histories, religious affiliations and personal preferences.

48. Facebook has portrayed Cambridge Analytica's data-gathering as an improper use inasmuch as it was not used for academic purposes. The Individual Defendants knew or should have known that Kogan, the Psychometrics Centre and/or Cambridge Analytica was/were not using Facebook user information for academic purposes.

49. User data was also sold by Facebook to other companies. Moreover, through the use of "scraper" programs, Facebook has permitted "researchers" to gain access to user data.

50. In the case of Cambridge Analytica, the data were used to create specific personality profiles for large swaths of the American populace, allowing it to craft marketing strategies targeted to the sensitivities of any personality type. These personality profiles were sold, *inter alia*, to the presidential campaign of Donald J. Trump ("President Trump") and have been partially credited with aiding President Trump's victory in the election. Data from as many as 2.7 million European users were also shared with Cambridge Analytica.

51. On June 29, 2018, Facebook revealed in its report to the United States Congress ("Congress") that Facebook and its Board not only failed to protect users' information but, as set forth above, intentionally shared users' information with developers and hardware/software manufacturers, including some of the

largest companies in the world, many of whom still have access to user information.

52. Despite being aware since 2015 that Cambridge Analytica and other third parties had amassed data from millions of Facebook's users, Facebook's management has intentionally done virtually nothing in response. To the contrary, the Company's executive management and Board – the Individual Defendants herein – consistently misrepresented to users, shareholders, regulators and Congress that Facebook had a comprehensive privacy program in place, that Facebook notified users if their information had been compromised, and that Facebook required third-party developers to adhere to strict confidentiality provisions.

53. On March 17, 2018, *The Guardian* published another dramatic report describing how Facebook allowed Cambridge Analytica to misappropriate and retain the personal data of 50 million users in order to target them with personalized political advertisements. Indeed, Facebook had its employees embedded at the campaign headquarters of President Trump to facilitate such personalization. *The Guardian*'s investigation included documents provided by a whistleblower named Christopher Wylie, a data analytics expert that formerly worked at Cambridge Analytica.

54. On March 18, 2018, *The New York Times* reported that members of Congress called for an investigation of the Facebook data leak and pressed Zuckerberg to appear before the Senate Judiciary Committee to explain what the social network knew about the misuse of its data "to target political advertising and manipulate voters."

55. On March 20, 2018, *The Guardian* followed up with a report from a Facebook whistleblower, Sandy Parakilas, a former platform operations manager at the Company, who revealed that Facebook routinely shared user data without consent, had "'no idea what developers were doing with the data,'" and "did not use its enforcement mechanisms" to remedy known violations. *The Guardian*'s report also indicated that Parakilas had "warned senior executives at the company," but that "'Facebook was in a stronger legal position if it didn't know about the abuse that was happening. . . . [t]hey felt that it was better not to know.'"[7]

56. On March 26, 2018, the FTC issued a press release confirming that it was investigating Facebook's privacy practices and compliance with the Consent Decree.

[7] Lewis, Paul, *'Utterly Horrifying': Ex-Facebook Insider Says Covert Data Harvesting Was Routine* (2018), https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas (last visited Apr. 30, 2019).

57. On April 10 and 11, 2018, Zuckerberg appeared before Congress and apologized for Facebook's conduct, but deceptively downplayed the extent of the unauthorized use of user data to the acts of a single, rogue company which intentionally skirted Facebook's privacy policies. According to Zuckerberg, Facebook had effectively restricted the disclosure of users' personal information to outsiders in 2015, when it implemented new policies. Zuckerberg's statement before Congress on this point was false, and all the Individual Defendants knew or should have known that it was false.

58. On April 13, 2018, in the midst of the Cambridge Analytica scandal, the Individual Defendants issued Facebook's annual Proxy Statement (the "2018 Proxy Statement"), soliciting their re-election to the Board at the annual meeting scheduled for the following month. Shockingly, in breach of their respective duties of candor and their obligations under federal securities law, the Individual Defendants did not disclose anything about the user privacy scandal that had engulfed the Company and, in particular, the Individual Defendants' personal breaches of the Consent Decree.

59. The 2018 Proxy Statement did not contain a single statement regarding Cambridge Analytica, and it also failed to disclose material facts concerning the FTC's investigation into possible violations of the Consent Decree. The Individual Defendants recommended that Facebook's shareholders vote

against proposals to: (i) create a new committee of the Board and (ii) require reports that would enhance the Board's oversight of the very issues that gave rise to the scandal and to multiple government investigations, and that have caused serious harm to Facebook. The Board's recommendations, like the rest of the 2018 Proxy Statement, were false and misleading because they failed to disclose material facts concerning Facebook's business practices and the Company's policies relating to gathering and sharing information and user data with third parties. Instead, the Individual Defendants assured Facebook's stockholders that the Company's "current corporate governance structure is sound and effective." Nothing could be further from the truth.

60. On June 29, 2018, in response to questions from representatives of Congress to Zuckerberg, Facebook provided a seven hundred forty-seven (747)-page document and admitted that it actually gave dozens of companies special access to user data, contrasting with the Company's prior public statements.[8] Indeed, Facebook disclosed that it was still sharing information of users' "friends" on Facebook, such as name, gender, birth date, current city or hometown, photos and page likes, with over sixty (60) application developers nearly six (6) months

[8] Plaintiff incorporates by reference Facebook's June 29, 2018 responses to the House Energy and Commerce Questions for the Record, available at: https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/House%20QFRs.compressed.pdf (last visited Apr. 30, 2019).

after it claimed it had stopped access to this data in 2015. Facebook also admitted that it had shared information about its users with fifty-two (52) hardware and software makers, including such large United States corporations as Amazon.com, Apple Inc. and Microsoft Corp, as well as Chinese firms such as Huawei Technologies Co. and Alibaba Group. Fourteen companies continue to have access to information about Facebook's users.

61. As these reports made public, the Individual Defendants have repeatedly concealed critical facts that are necessary to inform users and comply with applicable law. This concealment has severely damaged Facebook's reputation and imposed significant costs on Facebook, including costs due to the massive amounts of regulatory interest, inquiries, and investigations commenced in the wake of the Cambridge Analytica scandal. In addition, the Company has suffered a loss of user trust, harm to its core advertising business, and other damages associated with its exposure to litigation, regulation, fines, and other penalties. If, after investigation, Facebook is found to have violated the Consent Decree, Facebook could face billions of dollars more in fines and penalties from the FTC, the British Parliament, and the European Union.

62. Facebook's long-term financial health will suffer lasting damages as a result of the Individual Defendants' wrongful conduct. The confidence of advertisers in Facebook, which are virtually the only source of revenue for the

Company, have been shaken by the foregoing controversies, and said advertisers have publicly expressed concern about Facebook's mishandling of user data. Numerous large advertisers have demanded assurances from the Company, and others have pulled advertisements from Facebook's platforms.

63. Facebook's shares dropped precipitously and lost $50 billion in market value in the first two days following public revelation of the Cambridge Analytica scandal. The Board and senior executives have failed—repeatedly, and brazenly—to serve the best interests of Facebook, its shareholders, and the public at large. As a result of their misconduct, the Individual Defendants are liable to the Company for their respective breaches of fiduciary duty, misrepresentations, and omissions of material facts.

64. Although the public outcry is relatively recent, the Board has known for years of the privacy and security risks posed by companies such as Cambridge Analytica. Despite a number of such incidents throughout the years that Facebook has been in existence, the Board has failed to properly advise Facebook users of privacy risks or take action to protect the Company from the fallout of privacy breaches. In fact, the Board has actively ignored early warnings signs of trouble to the Company's detriment.

65. In 2007, Facebook announced that it would become an "open platform," allowing outside developers to build applications and programs based

on user data and preferences, but assured users that they could control access to their private information through their Facebook privacy settings. Facebook failed to disclose that the restrictions set by users did not apply to third-party application developers. This misrepresentation came to light in 2010, when *The Wall Street Journal* reported that an online tracking company, RapLeaf, was engaging in conduct very similar to that of Cambridge Analytica: culling Facebook users' data via third-party applications and selling the data to marketing firms and political consultants. Facebook was a smaller and less influential company in 2010 than it is now in 2018, and RapLeaf's Facebook-related activities did not engender the same level of public criticism that Cambridge Analytica faced eight years later. The public ire caused by the *Journal*'s 2010 RapLeaf article forced Facebook to remove RapLeaf's access to Facebook data, but the Company, with the Board's acquiescence, took no steps to change Facebook privacy controls or impose any limits on the data that could be collected by third-party applications.

66. Despite its agreement to protect users' privacy pursuant to the Consent Decree, Facebook continued to flout that responsibility. It was not until April 2015 that Facebook announced that applications would no longer be able to cull information from Facebook users' "friends" who had installed the application. This action fell far short of fulfilling Facebook's duty to protect user data pursuant to the Consent Decree and otherwise. Facebook had no way to track the user data

that had been accessed by applications prior to 2015, and therefore had no way to determine whether the data had been destroyed, saved, or transferred to a third party. With the knowledge of the Individual Defendants, Facebook failed to take any steps to determine what happened to data gathered prior to 2015, despite being aware since at least 2010 that applications such as RapLeaf had mishandled data obtained from "friends" of Facebook's users who had installed a third-party application.

67. Eight months later, in December 2015, *The Guardian* published an article detailing how an application company called Global Science Research "GSR") had harvested data from an estimated forty (40) million Facebook user profiles and sold the data to a little-known marketing company called Cambridge Analytica. Cambridge Analytica had used the data to create targeted campaign messages for Ted Cruz, whose 2016 presidential campaign paid Cambridge Analytica at least $750,000 for its services. The article noted that Robert Mercer, a prominent Republican donor who donated $11 million to one of Mr. Cruz's Super PACs, was the primary investor behind Cambridge Analytica. Facebook banned the GSR application through which Cambridge Analytica had obtained the information and required GSR to formally certify that the data it collected had been deleted. However, Facebook did not disclose any of these actions to its users, nor did it take any steps to ensure that GSR actually deleted any of the data harvested

from Facebook. Not surprisingly, Facebook has the ability to "flag" instances when its employees and others access user data, with the user getting a so-called "Sauron" alert. The Company does not make such technology available to non-employee users.

68. By 2016, Facebook (and, presumably, the Individual Defendants) had been made aware of at least two companies that had purchased users' private information without users' knowledge or consent, then used that data to craft political campaigns targeted to specific personality profiles of American voters. Additionally, in 2016, Facebook's now-former Chief Security Officer, Alexander Stamos ("Stamos"), prepared an internal report on Russia's use of Facebook to interfere in the 2016 United States presidential election. Despite mounting evidence that users' private information was being improperly utilized by political entities, on November 10, 2016, while speaking onstage at a Techonomy conference, Zuckerberg publicly dismissed concerns that Facebook had influenced or impacted the United States election in any way.

69. In March 2018, the Cambridge Analytica story broke to significant public outcry. Several former Facebook employees have since come forward to expose the cavalier approach Facebook took with regard to protection of user data, including Stamos, who was pushed out of his position with Facebook due to his investigation of the Russian election interference.

70. Following the March 2018 Cambridge Analytica exposés, Facebook refused to address the scandal publicly for several days, during which time public hysteria mounted. Finally, on March 25, 2018, in a full-page newspaper ad, the Individual Defendants directed Facebook to issue a public apology for the violation of users' privacy and admitted that it was likely that other applications had accessed data in a manner similar to Cambridge Analytica. Zuckerberg also appeared before Congress to answer questions about Facebook's use of user data. These steps were too late to assuage the public. Numerous media outlets published opinion pieces recommending that people delete Facebook to protect their privacy, and "#deleteFacebook" started to trend on Twitter.

71. The timeline above clearly illustrates that the Individual Defendants were aware that Facebook users' data was culled without users' knowledge or consent. They were also aware that users' data was an invaluable trove of information for political consulting firms like RapLeaf and Cambridge Analytica, who have been experimenting with the ability to manipulate the United States population through social media. In the face of these risks, the Board failed to: (i) protect the Company, (ii) take adequate action to ensure the safety of users' private information; and (iii) prevent the cultivation of users' data for marketing and political purposes.

72. The Individual Defendants caused further damage to Facebook when, in 2014, the Individual Defendants authorized the acquisition of WhatsApp, a popular messaging service, for $22 billion, notwithstanding fundamental disagreements regarding user privacy with WhatsApp's founders. These co-founders, Koum and Brian Acton, were (and are) strong advocates for user privacy, with "respect for[user] privacy coded into our DNA" and the business built "around the goal of knowing as little about [users] as possible." These strongly-held philosophies undergirded WhatsApp and, from the date of its acquisition, created wholesale conflicts with Facebook's misuse of user data. Ultimately, in the wake of the Cambridge Analytica debacle, Koum and Mr. Acton announced their resignations, leaving Facebook with a substantially-devalued WhatsApp.

OTHER WRONGDOING

73. In testimony before the United States Senate, Zuckerberg said: "I think everyone should have control over how their information is used." Notwithstanding such oft-repeated claims, Facebook has continued to undermine user privacy by making it unduly cumbersome for such users to "opt out" of the Company's sharing features. The Company, with the knowledge of the Individual Defendants, makes it extremely difficult for users to recover data pertaining to them from the Company's databases.

74. In a misguided attempt to re-enter the Chinese market out of which the Company had been excluded, Facebook has, according to *The New York Times*, "worked on a tool that allowed targeted censorship, prompting some employees to quit over the project."

75. In 2010, the Company transferred to its subsidiary, Facebook Ireland Holdings, Unlimited, the rights to its "online platform" and "marketing intangible" assets outside the United States and Canada. In the wake thereof, since 2010, the Company's assets have been materially undervalued through artificial means. This led, in turn, to a July 2016 lawsuit by the Internal Revenue Service complaining of *de facto* underpayment of taxes as well as non-compliance with an Order to produce relevant documents by June 17, 2016. While Facebook has sustained damages as a consequence thereof, those damages have not been disclosed publicly.

76. During 2017, in the wake of Facebook's acquisition of WhatsApp, the European Commission fined Facebook 110 million Euros (approx. $122 million) for falsely representing that it was impossible to combine user data collected by Facebook and WhatsApp. Facebook management represented that Facebook would not appropriate the user data of WhatsApp's members or track who such users communicated with, and when and where such communications took place. The reverse was true.

77. Facebook also tracks and stores data on non-members despite being ordered to cease and desist from doing so by judges in Belgium and France between 2015 and this year. In connection with member and non-member data, Facebook plans to expand its monitoring of almost every aspect of their lives and has filed numerous patent applications to enable it to do so. *See, e.g*. U.S. patent applications ## 9,740,752; 12/839,350; 15/203,063. Despite widespread public criticism of the Company's privacy policies and a commitment from Zuckerberg to "do better," Facebook's patent applications demonstrate a plan to collect and exploit even more personal data than it does at present.

78. In connection with its misuse of user data and the other wrongful conduct referred to herein, each of the Individual Defendants concealed and misrepresented such misuse and wrongful conduct on Facebook's behalf, through SEC filings, press releases and other communications. The misuse and wrongful conduct by the Individual Defendants caused Facebook shares to be artificially inflated and, by extension, defrauded investors therein. As a result, the Company has been vulnerable to -- and will be damaged by -- the pending lawsuits commenced by such investors as well as the expenses of defending against them. Specifically, the Company is subject to class action lawsuits brought on behalf of Facebook users who have complained about its misuse of their personal data as described herein.

INSIDER TRADING

79. In 2018, prior to the exposure of the Cambridge Analytica scandal, three of the Individual Defendants -- each a Facebook Director -- sold a total of $1.5 billion of Facebook stock: (i) Zuckerberg sold over $978 million of his Facebook holdings; (ii) Sandberg sold over $35 million of her Facebook holdings; and (iii) Koum sold over $442 million of his Facebook holdings. At the time Zuckerberg, Sandberg and Koum sold their respective shares of Facebook stock in 2018, Facebook had been aware of the activities of Cambridge Analytica and the other misconduct referred to herein since at least 2015, and had been putting out a growing number of privacy-related "fires" since its inception in 2007. The 2018 stock sales by Zuckerberg, Sandberg, and Koum helped them avoid the losses that they would have incurred if they had sold their shares following the public disclosure of Cambridge Analytica's data breaches. Additionally, the 2018 stock sales helped Zuckerberg, Sandberg and Koum avoid potentially substantial future losses that may result from governmental intervention post-Cambridge Analytica, including (i) increased regulations that strike at the heart of Facebook's business model and (ii) large fines for violation of the Consent Decree.

Each of Zuckerberg, Sandberg & Koum were aware at the time of the 2018 stock sales referenced above that Facebook faced a looming crisis over privacy concerns and that the value of Facebook equity shares did not reflect such "inside

information" known to them.

I. THE INDIVIDUAL DEFENDANTS WERE OBLIGATED TO SAFEGUARD THE COMPANY'S INTERESTS AND COMPLY WITH APPLICABLE LAWS

80. By reason of their positions as directors and/or officers of Facebook, and because of their ability to control the business, corporate, and financial affairs of Facebook, the Individual 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 ensuring that Facebook operated in compliance with all applicable federal and state laws, rules and regulations. The Individual Defendants were and are required to act in furtherance of the best interests of Facebook and its shareholders so as to benefit all shareholders equally; the Individual Defendants may not place their personal interest or benefit ahead of their responsibilities to Facebook and its shareholders. Each director and/or officer of Facebook (including the Individual Defendants) owes to Facebook and its shareholders the fiduciary duty to exercise good faith and diligence in the administration of the affairs of the Company and in the use and preservation of its property and assets. Each director and/or officer of Facebook also owes to the Company and its shareholders the highest obligations of fair dealing and loyalty.

81. Because of their positions of control and authority as directors and officers of Facebook, the Individual Defendants, directly or indirectly, exercised

control over the wrongful acts detailed in this Complaint. Because of their positions with Facebook, the Individual Defendants had knowledge of material non-public information regarding the Company.

82. To discharge their duties, the Individual Defendants were required to exercise reasonable and prudent supervision over the management, policies, practices, controls, and financial and corporate affairs of the Company. 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 by-laws of Facebook;

b. Ensure that Facebook did not engage in imprudent and/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 issued by Facebook, and to examine and evaluate any reports of examinations or investigations concerning the practices, products, or conduct of Facebook officers;

e. Preserve and enhance Facebook's reputation as befits a public corporation;

f. Exercise good faith to ensure that Facebook's affairs were conducted in an efficient, business-like manner so as to make it possible to provide the highest quality performance of its business; and

g. Refrain from unduly benefiting themselves and other Facebook insiders at the expense of the Company.

83. Facebook's preliminary proxy statement, filed with the SEC on or about April 14, 2017 (the "2017 Proxy Statement"), provides:

a. "The full board of directors has primary responsibility for evaluating strategic and operational risk management, and for CEO succession planning."

b. The audit committee "has the responsibility for overseeing our major financial and accounting risk exposures as well as legal and regulatory risk exposures[,]" "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[,]" and "oversees our internal audit function."

c. The compensation & governance committee "evaluates risks

arising from our compensation policies and practices[.]"

d. The audit committee and the compensation & governance committee "provide reports to the full board of directors regarding these and other matters."

84. In addition to Board/Board committee responsibilities identified in the 2017 Proxy Statement, the Individual Defendants also have specific obligations under the Consent Decree (to which all members of the Board specifically acquiesced) and are duty-bound to oversee Facebook's compliance with its terms. Specifically, under the Consent Decree, Facebook is:

a. barred from making misrepresentations about the privacy or security of consumers' personal information;

b. required to obtain consumers' affirmative express consent before enacting changes that override their 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 to protect the privacy and confidentiality of consumers' information; and

e. required, every two (2) years for the next twenty (20) years

after entry of the Consent Decree, 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 consumers' information is protected.

85. As FTC Chairman Jon Leibowitz stated in the FTC's press release announcing the settlement and terms of the Consent Decree on November 29, 2011:

> *Facebook is obligated to keep the promises about privacy that it makes to its hundreds of millions of users*… Facebook's innovation does not have to come at the expense of consumer privacy…

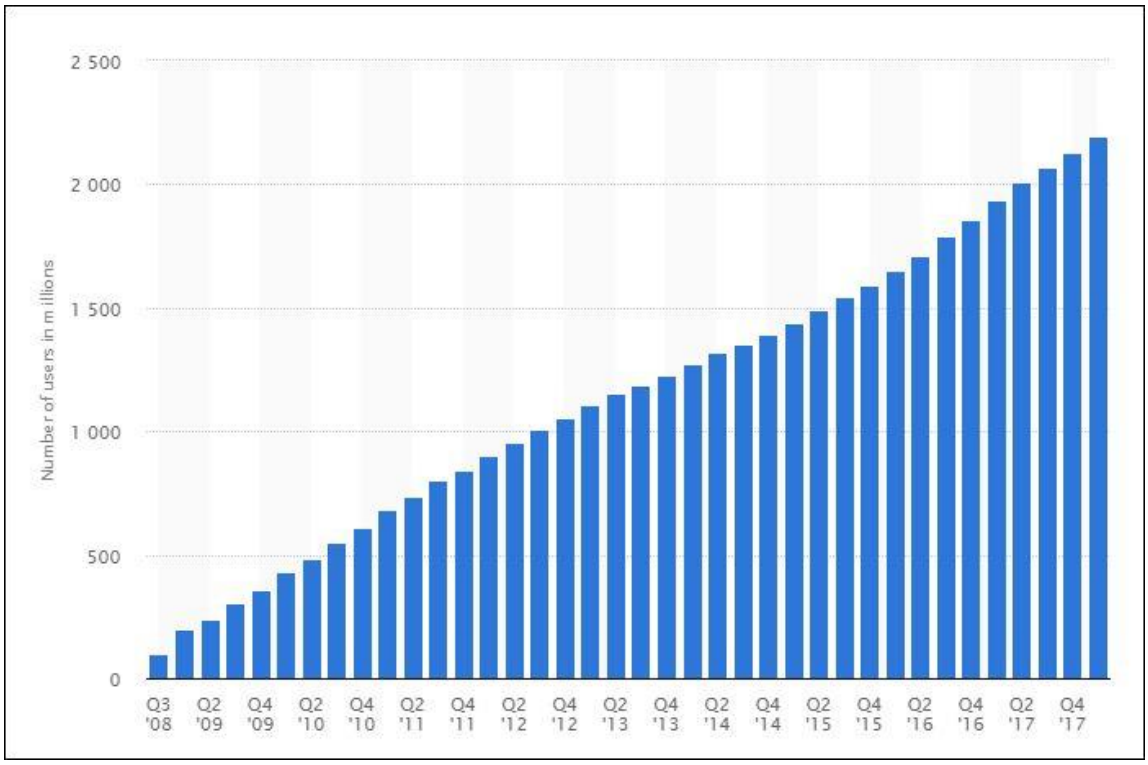
The Individual Defendants failed to keep the promises about privacy that it made to its users, and permitted Facebook to violate federal, state and foreign laws as set forth below.

II. BACKGROUND OF THE COMPANY AND ITS BUSINESS

86. Founded in 2004 by Zuckerberg when he was a student at Harvard University, Facebook is the biggest social networking service based on global reach and total active users. According to Facebook's Newsroom, Facebook had 1.45 billion daily active users on average in March 2018, and 2.2 billion monthly active users as of March 31, 2018.

87. Monthly active users ("MAUs") are those which have logged in to Facebook during the last 30 days. Facebook's number of MAUs has reportedly

increased in every quarter since 2008, as shown in the following chart:



(Chart: Number of monthly active Facebook users worldwide as of 1st quarter 2018 (in millions)).

88. Facebook users must register before using the social network and are free to create a personal profile in order to interact with other Facebook users which they can add as "friends." Furthermore, Facebook users may join user groups and can categorize their Facebook contacts into lists. Facebook users can post status updates or other content and message each other. Facebook users can also interact with a wide selection of applications, including social games or other

services like the photo-sharing app Instagram.

89. Facebook's users provide personal information to Facebook, which has economic value because this data can be exchanged for content and services

THE FACEBOOK PLATFORM ALLOWS APPLICATIONS, WEBSITES, AND DEVICES TO ACCESS AND USE THE PERSONAL INFORMATION OF BILLIONS OF USERS

A.

90. The Facebook Platform has grown over time to allow ever greater access to the personal information of Facebook users. The Facebook Platform was launched in 2007. The Facebook Platform originally supported only applications created by Facebook for use on Facebook, but soon expanded to allow third-party developers to develop their applications using the Platform. Zuckerberg announced the expansion of the Facebook Platform to third-party developers in 2008, stating:

> With-this evolution of Facebook Platform, we've made it so that any developer can build the same applications that we can. And by that, we mean that they can integrate their application into Facebook —into the social graph — the same way that our applications like Photos and Notes are integrated.

91. In a further expansion of the Facebook Platform, Zuckerberg announced the launch of Graph Application 19 Programming Interface ("Graph API") at Facebook's annual developer conference in 2010. Graph API allows developers to read and write data from and to Facebook and to obtain, track, and share information.

92. Through Graph API and later iterations of the "social graph," Facebook obtains and shares information about users through "features" that third parties can implement on their own websites, such as the "Like" button, the "Share" button, and the "Log in with Facebook" option, among other things. These "social plug-ins" enable Facebook and third-party websites to exchange user information. Facebook obtains information about the websites' users and activities, including purchases, and the third-party websites can also receive information from Facebook.

93. Facebook has similarly expanded its access to (and use of) personal information through partnership agreements and referral services with third-party companies. For example, Facebook's agreements with mobile device manufacturers allow Facebook to implement its features directly on mobile devices. Facebook's presence on mobile devices has enabled Facebook to obtain information about mobile device users, including non-Facebook users, and to track users across devices.

94. As stated in a letter that Facebook sent to the Law Commission of New Zealand in 2011:

> [a]t Facebook's core is the social graph: people and the connections they have to the things they care about. In 2010, we began extending the social graph, via the Open Graph protocol, to include websites and pages that people like throughout the web. This is referred to as 'Facebook Platform.'" The letter further explained: "Facebook Platform enables developers to build social apps, websites and devices

that integrate with Facebook and reach millions of people.

B. FACEBOOK'S CORE ADVERTISING BUSINESS IS THE PRIMARY SOURCE OF THE COMPANY'S REVENUE

95. Facebook offers advertising services to its customers that include (or have included at various points in time), among other things: (i) assisting customers in developing and creating advertisements and advertising strategies; (ii) obtaining information about Facebook users from the Company's website and third- party sources; (iii) compiling user data and maintaining databases of information about Facebook users; (iv) developing a marketing and advertising strategy to target and exclude certain groups of Facebook users from receiving advertisements; (v) tracking and evaluating the effectiveness of advertisements and user targeting strategies; (vi) implementing advertising campaigns; and (vii) delivering advertisements to Facebook users, including via News Feed.

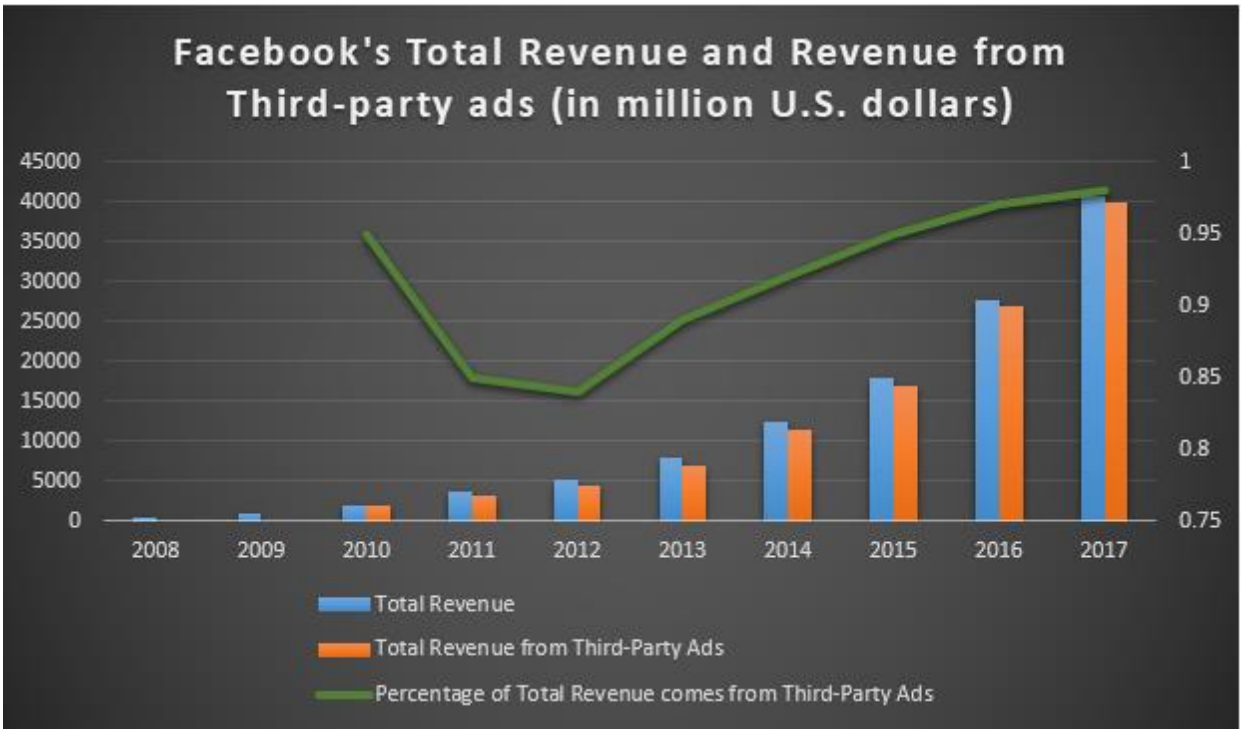
96. Facebook's customers (advertisers) can use Facebook's advertising services to target users with specific attributes. Facebook applies its own algorithm to categorize Facebook users and to determine which users and groups of users will be targeted to receive advertisements via its advertising platform. As stated on Facebook's website:

> With our powerful audience selection tools, you can target people who are right for your business. Using what you know about your customers—like demographics, interests and behaviors—you can connect with people similar to them.

97. Facebook also provides detailed analytical data to advertisers on how their ad campaigns are performing, including among certain groups of Facebook users with specified attributes and characteristics that the advertiser seeks to target. By monitoring this data and providing this information to its customers on an ongoing basis, Facebook captures consumer behavior, profile, preferences, lifestyle, and other attributes which allow Facebook to run targeted ads. This enables advertisers to specify the groups of users that will be targeted to receive the advertisements.

98. Facebook's data about its users is highly valuable. The average cost per click for an online Facebook ad was $1.72 in 2017, and the average U.S. Facebook user is reportedly worth about $200 a year.

99. Facebook's advertising business accounted for substantially all of the Company's revenue through 2017:



III. FACEBOOK'S TRANSFORMATION FROM "SOCIAL NETWORK" TO DATA- GATHERING EMPIRE

A. SINCE 2007, FACEBOOK HAS WORKED WITH THIRD-PARTY COMPANIES, INCLUDING COMPETITORS, TO GAIN ACCESS TO DATA

100. The Facebook Platform has grown over time to allow ever greater access to the personal information of Facebook users. The Facebook Platform was launched in 2007. The platform originally supported only applications created by Facebook for use on Facebook, but soon expanded to allow third-party developers to develop their applications using the Facebook Platform.

101. Facebook launched Beacon in 2007, part of the Company's advertisement system by which information about a Facebook user's purchases from third-party websites would be provided to Facebook after the transaction

occurred. Facebook then publicized this information to the user's Facebook "friends" via News Feed, which would include the user's name, what they did (*i.e.* purchased an item), what they purchased, and where they purchased the item.

102. *TechCrunch* reported at the time, "Beacon is the internal project name at Facebook around an effort to work with third parties and ***gain access to very specific user data***." (Emphasis added). According to *TechCrunch*, third parties supply this data to Facebook "without compensation; what they get in return is a link back in the News Feed (which is effectively a free ad). Facebook, of course, gets incredibly valuable data about the user." *TechCrunch* noted that this data could be used to serve targeted ads back to users "in various other places on Facebook and elsewhere."

103. On November 2, 2007, *TechCrunch* also noted that there had been "endless speculation around the new advertising network that Facebook will be launching[,]" but that "a leaked Facebook document makes at least one part of the network clear. Facebook is going to be gunning hard to get lots and lots of third-party data about its users into its database."

104. The Individual Defendants pursued their strategy of monetizing the Facebook Platform by (i) forming partnerships with third-party companies, (ii) utilizing third-party developers to obtain as much user data as possible, and (iii) acquiring competitors.

105. FriendFeed: Facebook acquired FriendFeed in 2009 for $47.5 million. FriendFeed was a social media platform that created a number of features that Facebook subsequently popularized, such as the "Like" button, and News Feed, which was the first time that the website actively updated users with news (about their Facebook "friends'" activities) in real-time.

106. Instagram: In 2012, Facebook acquired Instagram, a photo and video-sharing application, after Zuckerberg had famously agreed to the $1 billion purchase price in its founder's living room, without consulting the rest of the Board. "By the time Facebook's board was brought in, the deal was all but done," according to *The Wall Street Journal*. The Board, reportedly, "was told, not consulted." Facebook and Instagram share data to better target advertising to consumers, including location data, interests and past searches.

107. Face.com: In 2012, Facebook acquired Face.com, which pioneered facial recognition technology on mobile devices, for a reported $100 million. Facebook uses Face.com's technology to power its photo-tagging feature, which allows users to receive quick and accurate suggestions on who to tag in their photos.

108. Onavo: Facebook acquired Onanvo in October 2013. Onavo has two parts: a consumer-facing app that helps improve application and data performance on Android and iOS devices, and an analytics business, which giving mobile

publishers tools to track how well their applications are performing, compared to the competition.

109. Atlas: Facebook acquired Atlas from Microsoft in 2013 and relaunched it the following year with a focus on what it calls "people-based marketing" – namely, the ability for advertisers to track users across devices. In short, Atlas tracks the relationship between Facebook's online advertising and actual offline sales.

110. Oculus: Facebook acquired Oculus, a virtual reality ("VR") device maker, in 2014 for $2 billion. According to defendant Zuckerberg, the goal was to first develop immersive VR gaming and then expand to include all sorts of virtual experiences, including social networking. Facebook operates Oculus through Oculus Ireland Limited.

111. WhatsApp: Facebook acquired WhatsApp in 2014 for $19 billion. Notably, former Facebook director and defendant Koum is the co-founder and was CEO of WhatsApp until April 2018. WhatsApp is the preferred instant messaging platform in the developing world.

B. THE INDIVIDUAL DEFENDANTS TRANSITIONED FACEBOOK'S ADVERTISING BUSINESS TO MOBILE DEVICES BEGINNING IN 2011, AND THE COMPANY'S REVENUES SKYROCKETED

112. In 2011 and 2012, to transition Facebook from its collapsing desktop advertising business to mobile advertising, Zuckerberg and others in senior

management implemented a strategy to leverage user data through though what they called "reciprocity." "Reciprocity" meant that Facebook shared user data with over fifty (50) companies, pursuant to agreements that, for the most part, are still in effect. The plan involved obtaining additional data about Facebook users and non-users from third parties, including data brokers, and leveraging data that Facebook obtained through relationships and agreements with other third-party companies.

113. In 2012, most of Facebook's revenue came from generic banner ads delivered to users visiting the Company's website on a desktop computer. By the fourth quarter of 2013, fifty-three percent (53%) of the Company's advertising revenue came from targeted advertisements that Facebook delivered to smartphones, tablets, and other mobile devices, with many of those ads highly targeted by gender, age and other user demographics. "I think it's inarguable that Facebook is a mobile-first company," Facebook's Chief Financial Officer said in an interview at the time.

114. Facebook had total revenue of $2.59 billion in the quarter that ended December 31, 2013, up from $1.59 billion in the same quarter the previous year. Revenue from advertising was $2.34 billion, up 76 percent from the previous year. Excluding compensation costs related to Facebook's initial public offering ("IPO") in 2012, the Company's profits were up 83 percent. "It's hard to see any flaws in

this quarter," commented one analyst, Ron Josey of JMP Securities. "They're seeing demand for their ad product go through the roof."

FACEBOOK PURCHASED DATA FROM THIRD-PARTY DATA BROKERS SINCE AT LEAST 2012

C. 115. Beginning in or around 2012, Facebook obtained information from data collection companies like Datalogix, Acxiom, Epsilon, and BlueKai, which collect information about consumers through store loyalty cards, mailing lists, public records information (including home or car ownership), browser cookies, and other devices. Facebook combined its user information with the information obtained from these companies to generate more information about Facebook users and to enhance its targeted advertising services.

116. A *ProPublica* blog post dated December 27, 2017, titled "Facebook Doesn't Tell Users Everything It Really Knows about Them," reported that "Facebook has been working with data brokers since 2012 when it signed a deal with Datalogix." This prompted Jeffrey Chester, executive director of the privacy advocate Center for Digital Democracy, to file a complaint with the FTC alleging that Facebook had violated the Consent Decree with the agency on privacy issues. Facebook was "not being honest," said Chester. "Facebook is bundling a dozen different data companies to target an individual customer, and an individual should have access to that bundle as well." The FTC did not publicly respond to that

complaint, and Facebook subsequently signed deals with five other data brokers.

117. When asked by ProPublica about the lack of disclosure by Facebook concerning the data bundling practices, Facebook responded that users can discern the use of third-party data if they know where to look. The Company said it does not disclose the use of third-party data on its general page about ad targeting because the data is widely available and was not collected by Facebook. "Our approach to controls for third-party categories is somewhat different than our approach for Facebook-specific categories," said Steve Satterfield, a Facebook manager of privacy and public policy. "This is because the data providers we work with generally make their categories available across many different ad platforms, not just on Facebook." Satterfield said users who don't want that information to be available to Facebook should contact the data brokers directly. Satterfield further said users can visit a page in Facebook's help center, which provides links to the opt-outs for six data brokers that sell personal data to Facebook.

118. However, as ProPublica noted, "[l]imiting commercial data brokers' distribution of your personal information is no simple matter." Basically, a Facebook user would need to opt out in at least three different places: with Acxiom, Datalogix, and Epsilon. However, BlueKai did not offer a direct way to opt out, and Acxiom required people to send the last four digits of their Social Security number to obtain their data. Further, because Facebook changes its

providers from time to time, users would have to regularly visit the help center page to protect their privacy. Most shocking, however, is ProPublica's report that, "[f]or non-Facebook users whose data had been involuntarily collected, individuals are directed to creating a Facebook account, and accessing the account settings in order to view the data collected by the social media platform."

119. ProPublica's investigation confirmed that limiting commercial data brokers' distribution of your personal information is no simple matter. For instance, opting out of Oracle's Datalogix, which provides about three hundred fifty (350) types of data to Facebook according to our analysis, requires "sending a written request, along with a copy of government-issued identification" in postal mail to Oracle's chief privacy officer.

120. ProPublica's report also indicated that one reporter (Julia Angwin) had actually tried to do what Facebook suggested; Ms. Angwin tried in 2013 to opt out from as many data brokers as she could. Of the ninety-two (92) brokers she identified that accepted opt-outs, sixty-five (65) of them required her to submit a form of identification such as a driver's license. In the end, she could not remove her data from the majority of providers.

121. Facebook entered into a data-matching deal with Datalogix, a U.S.-based data-mining company that collects information about consumer behavior from more than 1,000 offline retailers, as part of a larger expansion of advertising

based on the personal information of Facebook users. Under the deal terms, Facebook allowed Datalogix to match the personal information of Facebook users with personal information held by Datalogix in order to track Facebook users' offline commercial activity.

122. According to the Electronic Privacy Information Center ("EPIC"), Facebook did not attempt to notify users of its decision to disclose user information to Datalogix. Further, EPIC has indicated that neither Facebook's data use policy nor its statement of rights and responsibilities adequately explain the specific types of information Facebook discloses, the manner in which the disclosure occurs, or the identities of the third parties receiving the information.

D. THE BOARD INCREASED FACEBOOK'S LOBBYING EXPENDITURES AND EFFORTS TO INFLUENCE LEGISLATORS RATHER THAN ADOPTING REASONABLE PRIVACY PRACTICES TO PROTECT USERS AND COMPLY WITH EXISTING LAWS

123. Beginning in 2011, the Board sharply increased Facebook's lobbying expenditures in an effort to influence key bills and regulations that threatened to prohibit the type of data gathering and information sharing that the Individual Defendants' strategy of targeted advertising services – and its revenues – depended upon. In 2011, Facebook's efforts centered largely on Federal policy involving Internet privacy. The Individual Defendants targeted several existing privacy laws slated for updates in 2011, including the Children's Online Privacy Protection Act,

the Electronic Communications Privacy Act, and the Communications Assistance for Law Enforcement Act. Facebook lobbied against policies relating to location-based services, including the proposed Location Privacy Protection Act, and lobbied against two other bills, the Do-Not-Track Online Act and the Personal Data Privacy and Security Act, which (i) proposed creating a mechanism for allowing people to easily opt out of behavioral tracking online and (ii) increased penalties for unauthorized access to data containing personal information.

124. The Board characterized Facebook's lobbying efforts and expenditures as a general push to raise awareness about its functions and overall goals, but were purposefully vague about what those goals were, and deliberately failed to disclose that the "service" the Board sought to protect was Facebook's advertising service that generated nearly all of its revenue; protecting Facebook's users was not a priority. As Facebook spokesman Andrew Noyes stated:

> "This increase represents a continuation of our efforts to explain how our service works as well as the important actions we take to protect people who use our service and promote the value of innovation to our economy."

125. At the time, John Simpson, Director of the nonprofit Consumer Watchdog's privacy project, called Facebook's increased spending on lobbying and hiring of Washington "heavy-hitters" a worrying development. Facebook, he said, was moving farther away from protecting consumers. "When large corporations spend big dollars to get their agenda through, it is not at all a positive

sign for their customers or consumers," Simpson said.

Simpson further said:

> The troubling thing is that these guys have a record of overstepping and overreaching on privacy issues, and they haven't been at all responsible about protecting users.

126. In 2012, Facebook spent record amounts to lobby Congress on privacy and cybersecurity legislation. Again, the Individual Defendants attempted to explain away Facebook's lobbying as a means to protect users, while Facebook aggressively lobbied against legislation that would have decreased Facebook's profits by increasing privacy controls and children's online safety. "Our presence and growth in Washington reflect our commitment to explaining how our service works, the actions we take to protect the more than 900 million people who use our service, the importance of preserving an open Internet, and the value of innovation to our economy," a Facebook representative said in a statement. In total, Facebook spent nearly $4 million on its lobbying efforts in 2012.

127. In 2013, Facebook spent a Company record $2.45 million in the first quarter to lobby federal lawmakers and regulators on the same cybersecurity and children's privacy issues.

128. Facebook set a new company record for lobbying expenditures again in the first quarter of 2014, as the Individual Defendants continued their attempts to influence federal lawmakers on similar cybersecurity issues and issues relating

to "government surveillance," according to Facebook's disclosures.

129. Facebook's lobbying expenditures continued over the next few years until the Cambridge Analytica scandal exposed the seriously inadequate privacy controls at the Company. On April 12, 2018, it was announced that Facebook was backing off its opposition to a proposed ballot initiative in California that would allow consumers to find out more information about (and have more control over) the way businesses collect, use, share and sell their personal data.

IV. THE BOARD FAILED TO ENFORCE FACEBOOK'S STATED POLICIES AND TURNED A BLIND EYE TO REPEATED VIOLATIONS OF DATA PRIVACY LAWS

130. The Board was required to ensure Facebook's compliance with the Consent Decree and other applicable laws. The Board was also required to implement and monitor a reasonable system of internal controls and policies relating to user privacy and data security at Facebook.

131. Notwithstanding the Board's heightened duties under the Consent Decree to oversee Facebook's compliance with pertinent data privacy laws and regulations, the Individual Defendants failed to ensure that Facebook implemented adequate internal controls and reporting systems that would detect and prevent violations of law similar to those which gave rise to the Consent Decree.

132. Since the Cambridge Analytica scandal, it has been reported that the Individual Defendants continue to ignore reports of data sharing and exfiltration of

Facebook information and user data.

133. On June 29, 2018, MobileMarketing Magazine reported that a security researcher had discovered a third-party app called NameTest had accessed the data of up to one hundred twenty (120) million Facebook users that was left exposed as recently as the previous month.

134. The security researcher, Inti De Ceukelaire ("De Ceukelaire") said he discovered and reported the incident to Facebook via its Data Abuse Bounty Program on April 22, 2018, but the Company did not respond for eight (8) days. When De Ceukelaire contacted Facebook again on May 14, 2018 to see if the Company had contacted NameTest's developers, another eight (8) days passed before De Ceukelaire was later told it could potentially take Facebook three to six months to investigate the issue. According to De Ceukelaire, NameTest fixed the issue first, on June 25, 2018, and De Ceukelaire had to chase someone down again at Facebook to acknowledge the fix and confirm his $8,000 reward under the program.

135. De Ceukelaire said he installed the NameTest application which, like Kogan's "thisisyourdigitallife" application, is a personality test. After De Ceukelaire tried it, he tracked how his data was being processed and said he discovered that his personal information, along with that of every other person who had taken the quiz, was being held in a JavaScript file that could easily be

requested by any website that knew to ask. In addition to enabling any site to request data points, NameTest provided those who requested information with an access token that would allow continued access to a user's posts, photos and friends' data for up to two months.

136. De Ceukelaire said:

> Depending on what quizzes you took, the JavaScript could leak your Facebook ID, first name, last name, language, gender, date of birth, profile picture, cover photo, currency, devices you use, when your information was last updated, your posts and statuses, your photos and your friends.

137. De Ceukelaire further said:

> If you ever took a quiz and removed the app afterwards, external websites would still be able to read your Facebook ID, first name, last name, language, gender, date of birth. You would have only prevented this from happening if you manually deleted your cookies, as the website does not offer a logout functionality.

138. On June 27, 2018, De Ceukelaire posted the following "Timeline of Events," along with Facebook's response, on his blog:[9]

- On April 22nd, I reported this to Facebook's Data Abuse program.
- On April 30th, I received an initial response from Facebook, stating that they're still looking into it.
- On May 14th, I sent a follow-up mail, asking whether they already reached out to the app developers.

[9] De Ceukelaire, Inti, *This Popular Facebook App Exposed Your Data For Years* (2018), https://medium.com/@intideceukelaire/this-popular-facebook-app-publicly-exposed-your-data-for-years-12483418eff8 (last visited Apr. 30, 2019).

- On May 22th, Facebook said that it could take three to six months to investigate the issue (as mentioned in their initial automated reply) and that they would keep me in the loop. At this time, the NameTests quizzes were still up and running.

- On June 25th, I noticed NameTests had changed the way they process data. Third-parties could no longer access its users' personal information. I contacted them about the fix, told them about this blogpost and asked them to donate the bounty to Freedom of the Press Foundation.

- On June 26th, I reached out to NameTest's Digital Protection Officer to answer some questions regarding the vulnerability and the disclosure process by Facebook.

- On June 27th, Facebook informed me they donated $8,000 ($4,000 bounty, doubled because I chose to donate it to charity) to the Freedom of the Press foundation as part of their data abuse bounty program.

139. The most recent reports confirm that the Individual Defendants continue to turn a blind eye to Facebook's internal control failures and have further exposed the Company to potential violations of the Consent Decree.

A.

THE INDIVIDUAL DEFENDANTS MAINTAINED POLICIES THAT PERMITTED DEVELOPERS TO OBTAIN FACEBOOK USERS' PERSONAL INFORMATION

140. Since 2007, Facebook has allowed outside developers to build and offer their own applications within its space. Facebook's 2013 Data Use Policy states, in relevant part:

> 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.

(https://www.facebook.com/full_data_use_policy).

141. Despite this policy, developers could generally launch applications on the Facebook Platform without affirmative approval or review by Facebook. Facebook allowed third-party application developers to use the Facebook API to download a user's friends and friendships.

142. Facebook's API allowed developers to access a Facebook user's and the user's Facebook "friend's" account information through "extended profile properties."

143. The availability of extended profile properties show that Kogan, like other developers that utilized Facebook's API, could access Facebook users' personal information, consistent with the Company's policies permitting such third-party access.

B. FACEBOOK EXPANDED GRAPH API IN 2014 AND ALLOWED THIRD-PARTY DEVELOPERS TO ACCESS USERS' INBOXES ON FACEBOOK MESSENGER

144. In 2014 Facebook expanded Facebook's Graph API and policies so that application developers could get data off the platform by asking for a "read mailbox" permission, which allowed them access to a user's inbox. That was just one of a series of extended permissions granted to developers under version 2.0 of Graph API.

145. Facebook confirmed to *The Register* that this access had been requested by the application developers and that a small number of people had granted it permission. "In 2014, Facebook's platform policy allowed developers to request mailbox permissions but only if the person explicitly gave consent for this to happen," a Facebook spokesperson stated. Facebook tried to downplay the significance of the eyebrow-raising revelation, saying it was at a time when mailboxes were "more of an inbox", and claimed it was mainly used for apps offering a combined messaging service. The spokesperson said:

> At the time when people provided access to their mailboxes – when Facebook messages were more of an inbox and less of a real-time messaging service – this enabled things like desktop apps that combined Facebook messages with messages from other services like SMS so that a person could access their messages all in one place.

146. On May 22, 2014, Facebook announced an expanded "privacy checkup" tool that would enable users to review the privacy of "key pieces of information" on their profiles, as well as a change to the default sharing setting for new members' first post from "public" to "friends. First-time posters will also see a reminder to choose an audience for their first post, although the company stressed that the new default "friend" setting will apply even if they don't make an audience choice. "Users will also still be able to change the intended audience of a post at any time, and can change the privacy of their past posts as well," Facebook's website post added.

147. A *Law360* article noted that Facebook's changes to the privacy practices were prompted by the approval of a contested $20 million privacy settlement that required the Company to make changes to its policies in order to give minor and adult users more information about how their names and likenesses are employed in connection with ads displayed through the site's Sponsored Stories program and that, contrary to Facebook's statement on its website, they were not changes Facebook had "elected" to make on its own.[10]

148. On November 13, 2014, Facebook announced it would give users

[10] Law360, *Facebook Debuts Changes to Curb Unwanted Data Sharing* (2014), https://www.law360.com/articles/540616/facebook-debuts-changes-to-curb-unwanted-data-sharing (last visited April 30, 2019).

more information about how their data is being collected and used, rolling out privacy policy changes that allow the site to do more with location and transactional data and implementing new controls that enable users to limit the ads they see.

149. The updates included explaining that Facebook will soon begin showing users that share location information menus from restaurants nearby or friends in the area, and clarifying that it will ask for permission to use a phone's location to offer optional features like check-ins or adding locations to posts. The policy changes also revealed that Facebook was testing a "buy" button to help people discover and purchase products without leaving the site, as part of its foray into mobile payments, and provide more information about how the company's growing family of companies and apps — which now included services such as Instagram and WhatsApp — work together.

150. The policy updates did not amend the way Facebook collects or shares data with advertisers — including Facebook's recently announced plan to leverage data culled from outside websites and applications members visit, supposedly to serve them with more relevant ads. Rather, they confirm that the Individual Defendants actually encouraged the same practices that enabled Cambridge Analytica to obtain the personal information of at least eighty-seven (87) million Facebook users without their knowledge and informed consent.

151. Further, it was not until April 2015 that Facebook turned off the permission that allowed developers to access a Facebook user's inbox, following pressure from privacy activists – but much to the disappointment of developers – and the changelog on Facebook's website shows that "read_mailbox" wasn't deprecated, i.e., remained usable, until October 6, 2015.

C. THE INDIVIDUAL DEFENDANTS FALSELY ASSURED FACEBOOK'S USERS THAT THEY COULD TRUST FACEBOOK TO PROTECT THEIR PERSONAL INFORMATION

152. The Individual Defendants recognized the importance of maintaining user trust and repeatedly emphasized in public statements that privacy and data security are critically important to Facebook's brand.

153. Throughout the relevant period, the Individual Defendants emphasized the importance of user privacy to Facebook's revenues and business. At the same time, the Individual Defendants concealed the fact that the Company's policies allowed third-party developers to obtain massive amounts of Facebook users' personal information without verification as to the nature of its use. The Individual Defendants claimed to protect this information by reasonable efforts to maintain its privacy.

154. Facebook's Data Policy states:

> We will never sell your information to anyone. We have a responsibility to keep people's information safe and secure, and we

> impose strict restrictions on how our partners can use and disclose data. We explain all of the circumstances where we share information and make our commitments to people more clear.

155. Maintaining user privacy and data security has long been considered central to Facebook's business and growth prospects. The Individual Defendants have assured users and investors for years that the Company monitors user accounts for precisely the type of leaks that allowed Cambridge Analytica to obtain millions of users' personal information without their knowledge, and to retain such information for years after Facebook claimed to have confirmed that neither Cambridge Analytica nor any unauthorized person or entity associated with it was in the possession of any misappropriated user data.

156. For instance, a June 21, 2013 blog post entitled "Important Message from Facebook's White Hat Program" states:

> At Facebook, we take people's privacy seriously, and we strive to protect people's information to the very best of our ability. We implement many safeguards, hire the brightest engineers and train them to ensure we have only high-quality code behind the scenes of your Facebook experiences. We even have teams that focus exclusively on preventing and fixing privacy related technical issues before they affect you…. Your trust is the most important asset we have, and we are committed to improving our safety procedures and keeping your information safe and secure.

157. The Individual Defendants repeatedly emphasized the importance of data security and privacy to the Company in Facebook's public statements, and acknowledged their specific responsibility for overseeing the substantial risks that

a breach, like the Cambridge Analytica debacle, posed to the Company. According to 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.

D. THE INDIVIDUAL DEFENDANTS WERE WARNED ABOUT DATA SECURITY ISSUES IN 2012 BY WHISTLEBLOWER SANDY PARAKILAS BUT DID NOTHING

158. In testimony to the House of Commons' Digital, Culture, Media and Sport committee ("DCMSC"), Sandy Parakilas, a former Facebook platforms operations manager for policing data breaches by third-party software developers between 2011 and 2012, stated that hundreds of millions of Facebook users are likely to have had their private information harvested by companies that exploited the same means as the firm that collected data from Facebook users and passed it on to Cambridge Analytica. Parakilas stated that in 2012 he warned senior executives at the company that its lax approach to data protection risked a major breach: "My 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," Parakilas said. When asked what kind of

control Facebook had over the data accessed by outside developers, Parakilas replied: "Zero. Absolutely none. Once the data left Facebook servers there was not any control, and there was no insight into what was going on." According to Parakalis, the Company did not use enforcement mechanisms, including audits of external developers, to ensure data was not being misused. Parakilas confirmed 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. Or, in Parakilas' own words, "[Facebook] felt that it was better not to know."

159. Parakilas testified that he had created a PowerPoint presentation warning about the areas where the Company was exposed and user data was at risk, and that he had shared the presentation with Facebook's senior executives, but they ignored his concerns. According to Parakilas, "it was known and understood … that there was risk with respect to the way that Facebook Platform was handling data" but "it was a risk that they were willing to take."

160. Parakilas also related how he discovered a social games developer using Facebook data to automatically generate profiles of children without their consent, and another developer asking permission to gain access to a user's Facebook messages and posted photos. In an Op-Ed in *The New York Times*,

Parakilas stated that when he reported these incidents to his superiors, they didn't care at all:

> At a company that was deeply concerned about protecting its users, this situation would have been met with a robust effort to cut off developers who were making questionable use of data. But when I was at Facebook, the typical reaction I recall looked like this: try to put any negative press coverage to bed as quickly as possible, with no sincere efforts to put safeguards in place or to identify and stop abusive developers. When I proposed a deeper audit of developers' use of Facebook's data, one executive asked me, 'Do you really want to see what you'll find?' The message was clear: The company just wanted negative stories to stop. It didn't really care how the data was used.

E. THE INDIVIDUAL DEFENDANTS KNEW ABOUT THE CAMBRIDGE ANALYTICA "BREACH" IN 2015 BUT CONCEALED THE "BREACH" AND FAILED TO ACT

161. In his testimony to Congress, Zuckerberg admitted that he had learned about Cambridge Analytica's unauthorized use of Facebook user data by at least 2015:

> Ms. Eshoo: …When did Facebook learn that? And when you learned it, did you contact their CEO immediately, and if not, why not?
>
> Mr. Zuckerberg: Congresswoman, yes. When we learned in 2015 that a Cambridge University researcher associated with the academic institution that built an app that people chose to share their data with –
>
> Ms. Eshoo. We know what happened with them, but I am asking you.
>
> Mr. Zuckerberg. Yes, I am answering your question.
>
> Ms. Eshoo. Right.

Mr. Zuckerberg. When we learned about that, we immediately –

Ms. Eshoo. So, in 2015, you learned about it?

Mr. Zuckerberg. Yes.

162. Zuckerberg took no action at the time, nor did anyone else at Facebook, until more than two years *after* he learned of Cambridge Analytica's unauthorized use of Facebook user data.

163. Even after learning of the misappropriation of Facebook users' data by Cambridge Analytica in 2015, per Zuckerberg's own testimony before Congress, neither Zuckerberg nor Sandberg, nor any of the other Individual Defendants, ensured that Facebook users were properly notified that their personal information had been compromised in accordance with applicable notification and disclosure laws. To the contrary, with knowledge of the practices that allowed Cambridge Analytica to access and copy Facebook's data, the Individual Defendants downplayed concerns about access to user information when addressing Facebook's role in the 2016 U.S. election and subsequent elections worldwide. The Individual Defendants denied that Facebook had experienced any illicit data leaks or security breaches, and continued to assure investors that Facebook maintained effective" internal controls and systems that automatically detected and appropriately flagged "suspicious activity."

164. The Individual Defendants also publicly affirmed the Company's

commitment to continually monitor and improve its data security systems.

A Facebook spokesman said in a statement to *The Guardian* in 2015:

> [M]isleading 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.

165. When the truth came out in 2018, Facebook representatives insisted that Kogan had violated Facebook policies. In a statement posted to the Company's Newsroom on March 16, 2018, a Facebook attorney said that Kogan had "gained access to this information in a legitimate way and through the proper channels," but "violated Facebook's platform policy" by "passing information on" to third parties, including Cambridge Analytica. As a result, Kogan's application was removed from Facebook and "all parties" who received the data from Kogan were required to certify that it had been destroyed in 2016.

166. According to Facebook:

> Facebook obtained written certifications from Dr. Kogan, GSR, and other third parties declaring that all such data they had obtained was accounted for and destroyed. In March 2018, after Mr. Milner's testimony, Facebook received information from the media suggesting that the certifications we [Facebook] received may not have been accurate… As part of our investigation, we have hired a forensic auditor to understand what information Cambridge Analytica had and whether it has been destroyed.

167. Although three years was more than enough time for Facebook to confirm the authenticity and accuracy of the certifications, it did not. Further, the

letter agreement that Facebook sent to Kogan and GSR regarding the destruction of the data and their "certifications" does not appear to have been signed by anyone at Facebook, suggesting that no one followed up until the truth came out in 2018, and that the agreement to destroy the data could potentially be invalid.

168. After *The Observer* asked Facebook to comment just a few days prior to breaking the news of the Cambridge Analytica leak, Facebook announced that it was (finally) suspending Cambridge Analytica and Kogan from the platform pending further information over misuse of data. Facebook also said it was suspending Wylie from accessing the platform while it carried out its internal investigation, despite his role as a whistleblower.

169. Just one month earlier, in February 2018, both Facebook and the CEO of Cambridge Analytica, Alexander Nix ("Nix"), had told a U.K. parliamentary inquiry on fake news that the company did not have or use private Facebook data. Nix told officials: "We do not work with Facebook data and we do not have Facebook data."

Simon Milner, Facebook's U.K. policy director, when asked if Cambridge Analytica had Facebook user data, told U.K. officials:

> They may have lots of data but it will not be Facebook user data. It may be data about people who are on Facebook that they have gathered themselves, but it is not data that we have provided.

170. Notwithstanding their significant obligations as members of the Board

or corporate officers, and (for some of the Individual Defendants) as members of committees charged with overseeing Facebook's risk exposure, corporate governance, and other critical aspects of the Company's business and operations, the Individual Defendants maintained policies that allowed Kogan and other third-party application developers to obtain mass amounts of Facebook user information without verification as to the nature of its use, and upon learning that fifty (50) million users' personal information had been misappropriated and used by Cambridge Analytica, failed to notify users or disclose anything about the misappropriation and use, or its significant impact on the Company, publicly and to investors. Worse, the Individual Defendants affirmatively misrepresented and concealed these facts from the Company's regulators and in public statements and filings with the SEC.

171. The Individual Defendants' failure to detect and prevent the Cambridge Analytica leak, or to adequately respond with proper notification and disclosures in accordance with best practices and applicable laws, belies any claim that Facebook's actual "monitoring" practices and internal controls were sufficient. In fact, Facebook's statements throughout the relevant period indicate that the Individual Defendants sought to conceal the deficiencies in Facebook's user privacy data security practices through materially false and misleading statements denying that any such leak had ever occurred and falsely assured that Facebook

maintained effective internal controls.

172. For example, a October 16, 2015 post by Stamos, Facebook's Chief Information Security Officer, stated:

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

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

Company's best interests, and noted the purportedly indirect effects maintaining user privacy has on Facebook's revenues. Bosworth wrote:

> Yes developers can receive data that helps them provide better experiences to people, but we don't make money from that directly and have set this up in a way so that no one's personal information is sold to businesses.

Bosworth further wrote:

> If people aren't having a positive experience connecting with businesses and apps then it all breaks down. This is specifically what I mean when we say our interests are aligned with users when it comes to protecting data.

174. On March 22, 2018, *The Guardian* reported, "Facebook provided the dataset of 'every friendship formed in 2011 in every country in the world at the national aggregate level' to Kogan" for a study on international friendships that was co-authored by two Facebook employees in 2015. Further, a University of Cambridge press release concerning the study's publication noted that the paper was "the first output of ongoing research collaborations between [Kogan's] lab in Cambridge and Facebook."

175. Wylie, a Canadian data analytics expert who worked with Cambridge Analytica and Kogan to create the app, also provided evidence about the data misuse to *The Observer*, the U.K.'s National Crime Agency's cybercrime unit, and the Information Commissioner's Office, including emails, invoices, contracts and bank transfers that reveal more than fifty (50) million profiles – mostly belonging

to registered U.S. voters – were obtained from Facebook, and Wylie said the Company was aware of the volume of data being pulled by Kogan's app. "Their security protocols were triggered because Kogan's apps were pulling this enormous amount of data, but apparently Kogan told them it was for academic uses," Wylie said. "So they were like: 'Fine.'"

176. The evidence Wylie supplied to U.K. and U.S. authorities includes a letter from Facebook lawyers sent to him in August 2016, asking him to destroy any data he held that had been collected by GSR, the company set up by Kogan to "harvest" the profiles. "Because this data was obtained and used without permission, and because GSR was not authorized to share or sell it to you, it cannot be used legitimately in the future and must be deleted immediately," the letter said. According to Wylie, Facebook did not pursue a response when the letter initially went unanswered for weeks because Wylie was travelling, nor did it follow up with forensic checks on his computers or storage.

> That to me was the most astonishing thing. They waited two years and did absolutely nothing to check that the data was deleted. All they asked me to do was tick a box on a form and post it back.

177. On March 27, 2018, Wylie testified before a U.K. Parliamentary Committee that is investigating "Fake News." According to Wylie, the personal information that Kogan's app was able to obtain via Facebook formed the "foundational dataset" underpinning Cambridge Analytica and its targeting

models. “This is what built the company,” he claimed. “This was the foundational dataset that then was modeled to create the algorithms.”

178. When asked by the Parliamentary Committee how the data was used by Cambridge Analytica, Wylie said the company’s approach was to target different people for advertising based on their “dispositional attributes and personality traits” — traits it sought to predict via patterns in the data. Wylie explained:

> For example, if you are able to create profiling algorithms that can predict certain traits — so let’s say a high degree of openness and a high degree of neuroticism — and when you look at that profiles that’s the profile of a person who’s more prone towards conspiratorial thinking, for example, they’re open enough to kind of connect to things that may not really seem reasonable to your average person. And they’re anxious enough and impulse [sic] enough to start clicking and reading and looking at things — and so if you can create a psychological profile of a type of person who is more prone to adopting certain forms of ideas, conspiracies for example, you can identify what that person looks like in data terms.
>
> You can then go out and predict how likely somebody is going to be to adopt more conspiratorial messaging. And then advertise or target them with blogs or websites or various — what everyone now calls fake news — so that they start seeing all of these ideas, or all of these stories around them in their digital environment. They don’t see it when they watch CNN or NBC or BBC. And they start to go well why is that everyone’s talking about this online? Why is it that I’m seeing everything here but the mainstream media isn’t talking about [it]…
>
> Not everyone’s going to adopt that — so that advantage of using profiling is you can find the specific group of people who are more

> prone to adopting that idea as your early adopters… So if you can find those people in your datasets because you know what they look like in terms of data you can catalyze a trend over time. But you first need to find what those people look like.[11]

179. "That was the basis of a lot of our research [at Cambridge Analytica and sister company SCL]," Wylie added in his statements to the Parliamentary Committee. "How far can we go with certain types of people. And who is it that we would need to target with what types of messaging." Wylie told the Committee that Kogan's company was set up exclusively for the purposes of obtaining data for Cambridge Analytica, and said the firm chose to work with Kogan because another professor it had approached first had asked for a substantial payment up front and a 50% equity share — whereas he had agreed to work on the project to obtain the data first, and consider commercial terms later.

180. Wylie also suggested Facebook found out about the data harvesting project as early as July 2014 —around the time Kogan had told him that he had spoken to Facebook engineers after his application's data collection rate had been throttled by the platform. "He told me that he had a conversation with some engineers at Facebook," said Wylie.

Wylie further stated:

So Facebook would have known from that moment about the project

[11] Lomas, Natasha, *Facebook Data Misuse Scandal Affects "Substantially" More Than 50 Million, Claims Wylie* (2018), https://techcrunch.com/2018/03/27/facebook-data-misuse-scandal-affects-substantially-more-than-50m-claims-wylie/ (last visited Apr. 30, 2019).

> because he had a conversation with Facebook's engineers — or at least that's what he told me… Facebook's account of it is that they had no idea until *The Guardian* first reported it at the end of 2015 — and then they decided to send out letters. They sent letters to me in August 2016 asking do you know where this data might be, or was it deleted?

Wylie noted:

> [i]t's interesting that… the date of the letter is the same month that Cambridge Analytica officially joined the Trump campaign. So I'm not sure if Facebook was genuinely concerned about the data or just the optics of y'know now this firm is not just some random firm in Britain, it's now working for a presidential campaign.

181. When asked whether Facebook made any efforts to retrieve or delete data, Wylie responded, "No they didn't." It was not until Facebook's image was threatened in 2018, "after I went public and then they made me suspect number one" that Wylie said he had heard anything from the Company. Wylie said that he suspected that when Facebook looked at what happened in 2016:

> "they went if we make a big deal of this this might be optically not the best thing to make a big fuss about…. So I don't think they pushed it in part because if you want to really investigate a large data breach that's going to get out and that might cause problems. So my impression was they wanted to push it under the rug."

He added, "[a]ll kinds of people [had] access to the data. It was everywhere."

182. In his testimony to the committee, Wylie discussed a connection between Cambridge Analytica and Palantir, a company that was co-founded in

2003 by Thiel. Palantir is known for providing government agencies and organizations with analytics, security and other data management solutions. According to Wylie, Palantir staff helped Cambridge Analytica build models based on the Facebook data. "That was not an official contract between Palantir and Cambridge Analytica but there were Palantir staff who would come into the office and work on the data," Wylie stated.

> And we would go and meet with Palantir staff at Palantir. So, just to clarify, Palantir didn't officially contract with Cambridge Analytica. But there were Palantir staff who helped build the models that we were working on.

183. Initially in response to a request for comment on Wylie's testimony, *TechCrunch* reported on March 27, 2018 that a Palantir spokesperson had denied the connection entirely in an emailed statement: "Palantir has never had a relationship with Cambridge Analytica nor have we ever worked on any Cambridge Analytica data." According to *The New York Times*, Palantir subsequently issued a revised statement: "We learned today that an employee, in 2013-2014, engaged in an entirely personal capacity with people associated with Cambridge Analytica," a Palantir representative said. "We are looking into this and will take the appropriate action."

184. On May 16, 2018, Jeff Silvester ("Silvester"), the Chief Operating Officer of AggregateIQ ("AIQ"), provided evidence to the DCMSC.

185. Silvester is a co-founder of AIQ, which was founded to "to provide IT

and web services to help [political] campaigns use technology to better organize operations." Until 2015, SCL was AIQ's largest client.

186. According to Silvester, AIQ's business involves "creating and placing online ads through platforms like Facebook[.]" In his testimony, Silvester explained, "The Facebook advertising platform provides all the necessary information and tools based on current and relevant FB information…"

He further explained:

> Facebook provides a platform that allows an advertiser to show ads to its users based on criteria such as demographic information …. And interests that people may have identified on Facebook. All of this allows a campaign to run a very complex and comprehensive advertising campaign without the need for any external information.
>
> [With that info] 'We would place this information on the Facebook platform along with the ads that we create at the direction of the client. Each ad consists of a picture, often with a few words on it, along with some descriptive text and a link to the webpage should someone click on the ad. We also sometimes assist in creating that web or 'landing' page. We then work with the client to decide how many times people should see these ads and over what time period.
>
> The Facebook platform takes care of the rest, showing these ads to its users and providing reports on how any times the ads have been shown and how many times the ads have been clicked…
>
> Facebook also gives advertisers the ability to count the number of people who might land on a certain webpage on the client site using a piece of code called a pixel. We often help our clients place this pixel code on their site so that the client can measure if a particular ad is reaching its goal to show people a video (versus, for example, signing people up to be on a mailing list).

187. On June 7, 2018, Facebook disclosed that the site "accidentally" made

the posts of fourteen (14) million users public, even when users had designated the posts to be shared with only a limited number of contacts, supposedly the result of a bug that automatically suggested posts be set to "public" (meaning that they could be viewed by anyone, including people not logged on to Facebook, just like any other webpage). As a result, from May 18, 2018 to May 27, 2018, as many as fourteen (14) million users who intended posts to be available only to select individuals were, in fact, accessible to anyone on the Internet. The statement said that Facebook technicians stopped automatically making private posts public on May 22, 2018, but that it took them another five (5) days to fully restore privacy settings for all the affected posts. Facebook did not start notifying the fourteen (14) million users affected by the bug that some of their private posts had been made public until June 7, 2018.

188. Mike Schroepfer, Facebook's Chief Technology Officer, admitted last May that he cannot determine what data has been transferred and shared across Facebook's platform. In an interview on May 30, 2018, Schroepfer stated,

> The problem is we can't observe the actual data transfer that happens there. I don't actually even know physically how the data went from one to the other. There isn't a channel that we have some sort of control over.

189. Worse, notwithstanding Defendants' repeated promises about the importance of privacy and maintaining trust, Schroepfer made clear that Facebook executives continue to blame ***users*** for trusting the Company. Schroepfer stated:

> Well, as a consumer you're ultimately trusting a third party with your data. Whatever data you brought from Facebook, whatever data, you're taking these personality quizzes and you're inputting new data in there. That's a relationship with that developer that you have to trust that they'll be responsible with the data they're using. Whether it's on Facebook or some map you downloaded from an app store, so we didn't observe that until we heard about it through third-party reports.

190. Rather than addressing the underlying problems, and despite the existence of the FTC Consent Decree, the Individual Defendants permitted Facebook to operate lawlessly; the Individual Defendants failed to implement and maintain adequate internal controls and procedures to detect and prevent violations of the Company's policies.

191. On April 11, 2018, Zuckerberg testified before Congress that "[t]he consent decree is extremely important to how we operate the company. . ." However, he and the rest of Facebook's Board of Directors failed to ensure that Facebook complied with the terms of the Consent Decree. Indeed, Zuckerberg's testimony deceptively maintained that Facebook was in substantial compliance with the Consent Decree when he knew it was not.

192. In an interview with the *Washington Post*, David Vladeck, former director of the FTC's Bureau of Consumer Protection, said the Cambridge Analytica incident may have violated Facebook's 2011 consent decree. "I will not be surprised if at some point the FTC looks at this. I would expect them to," he said. Jessica Rich, who also served as director of the Bureau, said:

> Depending on how all the facts shake out, Facebook's actions could violate any or all of these provisions, to the tune of many millions of dollars in penalties. They could also constitute violations of both U.S. and EU laws,' adding, 'Facebook can look forward to multiple investigations and potentially a whole lot of liability here.'

193. Indeed, after news of the Cambridge Analytica scandal broke, Facebook's user privacy and data security practices quickly became the topic of intense scrutiny by U.S. and foreign regulators; multiple government inquiries were launched and are ongoing.

F. U.S. AND FOREIGN GOVERNMENT OFFICIALS COMMENCED INVESTIGATIONS OF FACEBOOK IN RESPONSE TO THE CAMBRIDGE ANALYTICA SCANDAL

194. In the days after the scandal was publicly revealed, the Attorney General of the Commonwealth of Massachusetts announced an investigation into Facebook and Cambridge Analytica. Senator Ron Wyden followed up with a detailed series of questions for Facebook to answer, and Senators Amy Klobuchar and John Kennedy asked the chairman of the Judiciary Committee, Charles E. Grassley, Republican of Iowa, to hold a hearing. Republican leaders of the Senate Commerce Committee, organized by Senator John Thune, also wrote a letter to Zuckerberg demanding answers to questions about how the data had been collected and if users were able to control the misuse of data by third parties. "It's time for Mr. Zuckerberg and the other CEOs to testify before Congress," Senator Mark Warner said. "The American people deserve answers about social media

manipulation in the 2016 election." Zuckerberg eventually testified before Congress on April 10 and 11, 2018.

195. On March 20, 2018, a committee in the British Parliament sent a letter to Zuckerberg and asked him to appear before the panel to answer questions on the Company's connection to Cambridge Analytica. The president of the European Parliament also requested an appearance by defendant Zuckerberg. Damian Collins, chairman of the British committee wrote:

> 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.

"Your officials' answers have consistently understated this risk, and have been misleading to the committee."

196. On March 21, 2018, former Facebook employee Sandy Parakilas, who was a platform operations manager from 2011 to 2012, appeared before the DCMSC, which was investigating the impact of social media on recent elections, and testified about a PowerPoint presentation he had created and shared "with a number of people in the company" outlining his concerns about Facebook's platform. "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." Parakilas said that he "shared that

around with a number of people in the company at the time[,]" including "senior executives in charge of Facebook Platform and people in charge of privacy." When asked by the Chair of the DCMSC if any of those executives were still at the Company, Parakilas said they were, but declined to name them in public.

197. Parakilas also told *The Guardian* on March 20, 2018 that he had warned senior executives at Facebook of the risk that its data protection policies could be breached given the Company's minimal or nonexistent procedures for auditing and enforcing those policies. Parakilas explained, "My concerns were that all of the data that left Facebook servers to developers could not be monitored by Facebook." According to Parakilas, Facebook did not conduct regular audits, and although his primary responsibilities "were over policy and compliance for Facebook apps and data protection, Parakilas said that "during my 16 months in that role at Facebook, I do not remember a single physical audit of a developer's storage." Parakilas "asked for more audits of developers and a more aggressive enforcement regime" Parakilas said he did not get a specific response, but "[e]ssentially, they did not want to do that." According to Parakilas, "the company felt that it would be in a worse legal position if it investigated and understood the extent of abuse, and it did not." The DCMSC Chair commented, "it sounds like they turned a blind eye because they did not want to find out that truth." Parakilas agreed, stating, "That was my impression, yes."

198. In response to a question from the DCMSC regarding how many developers Facebook had taken action against between 2011 and 2014, Rebecca Stimson, Facebook U.K.'s Head of Public Policy, initially replied, "Due to system changes, we do not have records for the time-period before 2014 that establish we terminated for developer violations…" The DCMSC wrote back, "Do you really have no records of developer violations for the time-period before 2014? If you don't have records, would you agree that is a serious omission?"

199. The fact that Facebook has no records of terminating any developers is unsurprising. Although Facebook filed litigation against developers that were falsely premised on policy violations, the truth is that the Individual Defendants did not enforce those violations and only cited them when it would advance their own interests.

1. Facebook's Terms of Use Are Designed to Entice Users to Grant the Company Access to Their Data

200. Facebook's user agreement and associated privacy policies are set forth in the "Terms of Service" available on the Company's website. This document explains the Company's business model and represents the user's relationship with Facebook. The current version of the agreement is meant to inform users about Facebook's intentions with their data and act as the mechanism that gives the Company permission to proceed with its data gathering and data

sharing practices.

201. Facebook's Terms of Service available on its website and in effect on December 1, 2008 prohibited:

> harvest[ing] or collect[ing] email addresses or other contact information of other users from the Service or Site by electronic or other means for the purposes of sending unsolicited emails or other unsolicited communications.

202. In his testimony before Congress, defendant Zuckerberg highlighted that:

> the first line of our Terms of Service says that you control and own the information and content that you put on Facebook…you own [your data] in the sense that you chose to put it there, you could take it down anytime, and you completely control the terms under which it's used.

203. Facebook conceptualizes privacy in terms of control over the data collected, how it is used, and where it goes. The idea is that if a user is gifted with options about their personal data, then the Company must be protecting users' privacy. However, this practice is exactly what allows Facebook to turn people into data spigots.

204. Facebook highlights that users always have the option to "allow" it to collect and process your information. But because Facebook's business depends upon users selecting the "permission" option, their incentive is to use every possible strategy to engineer your consent. The notion of privacy as control benefits Facebook, at the expense of its users, by allowing the Company to

leverage an illusion of agency via terms and settings to keep the data engine humming.

205. Congress seemed to acknowledge these issues during the two-day hearing when Zuckerberg testified in April 2018. Senator Brian Schatz told Zuckerberg that with terms of service at 3,200 words and a privacy policy at 2,700 words, "people really have no earthly idea of what they're signing up for." Facebook's full-length privacy policy would take most people more than 10 minutes to read, though comprehension is another matter altogether. Indeed, some academics have hypothesized that it would take users twenty-five (25) days to read every agreement on every site they've visited.

206. Facebook's policies are so broad as to be meaningless. Facebook's Terms of Use say that Facebook collects almost everything users expose to it, from "things you do and information you provide" and "your networks and connections" to "information from third-party companies." But the availability of knowledge doesn't necessarily translate into meaningfully-informed decisions. In this context, users are being asked to consider the privacy implications of each post they create—an impossibly complex calculation to make about future risks and consequences, particularly given the highly technical issues involved. When combined with Facebook's purposefully ambiguous and unclear representations about its technology and the nature of its business, Facebook's Terms of Use and

overall approach to user privacy seriously oversimplifies risk. The modern data ecosystem is mind-bogglingly complex, with many different kinds of information collected in many different ways, stored in many different places, processed for many different functions, and shared with many other parties.

207. The ambiguous language of Facebook's data policy makes it hard for most users to assess the risks of their data being shared with an abstract "other partner." Did Facebook users anticipate the possibility that eighty-seven (87) million of them would have their information improperly shared with an academic who scraped data from an online quiz and provided it to a dubious data broker who weaponized the data against people in a way that was corrosive to autonomy and democracy? The vast majority of them probably did not. Because it is virtually impossible for Facebook's users to be fully informed of data risks and exert control at scale, the Company's policies unreasonably allow Facebook to favor its own interests at users' expense.

2. Facebook's Users Did Not Give Knowing Consent to (I) Provide Their Personal Information to Third Parties or (II) Any Alteration or Aggregation of the Data for Commercial Use

208. According to PricewaterhouseCoopers LLP's ("PwC") Initial Assessment Report, Facebook's Privacy Program encompasses the Facebook Platform, and:

> [t]he platform terms and policies outline a variety of privacy obligations and restrictions, such as limits on an application's use of data received through Facebook, requirements that an application obtain consent for certain data uses, and restriction on sharing user data.

209. The consent "requirements" of Facebook's Privacy Program are illusory, as the platform terms and policies were not enforced. Moreover, Facebook users did not consent to the practices. In a 2014 news release announcing changes to its developer policies, a Facebook executive wrote, "We've heard from people that they are often surprised when a friend shares their information with an app." That admission indicates that people were not given adequate understanding of how their data and their friends' data were used by third parties. Facebook "goes into this endless hairsplitting that people should have known," said Marc Rotenberg, president and executive director of EPIC. "No one could have known that their friends were disclosing their personal data on their behalf. It's entirely illogical, and it breaks the consent law."

210. Former Facebook employee Parakilas explained, "Facebook had very few ways of either discovering abuse once data had been passed or enforcing on abuse once it was discovered." Parakilas stated in his testimony before the British Parliament's House of Commons on March 21, 2018:

> …I can start by giving a brief description of how Facebook Platform, which is what apps use, works, because it would be helpful in understanding this. When you connect to an app, you being a user of Facebook, and that app is connected to Facebook there are a number of

> categories of these apps, including games, surveys and various other types. Facebook asks you, the user, for permission to give the developer, the person who made the app, certain kinds of information from your Facebook account, and once you agree Facebook passes that data from Facebook servers to the developer. You then give the developer access to your name, a list of the pages that you have liked and access to your photos, for example.
>
> The important thing to note here is that once the data passed from Facebook servers to the developer, Facebook lost insight into what was being done with the data and lost control over the data. To prevent abuse of the data once developers had it, Facebook created a set of platform policies—rules, essentially—that forbade certain kinds of activity, for example selling data or passing data to an ad network or a data broker.
>
> However, Facebook had very few ways of either discovering abuse once data had been passed or enforcing on abuse once it was discovered. In the event that Facebook received a report of a data violation, it could do one of four things: it could call up the developer and demand to know what they were doing with the data; it could demand an audit of the developer's application, their data storage, and that was a right that was granted to Facebook in these policies, the platform policies; it could delete the app and potentially ban the developer from using Facebook Platform or even using other Facebook products such as advertising; or it could sue the developer and pursue that app. Those are the only four things that Facebook could do once it had determined that the developer had been in breach of those policies….
>
> I think one of the key things to understand is that if you do not have access to the developer's data storage, which you would not have unless you sued them or they granted it to you willingly, then you cannot really see what data they have, because what is exposed to the public view is not indicative.

211. The Individual Defendants claimed that Facebook had implemented a new application review process in 2014, where the Company would purportedly

ensure that any new third-party applications were only using a limited amount of Facebook's data for legitimate purposes that were permitted under the Company's updated policy, which Facebook's users were informed of and had consented to by virtue of their acceptance of Facebook's Terms of Use. "People want more control," Facebook said at that time. "It's going to make a huge difference with building trust with your app's audience."

212. Facebook's response to an inquiry from *WIRED* regarding the Cambridge Analytica incident confirms that Facebook personnel were aware of similar user privacy issues by at least 2014. Further, Facebook personnel knew that updates to Facebook's policies and data security practices were necessary to alleviate concerns that had already expressed by Facebook users. Facebook stated:

> "In 2014, after hearing feedback from the Facebook community, we made an update to ensure that each person decides what information they want to share about themselves, including their friend list."
>
> "Before you decide to use an app, you can review the permissions the developer is requesting and choose which information to share. You can manage or revoke those permissions at any time."

213. In April 2014, Facebook announced it was changing what data was accessed on the site. In a buried footnote suggesting that Facebook was eliminating several "rarely used endpoints," developers were able to discover that Facebook was in fact removing their access to a user's newsfeed, their friendships,

and data about friends (*e.g.*, education, photos, and location). These end points were not rarely used, and given the millions of users of apps that leveraged Facebook's photo-sharing APIs, it is clear that something else was afoot. This data was being used at that time in many highly popular applications; technology journalism site Mashable Infographic suggested that Facebook platform data were used in seven of the top 10 applications on the Apple iOS app store as of 2012.

214. Even after Facebook changed its policy in 2014 -- supposedly to protect user information from being exploited by "bad actors" -- the Individual Defendants failed to disclose that this "change" only applied to new apps and did not change anything with respect to the apps that already existed on Facebook's platform. Given that existing apps were, according to the Individual Defendants, given another year before Facebook ended their access to friends' data, it appears that the policy did not actually change until 2015. At the very least, the policy "change" did not change the number of apps that could access, retain, and use for commercial purposes the personal information of Facebook users.

215. Around the same time that the Individual Defendants claim to have changed Facebook's policy in 2014, multiple sources reported to *TechCrunch* that old Facebook messages they received from Zuckerberg had disappeared from their Facebook inboxes, while their own replies to him conspicuously remained. *TechCrunch* reported on April 5, 2018:

> An email receipt of a Facebook message from 2010 reviewed by *TechCrunch* proves Zuckerberg sent people messages that no longer appear in their Facebook chat logs or in the files available from Facebook's Download Your Information tool.
>
> When asked by *TechCrunch* about the situation, Facebook claimed in this statement it was done for corporate security: "After Sony Pictures' emails were hacked in 2014 we made a number of changes to protect our executives' communications. These included limiting the retention period for Mark's messages in Messenger. We did so in full compliance with our legal obligations to preserve messages." However, Facebook never publicly disclosed the removal of messages from users' inboxes, nor privately informed the recipients.
>
> * * *
>
> Facebook's power to tamper with users' private message threads could alarm some. The issue is amplified by the fact that Facebook Messenger now has 1.3 billion users, making it one of the most popular communication utilities in the world. Zuckerberg is known to have a team that helps him run his Facebook profile, with some special abilities for managing his 105 million followers and constant requests for his attention. For example, defendant Zuckerberg's profile doesn't show a button to add him as a friend on desktop, and the button is grayed out and disabled on mobile.

216. *TechCrunch* commented that while it could be true that "Facebook may have sought to prevent leaks of sensitive corporate communications[,]" Facebook also "may have looked to thwart the publication of potentially embarrassing personal messages sent by Zuckerberg or other executives." *TechCrunch* pointed to the "now-infamous instant messages from a 19-year-old Zuckerberg to a friend shortly after starting "The Facebook" in 2004: "yea so if you ever need info about anyone at harvard . . . just ask . . . i have over 4000

emails, pictures, addresses…" Zuckerberg wrote to a friend. "what!? how'd you manage that one?" they asked. "people just submitted it . . i don't know why . . . they 'trust me' . . . ." Zuckerberg explained.

217. Although Facebook's practice of tracking users through their use of mobile devices was not well-known at the time, Zuckerberg likely did not want to be personally subjected to the same tracking methods and sharing of his personal information obtained by third parties as easily as Facebook allowed them to access information about all of its other users.

218. The Individual Defendants represented to Facebook's auditors and regulators that the Company "discussed" and "evaluated" whether it was necessary to obtain additional notice or consent from users, but nothing about the disclosures in Facebook's reports to the FTC suggests there was any mandatory procedure for determining whether to make such changes. All decision-making in this regard was left to the members of Facebook's XFN team, which was also responsible for enforcing any violations that Facebook subsequently learned about.

219. The unredacted portion of the Initial Assessment Report states with regard to Facebook's "Ongoing Monitoring of the Privacy Program:" "The XFN process ensures that new products and changes to existing products that result in material and/or retroactive changes to the use of information are evaluated to determine whether additional notice or consent from Facebook users is required.

Where required, key decisions around the need for additional consent from users are discussed and recommendations are made and implemented by the XFN team.

220. The fact that Facebook refers to the possibility of learning about "retroactive changes to the use of information" that may require consent is further confirmation that the Company's policies and views on consent are completely unreasonable; Facebook's policies and views on consent are based on a presumption that it is possible to obtain "retroactive" consent. It is not.

3. A German Court Found Facebook's Privacy Settings and Terms are Invalid to Obtain Consent in 2018

221. On January 16, 2018, the Regional Court of Berlin held that Facebook's default privacy settings and parts of their terms and conditions were invalid and violate data protection law. Facebook was sued by the Federation of German Consumer Organizations (the "Federation"), which argued that Facebook's default settings violated the requirement of explicit consent. For example, the default settings included a location service in Facebook's mobile application revealing the location of the person that the user is chatting to. In addition, boxes were pre-activated allowing search engines to link to the user's timeline.

222. The Federation also argued that various clauses in the terms and conditions of Facebook were invalid, including clauses that provide consent of the

user to (i) transferring personal data to, and processing personal data in, the U.S. and (ii) using the name and profile picture of the user for commercial, sponsored or related content.

223. The Court held that Facebook's default privacy settings and parts of their terms and conditions were invalid. The Court found, among other things, that the default privacy settings include a location service in the application that reveals the location of the person that the user is chatting to. In addition, boxes were pre-ticked, allowing search engines to link the user's timeline. The Court noted that there was no valid consent by users, as there was no guarantee that users knew that these boxes were ticked by default.

G. EARLY LITIGATION AND COMPLAINTS ABOUT FACEBOOK'S PRIVACY VIOLATIONS SHOULD HAVE PROMPTED THE BOARD TO IMPLEMENT REASONABLE CONTROLS

224. Facebook has weathered complaints about violating user privacy since its earliest days without radically altering its practices. In 2006, users protested that Facebook's News Feed was making public information that the users had intended to keep private. The News Feed went on to become a core service of the Company and the primary means by which Facebook users receive information including advertisements targeted to specific Facebook users.

225. In 2009, Facebook began making users' posts, which had previously been private, public by default. That incident triggered anger, confusion, an

investigation by the FTC, and ultimately, the Consent Decree.

226. The Individual Defendants responded by proposing a "site governance" system under which its users would supposedly be given some collective control over their data through "referendums" that Facebook planned to hold. At the time, Zuckerberg explained, "[r]ather than simply reissue a new Terms of Use, the changes we're announcing today are designed to open up Facebook so that users can participate meaningfully in our policies and our future."

227. Just three years later, in 2012, the final referendum was held, which involved setting the terms under which Facebook could share user data with other organizations. Because a relatively small percentage of users had voted in the prior referendums, the Individual Defendants decided that the referendum would only be considered binding in the (extremely unlikely) case that 30 percent of its global users voted. Ultimately, only 668,000 users voted, and the Individual Defendants ignored the result, and never held another user referendum again.

228. 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. Users were unaware that such features were being tracked, and the privacy settings originally did not allow users to opt out. As a result of widespread criticism, Beacon was eventually shut down. 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 "optout system instead of opt-in … if someone forgot to decline to share something, Beacon went ahead and still shared it with their friends."

229. In September 2011, the Office of the Data Protection Commissioner of Ireland initiated an audit of Facebook's activities outside the U.S. and Canada, after receiving complaints about how the social networking giant handled users' information. In its December 2011 audit report, the regulator suggested that the company implement several changes to improve compliance with EU data protection laws, including better educating users about its tag suggest tool. On September 21, 2012, a follow-up audit revealed that Facebook has failed to minimize the potential for ad targeting based on words and terms that could be considered "sensitive personal data," and that Facebook improve its new user education, deletion of social plug-in impression data for EU users and account deletion practices within the next month in order to bring it into compliance with Irish and EU data protection requirements.

230. On December 9, 2011, a bipartisan group sought answers from Zuckerberg regarding the Company's privacy practices, questioning why the site's privacy policy was longer than the United States Constitution. In a letter to Facebook, the group pointed out that Facebook's current privacy policy was almost

six (6) times as long as it was in 2005, longer than other social networks' policies and the Constitution, not including the amendments. The representatives asked Zuckerberg to give them data regarding the percentage of Facebook users who read the full policy. "We are concerned ... that long, complex privacy policy statements make it difficult for consumers to understand how their information is being used," the letter said.

231. Rather than be forthright about these issues, in 2013, Facebook represented that it had experienced at least one major "attack" to its security systems and that the Company was "working continuously" to prevent similar security threats in the future. A February 15, 2013 post entitled "Protecting People On Facebook" states:

> Facebook, like every significant internet service, is frequently targeted by those who want to disrupt or access our data and infrastructure. As such, we invest heavily in preventing, detecting, and responding to threats that target our infrastructure, and we never stop working to protect the people who use our service. The vast majority of the time, we are successful in preventing harm before it happens, and our security team works to quickly and effectively investigate and stop abuse.
>
> Last month, Facebook Security discovered that our systems had been targeted in a sophisticated attack. As soon as we discovered the presence of the malware, we remediated all infected machines, informed law enforcement, and began a significant investigation that continues to this day. We have found no evidence that Facebook user data was compromised.
>
> As part of our ongoing investigation, we are working continuously and closely with our own internal engineering teams, with security teams at other companies, and with law enforcement authorities to learn

> everything we can about the attack, and how to prevent similar incidents in the future.
>
> * * *
>
> We will continue to work with law enforcement and the other organizations and entities affected by this attack. It is in everyone's interests for our industry to work together to prevent attacks such as these in the future.

1. The FTC Complaint Alleged that Facebook's Statements About its Privacy Practices Were Unfair, Deceptive, and Violated Law

232. In 2011, following an investigation by the FTC, Facebook entered into the Consent Decree to resolve the FTC's complaint alleging that the claims the Company made about its privacy practices were unfair and deceptive, and violated federal law.

233. The FTC complaint listed a number of instances in which Facebook allegedly made promises that it did not keep:

a. 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 Individual Defendants did not warn users that this change was coming, or get their approval in advance.

b. Facebook represented that third-party apps installed by users would have access only to user information that they needed to operate. In fact, the apps could access nearly all of users' personal data – data the apps did not

need.

c. Facebook told users they could restrict sharing of data to limited audiences – for example with "Friends Only." In fact, selecting "Friends Only" did not prevent their information from being shared with third-party applications their friends used.

d. Facebook had a "Verified Apps" program & claimed it certified the security of participating apps. It did not.

e. Facebook promised users that it would not share their personal information with advertisers. It did.

f. Facebook claimed that when users deactivated or deleted their accounts, their photos and videos would be inaccessible. But Facebook allowed access to the content, even after users had deactivated or deleted their accounts.

g. Facebook claimed that it complied with the U.S.- EU Safe Harbor Framework that governs data transfer between the U.S. and the European Union. It did not.

234. On November 29, 2011, the FTC announced that Facebook and the agency had reached an agreement on a Consent Decree relating to the FTC's charges that the company had "deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be

shared and made public."

235. According to the FTC's Complaint, the Company had allegedly failed to disclose to Facebook users that: (i) "a user's choice to restrict profile information to 'Only Friends' or 'Friends of Friends' would be ineffective as to certain third parties;" (ii) the company's "Privacy Wizard" tool for controlling access to user information "did not disclose adequately that users no longer could restrict access to their newly-designated (publicly available information) via their Profile Privacy Settings, Friends' App Settings, or Search Privacy Settings, or that their existing choices to restrict access to such information via these settings would be overridden;" and (iii) after making changes to its privacy policy, Facebook "failed to disclose, or failed to disclose adequately, that the December Privacy Changes overrode existing user privacy settings that restricted access to a user's Name, Profile Picture, Gender, Friend List, Pages, or Networks."

236. In the Consent Decree, the Individual Defendants agreed that: (i) Facebook will not "misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information," including "the extent to which [Facebook] makes or has made covered information accessible to third parties;" (ii) prior to sharing of a user's nonpublic information, Facebook will "obtain the user's affirmative express consent;" and (iii) Facebook would, among other stipulations:

> establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to (a) address privacy risks related to the development and management of new and existing products and services for consumers, and (b) protect the privacy and confidentiality of covered information.

237. The Consent Decree (i) barred Facebook from making any further deceptive privacy claims, (ii) required Facebook to obtain consumers' approval before it changed the way it shared their data, and (iii) required Facebook to obtain periodic assessments of its privacy practices by independent, third-party auditors for twenty (20) years following its entry.

238. The Board was well aware of the Consent Decree and the obligations placed on Facebook, as each director personally received a copy of the Consent Decree on September 12, 2012, according to the Facebook Compliance Report that was submitted to the FTC by Facebook's in-house attorneys on November 13, 2012, and those who joined the Board after that date also received a copy within thirty (30) days after their appointment as directors. Moreover, each of the directors (i.e. the Individual Defendants) is specifically obligated to oversee the Company's compliance with its terms.

239. The Individual Defendants' failure to cause the Company to comply with the Consent Decree has exposed Facebook to substantial liability for violating the Consent Decree. The FTC confirmed on March 23, 2018 that it is investigating Facebook for potential violations of the Consent Decree and, as set forth above,

Facebook estimates that its likely fine by the FTC will be in the range of $3-5 billion.

240. Rather than complying with the Consent Decree and adopting a reasonable Privacy Program and internal controls and procedures designed to detect and prevent violations of law, the Individual Defendants deliberately concealed from Facebook's users, shareholders, regulators, and government officials the true nature of Facebook's business and the continuing violations of the Company's obligations pursuant to the Consent Decree.

241. The Individual Defendants issued misleading statements in attempt to conceal that Facebook's advertising services were (and are) critically dependent upon obtaining large amounts of user data and aggregating this data in ways that most people did not know was possible.

242. The Individual Defendants' actions (and inactions) have exposed Facebook to liability for violating the Consent Decree. Defendants failed to comply with the Consent Decree in at least the following ways.

243. First, the public statements of the Individual Defendants and others do not comply with Section I of the Consent Decree, which prohibits Facebook from misrepresenting any of its privacy settings. The FTC evaluates misrepresentations based on what consumers reasonably understand. In its Complaint, the FTC found that Facebook had misrepresented the extent of access that third-party applications

had to user data. After the Consent Decree went into effect, Facebook continued to grant third-party applications the same level of access to user data as it had before, without ever correcting its misrepresentation. GSR, the company that transferred data to Cambridge Analytica, acquired its data from Facebook in June 2014, two years after the Consent Decree went into effect.

244. Second, the Board failed to implement and revise Facebook's policies and Terms of Use to ensure they complied with Section II of the Consent Decree, which required Facebook to obtain affirmative express consent and give its users clear and prominent notice before disclosing their previously collected information with third parties in a way that exceeds the restrictions imposed by their privacy settings. As the FTC found, Facebook granted third-party applications access to user data by overriding users' privacy settings. After the Order went into effect, Facebook never clearly and prominently disclosed this practice to users and did not retroactively seek users' express affirmative consent to continue disclosing their previously-collected data to third-party applications.

245. On April 19, 2018, Senator Blumenthal sent a letter to the FTC, noting that Facebook by default continued to provide access to personal and non-public data to third-party applications even after the Consent Decree. As he did at the April 10 Senate hearing, Senator Blumenthal specifically called out Facebook for failing to notice that Kogan submitted terms of service for his application that

explicitly stated that he reserved the right to sell user data and would collect profile information from the friends of those who downloaded the application. "Even the most rudimentary oversight would have uncovered these problematic terms of service," Sen. Blumenthal wrote. "This willful blindness left users vulnerable to the actions of Cambridge Analytica."

246. According to PwC's Initial Assessment Report, which is based on "Management Assertions," Facebook's Privacy Program is routinely monitored, reviewed, and improved. The report states, in relevant part:

> Monitoring Activities: Members of Facebook's Legal team periodically review the Privacy Program to ensure it, including the controls and procedures contained therein, remains effective. These legal team members also will serve as point of contacts for control owners and will update the Privacy Program to reflect any changes or updates surfaced.
>
> Monitoring: Facebook's Privacy Program is designed with procedures for evaluating and adjusting the Privacy Program in light of the results of testing and monitoring of the program as well as other relevant circumstances. The Privacy XFN Team assesses risks and controls on an on-going basis through weekly meetings and review processes. Members of Facebook's legal team support the Privacy Program and serve as points of contact for all relevant control owners to communicate recommended adjustments to the Privacy Program based on regular monitoring of the controls for which they are responsible, as well as any internal or external changes that affect those controls.

247. The Management Assertions and other statements in PwC's reports about Facebook's Privacy Program are misleading and contradict Defendants' own representations. For example, Sandberg admitted in an interview with Recode Media on May 30, 2018 that Facebook had not audited Cambridge Analytica to

ensure they had actually deleted the data. Sandberg said:

> Looking back, we definitely wish we had put more controls in place. We got legal certification that Cambridge Analytica didn't have the data, we didn't audit them.

248. Third, Facebook was required under Section IV of the Consent Decree to establish a "comprehensive privacy program" that would: "(1) address privacy risks related to the development and management of new and existing products and services, and (2) protect the privacy and confidentiality of covered information." The privacy program required by the Consent Decree had to be designed to prevent "unauthorized collection, use, or disclosure of covered information." PwC's Initial Assessment Report, which is based on Management Assertions, states that:

> Facebook has implemented technical, physical, and administrative security controls designed to protect user data from unauthorized access, as well as to prevent, detect, and respond to security threats and vulnerabilities.

However, Zuckerberg admitted in testimony before Congress and the British Parliament that Facebook failed to read the terms and conditions of the GSR application which procured the data that was sold to Cambridge Analytica.

249. Senator Blumenthal, in his letter to the FTC sent on April 19, 2018, noted that although the FTC explicitly put Facebook on notice about the privacy risks of third-party apps with the 2011 consent decree, the Company has "continued to turn a blind eye" to other outside parties that collect data from its users, and its procedures for verifying that new apps comply with its remain

"murky," Senator Blumenthal said in his letter. Indeed, as the *New York Times* reported on June 3, 2018, Facebook still allows entities other than third-party application operators to access the same user data that the Company purportedly banned when it revised its policy in 2015, including Chinese mobile device manufacturers, such as Huawei, which poses a national security risk.

250. Fourth, the Consent Decree prohibits Facebook from misrepresenting the privacy or security of "covered information" -- broadly defined to include "photos and videos." The Order also requires Facebook to "give its users a clear and prominent notice and obtain their affirmative express consent" before disclosing previously-collected information. EPIC and other consumer privacy groups have alleged that since early 2018, Facebook has been routinely scanning photos, posted by users, for biometric facial matches without the consent of either the image subject or the person who uploaded the photo, in violation of these provisions (among other laws).

251. The Individual Defendants not only had the ability (and responsibility) to change Facebook's policies and practices with respect to third-party developer access to user information, they were also aware of, and facilitated, this activity through Facebook's unlawful business practices and inadequate privacy policies; the Individual Defendants knew such practices and policies could cause substantial damage to Facebook and potential violations of the Consent

Decree.

252. FTC Commissioner Chopra noted in a recent memorandum to FTC staff that going forward, "[w]hen orders are violated, a key question [the FTC] will evaluate … is whether the proposed remedies address the underlying causes of the noncompliance." Chopra said the FTC will "hold individual executives accountable for order violations in which they participated, even if these individuals were not named in the original orders[,]" noting that "[t]his relief is expressly contemplated by Fed. R. Civ. P. 65(d), which provides that an injunction against a corporation binds its officers." Moreover, Chopra explained, "this relief is important, because it ensures that individual executives who control the operation of the firm – and not just shareholders – bear the costs of noncompliance."

2.

The Individual Defendants Ignored Concerns Raised By Facebook's Chief Information Security Officer About the Security of Facebook's Platform

253. Stamos, Facebook's Chief Information Security Officer, wrote a memo in 2016 that was subsequently turned into a "white paper" titled "Information Operations and Facebook" (the "White Paper") which unquestionably alerted the Individual Defendants that those activities were pervasive and supported by management. The White Paper also confirmed that the Individual Defendants' public statements were false and misleading. Among other things, the White Paper

affirmatively misrepresented that Facebook had "no evidence of any Facebook accounts being compromised" in connection with the 2016 election as of the date it was published on April 27, 2017.

254. Stamos later said that he had initially provided a written report to Facebook executives concerning the circumstances which led to the Cambridge Analytica leak. Instead of taking appropriate action and disclosing the leak, Facebook rewrote the report and presented it as a hypothetical scenario in a "whitewashed" version of the White Paper, published by Facebook, which further suppressed and concealed the wrongdoing at the Company.

255. On September 6, 2017, Stamos published "An Update on Information Operations on Facebook" in the Facebook newsroom, through which Stamos addressed some of the concerns that had been raised in the media about possible Russian interference with the U.S. presidential election.

256. Despite warnings from Stamos and others of similar concerns that Russian interference could have occurred via Facebook's Platform, the Individual Defendants brushed them aside as frivolous and initially acted as though it was impossible.

257. But on October 22, 2017, *The Guardian* reported that Facebook had handed the content of 3,000 political ads to the special counsel and congressional investigators looking into potential Kremlin interference with the U.S. presidential

election. The ads were paid for by a shadowy Russian entity called the Internet Research Agency.

258. Sandberg responded, saying that Facebook owed the nation "not just an apology but determination" to defeat attempts to subvert U.S. democracy. In an interview with the Axios media site, Sandberg did not address whether Russian trolls were targeting the same users as the campaign of President Trump, which would point towards collusion, but promised: "When the ads get released we will also be releasing the targeting for those ads. We're going to be fully transparent." However, Sandberg was purposely vague on the question of when Facebook's management became aware of large-scale Russian manipulation, saying only: *"*We started to hear the rumors around the election itself of a different kind of attack."

259. *The New York Times* reported that, by October 2017, the relationship between Stamos and Sandberg had deteriorated over how to handle Russian interference on Facebook and how best to reorganize Facebook's security team before the midterm elections, according to more than half a dozen people who work or formerly worked at the company. Stamos proposed that instead of reporting to Facebook's general counsel, he report directly to Facebook's higher-ups. Instead, executives reportedly reduced Stamos' day-to-day responsibilities.

Former Zuckerberg Mentor Warned of Data Security Issues in 2016

260. Roger McNamee ("McNamee"), a longtime Silicon Valley investor

and reported Facebook insider, also warned Facebook executives about data security issues by at least 2016. McNamee's warnings also went unheeded. McNamee was both Zuckerberg's mentor before Facebook went public and an early investor in the Company. McNamee and Zuckerberg first met in 2006 when Facebook's then Chief Privacy Officer, Chris Kelly, called McNamee to give some advice to defendant Zuckerberg on whether or not to sell the company to Yahoo!. As McNamee describes his first encounter with Zuckerberg: "I began by letting Mark know the perspective I was coming from. Soon I predicted, he would get a billion-dollar offer to buy Facebook from either Microsoft or Yahoo, and everyone, from the company's board to the executive staff to Mark's parents, would advise him to take it. I told Mark that he should turn down any acquisition offer. He had an opportunity to create a uniquely great company if he remained true to his vision… I told Mark the market was much bigger than just young people; the real value would come when busy adults, parents and grandparents, joined the network and used it to keep in touch with people they didn't get to see often." In short, McNamee advised Zuckerberg against selling the company prematurely. After this meeting, McNamee and Zuckerberg developed a close mentoring relationship, and McNamee reportedly acted as a father figure to Zuckerberg. McNamee suggested to Zuckerberg that he hire Sandberg as Facebook's COO. By the time Facebook went public, McNamee was no longer a mentor to Zuckerberg. That role was

taken over by Facebook directors Andreessen and Thiel.

261. In or about February 2016, McNamee began noticing "viciously misogynistic anti-Clinton memes originating from Facebook groups supporting Bernie Sanders." McNamee never suspected the Sanders campaign as pushing out the memes, which made McNamee worry that Facebook was being used in a way Zuckerberg had not intended. However, McNamee saw a similar thing happening before the Brexit vote when anti-European Union messages were all over Facebook.

262. Following the Brexit vote, McNamee wrote an op-ed piece for *Recode*, warning that Facebook was being manipulated by "bad actors." In the article, McNamee concluded that the problem seemed to be "systemic – the algorithms themselves made the site vulnerable because they were coded to prioritize attention, and attention is best gained by messages that elicit fear, outrage, and hate-sharing."

263. On October 30, 2016, McNamee sent a draft of the op-ed piece to Zuckerberg and Sandberg. According to McNamee,

> They each responded the next day. The gist of their messages was the same: We appreciate you reaching out; we think you're misinterpreting the news; we're doing great things that you can't see. Then they connected me to Dan Rose, a longtime Facebook executive with whom I had an excellent relationship. Dan is a great listener and a patient man, but he was unwilling to accept that there might be a systemic issue. Instead, he asserted that Facebook was not a media company,

> and therefore was not responsible for the actions of third parties.

264. McNamee ultimately decided to not publish the op-ed piece, explaining: "Mark and Sheryl were my friends, and my goal was to make them aware of the problems so they could fix them. I certainly wasn't trying to take down a company in which I still hold equity."

265. Zuckerberg and Sandberg ignored the warnings from McNamee. McNamee told *Quartz* that he didn't expect defendant Zuckerberg to "just accept" the warning message that he sent him,

> We hadn't spoken in a number of years at that point, but we had traded emails and it was always positive. But when I saw what was going on in 2016, I was genuinely concerned. I just assumed that he would have trouble accepting it, because they hadn't had anything negative in three or four years. It must have been really hard for him to appreciate that everything wasn't perfect. But I kind of hoped that if I talked to Dan Rose over a period of weeks or months, they would have eventually follow through. The shock would pass and they would think 'Roger is actually really serious about this, maybe we should just check it out.' But after three months, I realized they were never going to check it out.

266. The Individual Defendants also ignored numerous other "red flag" warnings regarding the Company's inadequate internal controls.

267. The periodic audits of Facebook's privacy program that were required by the consent decree have revealed serious procedural and substantive deficiencies in the Company's privacy program, internal audit practices, and platform policies.

268. On November 29, 2011, Facebook settled the FTC's claims that it deceived its users, which numbered approximately seven hundred fifty (750) million worldwide at the time, about the privacy of their personal data, including names, birthdays, location, friends and sexual orientation. The FTC took particular issue with privacy changes Facebook made in December 2009 that overrode users' privacy settings with no notice or consent.

V. THE INDIVIDUAL DEFENDANTS ALLOWED FACEBOOK TO ENGAGE IN ILLEGAL AND DECEPTIVE BUSINESS PRACTICES FOR MORE THAN A DECADE

269. Since at least 2008, the Board has pursued profits at the expense of compliance with the law.

270. Facebook's source code and associated documentation was used to (a) access other third-party websites to which Facebook's users did not consent and which was in violation of Facebook's Terms of Service; (b) allow other third-party websites to acquire Facebook user information and related data for commercial purposes; (c) download acquired user data to Facebook's own website, (d) display downloaded user data on other third-party websites and on Facebook's website without the users' permission; and (e) employ automated scripts to initiate unauthorized communications with non-Facebook users soliciting them to join Facebook. All of this source code was used by Facebook to improperly connect to other websites without users' permission to further the Individual Defendants' own

commercial purposes and gain.

271. The source code includes facebook.com website (i.e., html) source code, website sitemap, scripts, build files, readme files, tutorial examples, functional specifications and diagrams, architecture specifications and diagrams, system specifications and diagrams, website specifications and diagrams, server file system documentation, and database security documentation. The source code data is the best evidence of how Facebook (i) initiated unauthorized access to other websites, (ii) acquired, downloaded and displayed user information on Facebook's own website, and then (iii) "spammed" non-Facebook users with invitations to join Facebook. The source code includes: (i) any scripts, both server-side (runs on facebook.com servers) and client side (runs on the user's computer); (ii) all application source code written or used for gathering Facebook users' content or executing functions using Facebook's "Like" button; (iii) the database or databases used by the website and/or by Facebook; (iv) documentation on the email service or services used by Facebook; (v) files written or read by the programs; (vi) the source code used to compile, interpret, and execute scripts; and (vii) the source code for any spider(s) and any crawler(s) used by Facebook.

272. Facebook used various attributes and variables to: (i) associate downloaded information that Facebook obtained from third parties with the information Facebook stored about its own users, interact with other websites'

software, and initiate events (such as Group Events) to solicit Facebook users to join Power, (ii) identify the commands used by Power to obtain information from (and/or send communications to) Facebook users; and (iii) identify Facebook users in Power's own database, how Facebook user profile information was parsed and/or reformatted on the website www.power.com, or similar important critical technical details.

273. On April 18, 2018, researchers at Princeton University reported that third-party trackers employing code used across the internet to monitor user behaviors on websites, to optimize ads, and for other purposes, obtained Facebook user information on websites that support logging in through the social media platform. When users log in to websites using Facebook's Login feature, trackers reportedly grabbed Facebook user identifications and, in some cases, other information such as email address or gender, potentially without the knowledge of the operators of the websites where the trackers are installed, according to the researchers. "[W]hen a user grants a website access to their social media profile, they are not only trusting that website, but also third parties embedded on that site," wrote Gunes Acar, Arvind Narayanan, and Steven Englehardt, a Mozilla privacy engineer who also researches privacy at Princeton. The researchers posted their findings on "Freedom to Tinker," a website hosted by Princeton's Center for Information Technology Policy ("CITP"). CITP is a research center that studies

digital technologies in public life.[12]

274. The Princeton University researchers reporting on the acquisition of Facebook user information by third-party trackers said that they had found "another type of surreptitious data collection by third-party scripts" – "the exfiltration of personal identifiers from websites through 'login with Facebook' and other such social login APIs." Specifically, they found that "seven third parties abuse websites' access to Facebook user data" and "one third party uses its own Facebook 'application' to track users around the web." With regard to the seven third parties, researchers said that while "these scripts query the Facebook API and save the user's Facebook ID, we could not verify that it is sent to their server due to obfuscation of their code[.]" The researchers concluded,

> This unintended exposure of Facebook data to third parties is not due to a bug in Facebook's Login feature. Rather, it is due to the lack of security boundaries between the first-party and third-party scripts in today's web.

A.

FACEBOOK'S AGREEMENTS WITH THIRD-PARTY "SERVICE PROVIDERS" VIOLATED THE CONSENT DECREE

275. On June 3, 2018, an article published by *The New York Times* reported that Facebook had entered into agreements over the decade prior to publication

[12] Englehardt, Steven, "No boundaries for Facebook data: third party trackers abuse Facebook Login*"* (2018), https://freedom-to-tinker.com/2018/04/18/no-boundaries-for-facebook-data-third-party-trackers-abuse-facebook-login/ (last visited Apr. 30, 2019).

with at least sixty (60) device makers, including Apple, Amazon, BlackBerry, Microsoft and Samsung, that allowed them to access vast amounts of Facebook information, including data about users' friends who had blocked such third-party access. These data-sharing partnerships, which Facebook entered into as early as 2007, gave these companies the ability to offer "features" of the social network, such as messaging, "like" buttons and friends (contacts) lists, on their own websites and mobile devices. *The Times* reported that Facebook provided mechanisms for certain phone and device manufacturers to build software-accessing user data, supposedly to integrate Facebook features before application markets came into widespread use.

276. The following day, the *Times* reported that Facebook has similar data-sharing agreements with Chinese telecommunications companies, including Huawei, Lenovo, OPPO, and TCL. Notably, Facebook and its subsidiaries Instagram and WhatsApp have been blocked by the Chinese government since 2009, and the Pentagon recently banned the use of devices made by Huawei on U.S. military bases, citing national security concerns.

277. According to a 2012 report by the CIA and the FBI, a data-sharing agreement like the one between Facebook and Huawei could present a substantial threat of "economic espionage." Although Huawei has been flagged by American intelligence officials as a national security threat, Facebook's agreement with

Huawei was still in effect as of June 5, 2018, when Facebook representatives acknowledged these arrangements publicly for the first time.

278. Francisco Varela, Facebook's Vice President in charge of mobile partnerships, said in a statement that "many other U.S. tech companies have worked with [Huawei] and other Chinese manufacturers" and that "Facebook's integrations were controlled from the get go – and [Facebook] approved" everything they built using Facebook information. Varela said that these agreements with manufacturers were common at the time they were developed, and the deals were supposedly struck to help users access Facebook features such as the "like" button on their devices. Varela told the *Times* that Huawei used its Facebook access to feed a social phone app that lets users see messages and social media accounts in one place, and emphasized that the data Huawei had access to stayed on phones and was not transferred to or stored on its servers. Varela said:

> Given the interest from Congress, we wanted to make clear that all the information from these integrations with Huawei was stored on the device, not on Huawei's servers.

279. Another Facebook Vice President in charge of Product Partnerships, Ime Archibong ("Archibong"), also addressed the agreements in a Facebook Newsroom post titled "Why We Disagree With The New York Times." According to Archibong, "in the early days of mobile," Facebook had built a set of private APIs that allowed companies like Apple, Amazon and HTC to "recreate Facebook-

like experiences for their individual devices or operating systems" for users who weren't able to put a Facebook app on their device.

280. The Company's representatives claimed that Facebook had already decided to start winding down these data-sharing arrangements in April 2018, but did not explain why they had never previously been disclosed, particularly during Zuckerberg's testimony before Congress. He also disputed the assertion that the access afforded by the data-sharing arrangements went beyond what users had agreed to or were expecting.

281. Indeed, Zuckerberg did not even mention the contracts with other third-party companies in his testimony. There are two kinds of arrangements that Facebook has that are supposedly "winding down" because both appear, unsurprisingly, to violate Defendants' promises to protect user privacy (and perhaps, the Consent Decree).

B.

PWC IMPROPERLY CERTIFIED THAT FACEBOOK'S PRIVACY PROGRAM SATISFIED THE FTC CONSENT DECREE IN AUDIT REPORTS FROM 2013 AND THEREAFTER

282. PwC is the supposedly "independent" auditor that Facebook retained to conduct the audits that are required under Section VI of the Consent Decree. Thus far, PwC has prepared three assessments that Facebook has submitted to the FTC certifying that Facebook's privacy program meets or exceeds the requirements of the Consent Decree.

283. In the audit reports that Facebook has submitted to the FTC, PwC certified that Facebook's privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the reporting periods.

284. PwC's certifications are based on purported facts, called "assertions" in the audit reports, which are actually management's own assertions that were admittedly provided to PwC by Facebook for the purpose of the supposedly "independent" audits. These "assertions" were assumed true for purposes of the audit and were not (i) determined to be true in the course of an independent audit conducted by PwC or (ii) confirmed by PwC based upon reasonable auditing procedures independent from Facebook's management. PwC acted unreasonably in relying on management's assertions, and taking them as "fact," without conducting an appropriate investigation and review of the information that was provided to determine whether it was sufficiently reliable and supported by Facebook's records, documentation, or other evidence.

285. According to the audit report for the period February 12, 2015 to February 11, 2017, Facebook constantly enhances or updates its program to protect individuals'/users' information. Per the audit report, Facebook's Privacy XFN Team assists the chief officer and his team in reviewing and providing feedback on

new product proposals and any material changes to existing products from a privacy perspective.

286. The audit report for the period August 15, 2012 to February 11, 2013 indicates that Facebook's Privacy Program was defined by the following assertions: responsibility for the Facebook Privacy Program; privacy Risk Assessment; Privacy and Security awareness; notice; choice; consent; collection and assessment; security for privacy; third-party developers; service provider; and on-going monitoring of the privacy program. These assertions are based on the following "facts" that were not independently verified by PwC:

a. Facebook provides notices to users regarding its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained and disclosed.

b. Without users/individuals' explicit or implicit authorization, Facebook would not disclose users' information to any-third parties/developers;

c. Facebook collects personal information only for the purposes identified in the notice, and Facebook provides tools for users/individuals to manage their personal information.

287. Although Zuckerberg admitted that he learned of the data exfiltration to Cambridge Analytica in 2015, he claimed Facebook had no knowledge or reason

to believe that it was not deleted until more than two years later — during the same period that PwC assessed Facebook's privacy program and found the company's internal controls were effective to detect and prevent similar wrongdoing.

288. In its Biennial Report for the period from February 12, 2015 to February 11, 2017, PwC stated that there were no material weaknesses in Facebook's internal controls and determined that Facebook's privacy program was sufficient to comply with the Consent Decree.

289. At the same time, however, the Individual Defendants continued to operate Facebook's business in essentially the same manner that led to the Consent Decree being entered in the first place and were known to have previously made – and broken – their promises with regard to Facebook's user privacy practices. PwC simply relied on "Management Assertions" about Facebook's privacy program and certified, based on these representations, that Facebook's monitoring procedures, policies and internal controls were effective. If true, however, there is no doubt that Facebook's Board, if not PwC, would have learned that third-party application developers had access to Facebook's user data until at least 2015, a year after Defendants said Facebook's policy had been changed to prevent any similar future recurrence.

290. The Individual Defendants knew (or should have known) that once the data was exfiltrated by a third party, there was no way for Facebook to recover the

data or to ensure it would not be further exposed or compromised in the future. Even if there was, Defendants did not even attempt to secure Facebook's user data and failed to implement any auditing or enforcement procedures. Instead, the Individual Defendants (i) turned a blind eye to obvious violations of Facebook's policies, (ii) failed to ensure that Facebook's privacy program was effective, and (ii) failed to ensure that their statements about Facebook's data security and user privacy practices were not misleading.

291. The FTC announced on March 17, 2016 that it had issued warning letters to twelve (12) application developers who installed SilverPush software in their applications, which allowed them to monitor the television viewing habits of consumers who used the applications across various devices. The FTC warned that embedding this software in their applications without notifying users could violate Section 5 of the Federal Trade Commission Act.

292. As demonstrated by its March 17, 2016 announcement, the FTC had shown an interest in cross-device tracking because consumers were beginning to connect to the internet in a variety of ways, including smartphones, tablets and wearable devices, which raised (and continues to raise) privacy and security concerns as businesses develop new methods to track their behavior across devices. The FTC warning letters sought to address the privacy implications of the SilverPush software even *before* the technology had been directed at the United

States, and they demonstrated the need for Facebook to make disclosures about cross-device tracking, among other things.

293. Facebook was specifically obligated by the Consent Decree to notify users whenever any change was made that allowed additional or different Facebook information to be shared with other third parties, such as device manufacturers that Facebook had agreements with or similar data-sharing capabilities that enabled cross-device tracking of users.

294. Facebook's statements on its website confirm the company's cross-device tracking capabilities, and its partnerships with third-party device manufacturers indicate that Facebook enabled cross-device tracking on a much larger – and potentially more dangerous – scale than the scope of the FTC's March 17, 2016 announcement.

295. The Individual Defendants knew, and PwC should have uncovered in its audit, that Facebook embedded software and certain Facebook "features" in mobile devices manufactured by Apple -- and even allowed Chinese companies to embed Facebook "features" in their mobile devices -- despite the serious threat such practices posed to national security.

296. In PwC's Initial Assessment Report, Facebook's Control Activity with regard to Service Providers states,

> The privacy policies of Facebook and Instagram contain a section that 'informs users that the information Facebook and Instagram receive

> may be shared with service organizations when a user signs up for Facebook and Instagram accounts.'

The unredacted portions of the report do not disclose that certain multinational corporations were the "service organizations" with which Facebook maintained data-sharing agreements.

297. Although other companies are also referred to in the report, they are "Facebook Experience application developers" that

> must read and sign-off on the Extended API Addendum (the 'Addendum'), or … the terms and conditions for a developer's adherence to Facebook's Platform Policies, Statement of Rights and Responsibilities and data policies and procedures

that apply to third-party application developers like Kogan, who were supposedly required to follow the same policies that Defendants did not enforce.

298. Mobile device manufacturers like Apple and Huawei, however, are subject to different "Service Provider Contracts" that, according to the Initial Assessment Report, "*may* be terminated if Facebook identifies misuse of user information (based on violations of the Statement of Rights and Responsibilities and/or the vendor security policy)."

299. The FTC warning letters also demonstrate the need for disclosures concerning cross-device tracking, because consumers are now connecting to the internet in a variety of ways, including through smartphones, tablets and wearable devices, and the FTC noted concerns about privacy violations arising as businesses

developed new methods to track consumer behavior across devices as early as 2015, and again in 2016.[13]

300. The FTC further made clear as early as 2013 that these cross-device tracking activities implicate privacy issues and must be disclosed, and PwC's failure to detect or determine that Facebook's privacy program may be insufficient to prevent these type of disclosure violations is particularly egregious given the circumstances. Facebook acquired the Atlas technology from Microsoft in 2012 and also partnered with Apple; thus, it essentially pioneered this very activity.[14]

301. The fact that PwC found no deficiencies in Facebook's internal controls following the WhatsApp acquisition in 2014 is similarly egregious, given that the FTC specifically warned Defendants in 2014 about their obligations to protect the privacy of their users in light of the proposed acquisition.[15]

---

[13] *See*, *e.g.*, Fed. Trade Comm'n Press Release, *FTC To Host Workshop on Cross-Device Tracking Nov. 16*, (2015), https://www.ftc.gov/news-events/press-releases/2015/03/ftc-host-workshop-cross-device-tracking-nov-16 (last visited Apr. 30, 2019); Center for Democracy & Technology, *Comments for November 2015 Workshop on Cross-Device Tracking* (2015), https://www.ftc.gov/system/files/documents/public_comments/2015/10/00056-99849.pdf (last visited Apr. 30, 2019).

[14] *See* Fed. Trade Comm'n Staff Report, *Mobile Privacy Disclosures: Building Trust Through Transparency* (2013), *available at* https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf (last visited Apr. 30, 2019).

[15] *See* Fed. Trade Comm'n Press Release, *FTC Notifies Facebook, WhatsApp of Privacy Obligations in Light of Proposed Acquisition* (2014), *available at* https://www.ftc.gov/news-events/press-releases/2014/04/ftc-notifies-facebook-whatsapp-privacy-obligations-light-proposed (last visited Apr. 30, 2019).

FACEBOOK'S ACQUISITION OF WHATSAPP VIOLATED THE EUROPEAN UNION'S MERGER REGULATION

302. In a letter to Facebook and WhatsApp's general counsel sent on April 10, 2014, Jessica Rich, Director of the FTC's Bureau of Consumer Protection, noted that (i) WhatsApp made clear privacy promises to consumers and (ii) both companies told consumers that after any acquisition, WhatsApp will continue its current privacy practices. The letter from the FTC stated:

> We want to make clear that, regardless of the acquisition, WhatsApp must continue to honor these promises to consumers. Further, if the acquisition is completed and WhatsApp fails to honor these promises, both companies could be in violation of Section 5 of the Federal Trade Commission (FTC) Act and, potentially, the FTC's order against Facebook.[16]

303. The FTC specifically noted that the Consent Decree applies equally to "Facebook and its subsidiaries" and instructed that:

> [b]efore changing WhatsApp's privacy practices in connection with, or following, any acquisition, you must take steps to ensure that you are not in violation of the law or the FTC's order. First, if you choose to use data collected by WhatsApp in a manner that is materially inconsistent with the promises WhatsApp made at the time of collection, you must obtain consumers' affirmative consent before doing so. Second, you must not misrepresent in any manner the extent to which you maintain, or plan to maintain, the privacy or security of WhatsApp user data…. Finally, if you choose to change how you collect, use, and share newly collected WhatsApp data, we recommend that you offer consumers an opportunity to opt out of

[16] *See* Fed. Trade Comm'n Press Release, *FTC Notifies Facebook, WhatsApp of Privacy Obligations in Light of Proposed Acquisition* (2014), https://www.ftc.gov/news-events/press-releases/2014/04/ftc-notifies-facebook-whatsapp-privacy-obligations-light-proposed (last visited Apr. 30, 2019).

such changes[.]

304. On April 10, 2014, the FTC noted in a letter to Facebook and WhatsApp's general counsel,

> Following the announcement of the proposed acquisition of WhatsApp, Facebook chief executive Mark Zuckerberg was quoted as saying 'We are absolutely not going to change plans around WhatsApp and the way it uses user data.' Similarly, a Facebook spokesperson stated that 'As we have said repeatedly, WhatsApp will operate as a separate company and will honor its commitments to privacy and security.'

The FTC concluded that Facebook had "promised consumers that it would not change the way WhatsApp uses customer information" and specifically advised that "any use of WhatsApp's subscriber information that violates these privacy promises, by either WhatsApp or Facebook, could constitute a deceptive or unfair practice under the FTC Act" and "could violate the FTC's order against Facebook."

305. On March 12, 2018, WhatsApp attorneys signed an "undertaking" with the Information Commissioner responsible for enforcement of the Irish Data Protection Act ("DPA") acknowledging that WhatsApp's "shar[ing] any personal data with the Facebook family of companies" would be a violation of the DPA because WhatsApp had:

> (i) "not identif[ied] a lawful basis of processing for any such sharing of personal data;" (ii) "fail[e]d to provide adequate fair processing information to users in relation to any such sharing of personal data;" and (iii) "[i]n relation to existing users, such sharing … involved the

> processing of personal data for a purpose that is incompatible with the purpose for which such data were obtained."

WhatsApp "commit[ed]" not to engage in these practices only with respect to users in the European Union, and WhatsApp and Facebook continue to share the personal data of U.S. users with each other and with other third-party companies.

306. The acquisition of WhatsApp was made on the foundation of "no ads, no games, and no gimmicks." However, Zuckerberg broke his promise and reportedly pressured WhatsApp's founders to change its business model in order to generate more advertising revenue. Reportedly, when Koum complained that he "didn't have enough people" to implement the project, Zuckerberg dismissed him with the statement, "I have all the people you need," according to one person familiar with the conversation.

307. WhatsApp co-founder Brian Acton ("Acton") left Facebook in November of 2017 according to *The New York Times*. Acton later became the executive chairman of the Signal Foundation, the nonprofit that has run the encrypted communication app Signal, and he personally invested $50 million into the project that focuses on the development of privacy-focused apps.

308. On April 30, 2018, Koum publicly announced his departure from WhatsApp and resignation from the Board. "Koum's exit is highly unusual at Facebook," *The Washington Post* reported.

The inner circle of management, as well as the board of directors, has

> been fiercely loyal during the scandals that have rocked media giant. In addition, Koum is the sole founder of a company acquired by Facebook to serve on its board. Only two other Facebook executives, Zuckerberg and Chief Operating Officer Sheryl Sandberg, are members of the board.

309. Koum did not give any reasons for his exit. Nevertheless, he explained that he deeply cared about the privacy of communication in 2014 when he sold WhatsApp to Facebook, stating in a blog post,

> respect for your privacy is coded into our DNA, and we built WhatsApp around the goal of knowing as little about you as possible… If partnering with Facebook meant that we had to change our values, we wouldn't have done it.

310. The split between Facebook and WhatsApp was viewed as messy and expensive, according to *The Wall Street Journal.*

> "Behind the dishiness, however, is a very important story that pretty much clears up any doubt as to whether Mark Zuckerberg is a trustworthy man who keeps his promises – or a profit-obsessed machine who's much stronger on greed than he is on morals."

While Zuckerberg told stock analysts that he and Koum agreed that advertising wasn't the right way to make money from messaging apps," it was Zuckerberg's decision alone to depart from that principle.

311. According to *The Washington Post*, which spoke to "people familiar with internal discussions" over Koum's departure, there were tensions with Facebook over WhatsApp's end-to-end encryption, which ensures that messages can't be intercepted and read by anyone outside of the conversation, including by

WhatsApp or Facebook. Koum and other WhatsApp executives believed that Facebook's desire to make it easier for businesses to use its tools would require weakening some of the encryption.

312. Acton, who co-founded WhatsApp with Koum in 2009, left Facebook in November 2017, according to *The New York Times*. On March 20, 2018, Acton wrote on twitter five days after the Cambridge Analytica scandal, "It is time. #deletefacebook" to support the chorus of the #deletefacebook movement, *TechCrunch* reported.

313. Both Acton and Koum are purportedly big believers in privacy, and is the reason why WhatsApp insisted on no ads for its platform and operated independently even though Facebook scrapped the 99-cent annual charge to prevent WhatsApp from generating revenue, according to *The Washington Post*.

314. Sandy Parakilas, a former Facebook manager, told *The New York Times*, "Jan and Brian's departures mean that Facebook, WhatsApp and Instagram are all controlled even more tightly by a single person – Mark Zuckerberg; this centralized control is bad for the users of all of these products."

315. On May 18, 2017, the European Commission announced in a press release that it had fined Facebook €110 million "for providing incorrect or misleading information during the Commission's 2014 investigation under the EU Merger Regulation of Facebook's acquisition of WhatsApp." The press release

explained:

> When Facebook notified the acquisition of WhatsApp in 2014, it informed the Commission that it would be unable to establish reliable automated matching between Facebook users' accounts and WhatsApp users' accounts. It stated this both in the notification form and in a reply to a request of information from the Commission. However, in August 2016, WhatsApp announced updates to its terms of service and privacy policy, including the possibility of linking WhatsApp users' phone numbers with Facebook users' identities.

316. The Commission found that, "contrary to Facebook's statements in the 2014 merger review process, the technical possibility of automatically matching Facebook and WhatsApp users' identities already existed in 2014, and that Facebook staff were aware of such a possibility." The Commission said the decision was "based on a number of elements going beyond automated user matching" and was "unrelated to either ongoing national antitrust procedures or privacy, data protection or consumer protection issues," but noted that those issues "may arise following the August 2016 update of WhatsApp terms of service and privacy policy."

317. In its reply to the Commission's Statement of Objections, Facebook acknowledged its infringement of the rules.

D. THE FTC IS INVESTIGATING POSSIBLE CONSENT DECREE VIOLATIONS

318. Facebook is also facing an investigation by the FTC relating to Facebook's compliance with the Consent Decree after the FTC found that the Company told users that third-party apps, like games, would not be allowed to access their data. The FTC found that the apps, by contrast, were able to obtain almost all personal information about a user.

319. On March 20, 2018, former FTC Commissioner Terrell McSweeny issued the following statement regarding recent news reports of allegedly unauthorized use of Facebook user information by a data analytics firm:

> The FTC takes the allegations that the data of millions of people were used without proper authorization very seriously. The allegations also highlight the limited rights Americans have to their data. Consumers need stronger protections for the digital age such as comprehensive data security and privacy laws, transparency and accountability for data brokers, and rights to and control over their data.

320. A Facebook representative also said at that time that the company expected to receive questions from the FTC related to potential violations of the Consent Decree. "We remain strongly committed to protecting people's information," Facebook's deputy chief privacy officer, Rob Sherman, said in a statement. "We appreciate the opportunity to answer questions the FTC may have."

321. Just a few days later, the FTC announced it was investigating Facebook for violations of the Consent Decree. On March 26, 2018, Tom Pahl,

Acting Director of the FTC Bureau of Consumer Protection, issued the following statement regarding reported concerns about Facebook's privacy practices:

> The FTC is firmly and fully committed to using all of its tools to protect the privacy of consumers. Foremost among these tools is enforcement action against companies that fail to honor their privacy promises, including to comply with Privacy Shield, or that engage in unfair acts that cause substantial injury to consumers in violation of the FTC Act. Companies who have settled previous FTC actions must also comply with FTC order provisions imposing privacy and data security requirements. Accordingly, the FTC takes very seriously recent press reports raising substantial concerns about the privacy practices of Facebook. Today, the FTC is confirming that it has an open non-public investigation into these practices.

322. In an April 4, 2018 *Washington Post* article, David Vladeck, who was the Director of the FTC's Bureau of Consumer Protection when the Consent Decree issued, stated that Facebook is "likely grossly out of compliance with the FTC consent decree," adding, "I don't think that after these revelations they have any defense at all." In an April 8, 2018 article, Vladeck was reported as saying that Facebook may face fines of $1 billion or more for failing to comply with the Consent Decree, and that "[t]he agency will want to send a signal … that the agency takes its consent decrees seriously."

323. On April 19, 2018, Senator Blumenthal sent a letter to Acting Chairman of the FTC Maureen Ohlhausen, stating that he was "pleased" the FTC had opened an investigation of Facebook and identifying "evidence that Facebook may have violated its consent decree." He also "encourage[d] the FTC to pursue

strong legal remedies … and [to] set enforceable rules on [Facebook's] future conduct." Blumenthal's letter of April 19, 2018 attaches evidence of the certifications Facebook obtained from Cambridge Analytica and GSR, which confirm that Facebook did not even sign the "settlement agreement" concerning the data sharing and raising the possibility that the agreement is not enforceable.

324. On May 12, 2018, FTC Commissioner Chopra issued a memorandum to all FTC staff and commissioners regarding "Repeat Offenders" that specifically addresses the obligations that corporate officers and directors have to remedy the issues that a consent order is intended to address, noting that the FTC's "orders not only bind a firm, but also its officers." The Commissioner suggested in his recent memorandum that where a company violates a consent order, "a fair[] allocation of liability might include specific recoveries from executives" and that "it may be important for the violating company's board to exercise any rights it may have to claw back bonuses and order the forfeiture of certain unvested stock options and grants." The Commissioner also noted that "executive compensation arrangements may need to be amended to reflect a … commitment to compliance with the law."

325. The Commissioner noted in his memorandum that

> [w]hile these aggressive remedies are typically applied [only] in fraud cases, [the FTC] should not hesitate to apply them against repeat offender corporations and their executives[,] [r]egardless of their size and clout[.]

326. On June 4, 2018, Senators Markey and Blumenthal sent a letter to the FTC and noted that Facebook may have violated the FTC Consent Decree. "The American people deserve to fully understand with whom and under what conditions Facebook provides access to user data[,]" they stated. Also on June 4, 2018, Representative David N. Cicilline and then-New York Attorney General Barbara Underwood sent a letter to Zuckerberg which raised the issue of whether Facebook's data-sharing practices violate the Consent Decree.

327. Defendants' data sharing agreements with third-party companies may have exposed Facebook to liability for violating the Consent Decree. Under the Consent Decree, Facebook is required to obtain permission before sharing a user's private information in a way that exceeds that user's existing privacy settings. The Consent Decree defines "third party" to include a host of other individual entities, but it exempts "service provider[s]" who help Facebook carry out basic functions of its site.

328. PwC's reports to the FTC indicate that Facebook's Privacy Program encompasses these "service providers." The Initial Assessment Report states, in relevant part:

> Service Providers: Facebook has implemented controls with respect to third-party service providers, including implementing policies to select and retain service providers capable of appropriately protecting the privacy of covered information received from Facebook. Facebook's Security team has a process for conducting due diligence on service providers who may receive covered information in order to

> evaluate whether their data security standards are aligned with Facebook's commitments to protect covered information.
>
> As part of the due diligence process, Facebook asks prospective service providers to complete a security architecture questionnaire or vendor security questionnaire to assess whether the provider meets Facebook's functional security requirements to protect the privacy of user data. Based upon the service provider's response to the vendor security questionnaire and other data points, Facebook's Security team determines whether further security auditing is required.
>
> Facebook partners with an outside security consulting firm to conduct security audits, which may include testing of the service provider's controls, a vulnerability scanning program, a web application penetration test, and/or a code review for security defects. Facebook also has a contract policy which governs the review, approval, and execution of contracts for Facebook.

329. Accordingly, after it was revealed that Facebook has data sharing agreements with companies such as Apple and Huawei, Facebook representatives attempted to distinguish those agreements from the developer policies which allowed third-party applications to obtain Facebook information and user data. According to *The New York Times*, Facebook officials called Facebook's partnerships with device manufacturers "private data channels" and said they did not violate the Consent Decree because "the company viewed its hardware partners as 'service providers,' akin to a cloud computing service paid to store Facebook data or a company contracted to process credit card transactions."

330. Facebook could face fines of $40,000 a day per violation if the FTC finds that Facebook broke the agreement.

E. ZUCKERBERG'S TESTIMONY AT THE U.S. CONGRESSIONAL HEARINGS IN APRIL 2018 WAS EVASIVE AND DECEPTIVE

331. On April 10 and 11, 2018, Zuckerberg testified before Congress.

332. In his testimony before both the Senate and House committees, Zuckerberg claimed ignorance about Facebook, the company he created and has controlled. Zuckerberg was not merely dodging questions about obscure corners of Facebook or corporate minutiae, but the most plainly fundamental aspects of Facebook's business and privacy policies. Zuckerberg's deceptive responses reflected his intent to mislead.

333. For example, when asked about the role of Palantir, a data-mining defense contractor co-founded by Board member and early Zuckerberg ally Thiel, Zuckerberg responded, "I'm not really that familiar with what Palantir does."

334. Zuckerberg acted similarly confused when asked whether Facebook does things it openly says it does on its own website. When Senator Roger Wicker asked Zuckerberg if he could confirm whether "Facebook can track a user's internet browsing activity, even after that user has logged off of the Facebook platform," he replied, "Senator — I — I want to make sure I get this accurate, so it would probably be better to have my team follow up afterwards." The answer is unequivocally yes, according to Facebook.com, which stated: "If you're logged out or don't have a Facebook account and visit a website with the Like button or

another social plug-in, your browser sends us a more limited set of info." Zuckerberg could have answered Senator Wicker's question truthfully, but chose not to do so.

335. When Senator Roy Blount asked whether Facebook tracks users across devices (e.g., from their iPhone to their iPad), defendant Zuckerberg replied that he was "not sure of the answer to that question." Meanwhile, Facebook.com prominently displays a diagram and instructions about how to "Advertise to real people cross-device." Once again, his response was deceitful. In his follow-up responses in June, defendant Zuckerberg admitted that "we associate information across different devices" and that "Facebook's services inherently operate on a cross-device basis."

336. On the second day of testimony, Representative Ben Lujan of New Mexico noted that "Facebook recently announced that — a search feature allowing malicious actors to scrape data on virtually all of Facebook's 2 billion users" had previously been raised to Facebook in 2013, and again in 2015, and asked Zuckerberg, "Yes or no: This issue of scraping data was again raised in 2015 by a cyber security researcher, correct?" Zuckerberg responded,

> Congressman, I'm not specifically familiar with that. The feature that we identified — I think it was a few weeks ago, or a couple weeks ago, at this point — was a search feature that allowed people to look up some information that people had publicly shared on their profiles.... So names, profile pictures, public information.

337. Representative Lujan pressed Zuckerberg for an answer, stating:

> I will recognize that Facebook did turn this feature off. My question, and the reason I'm asking about 2013 and 2015, is Facebook knew about this in 2013 and 2015, but you didn't turn the feature off until Wednesday of last week — the same feature that Mr. Kinzinger just talked about, where this is essentially a tool for these malicious actors to go and steal someone's identity and put the finishing touches on it. So, again, you know, one of your mentors, Roger McNamee, recently said your business is based on trust, and you are losing trust. This is a trust question. Why did it take so long, especially when we're talking about some of the other pieces that we need to get to the bottom of? Your failure to act on this issue has made billions of people potentially vulnerable to identity theft and other types of harmful, malicious actors.

338. In response to Representative Lujan's questioning, Zuckerberg said he believed it was due to the fact that there are more than 100 million Facebook "like" buttons around the internet, but did not provide any explanation as to why Facebook did not turn the feature off until after a catastrophic breach two years after the data scraping issue had been reported for a second time.

339. The "like" button, and similar "social plug-in" features provided by Facebook, are actually trackers that transmit information back to Facebook about who visits a website that has the feature, even when the user is not logged in on Facebook. This kind of invisible tracker allows Facebook, and its customers, to track when users make purchases on unrelated third-party websites. Facebook's "like" button has enabled Facebook to track and collect an average of 29,000 data points for individual Facebook users, in comparison to the 1,500 data point average

for non-Facebook platforms that track user activity.

340. While Zuckerberg eventually admitted to the data collection of non-Facebook users, he stated it was "to prevent the kind of scraping" described by Representative Lujan, and claimed that he was not familiar with the "shadow profiles" that organize the data of non-Facebook users. Yet, Facebook's developer website specifically mentions "shadow profiles" that were permitted by the company's policies.

341. Of course, Facebook's partnerships with the data aggregators described above suggest that Zuckerberg is not only familiar with these practices, but knows they are a significant source of revenue that is derived from Facebook's advertising services and privacy policies permitting this type of activity to occur.

342. If Zuckerberg was actually unaware that these practices were occurring on Facebook's platform or as a result of services offered by Facebook, it would be a total abdication of his duty to be reasonably informed about the company's core advertising business and privacy policies.

343. Indeed, as Representative Dingell noted, it would be "striking" if defendant Zuckerberg did not know these "key facts" as CEO. In questioning defendant Zuckerberg, Representative Dingell pointed out many of the "key facts" Zuckerberg claimed not to know, stating:

> You didn't know about major court cases regarding your privacy

> policies against your company. You didn't know that the FTC doesn't have fining authority and that Facebook could not have received fines for the 2011 consent order. You didn't know what a shadow profile was. You didn't know how many apps you need to audit. You did not know how many other firms have been sold data by Dr. Kogan other than Cambridge Analytica and Eunoia Technologies, even though you were asked that question yesterday. And yes, we were all paying attention yesterday. You don't even know all the kinds of information Facebook is collecting from its own users.
>
> Here's what I do know. You have trackers all over the Web. On practically every website you go to, we all see the Facebook Like or Facebook Share buttons. And with the Facebook pixel, people browsing the Internet may not even see that Facebook logo. It doesn't matter whether you have a Facebook account. Through those tools, Facebook is able to collect information from all of us. So I want to ask you, how many Facebook like buttons are there on non-Facebook Web pages?

344. Defendant Zuckerberg responded with the same refrain echoed throughout the entire two days of his testimony, "Congressman, I don't know the answer to that off the top my head, but we'll get back to you."

345. Defendant Zuckerberg's claimed ignorance of the key facts identified by Representative Dingell is "striking" and unbelievable. As set forth herein, these facts go to the very heart of Facebook's business model, and all of the Individual Defendants had a duty to be reasonably informed about Facebook's core advertising business and practices, and a duty to oversee Facebook's operations and compliance with the law, pursuant to their fiduciary duties owed to Facebook and affirmative obligations under the Consent Decree.

346. During the House committee hearing on April 11, 2018, Representative David McKinley ("McKinley") noted that online pharmacies are using Facebook's website to sell drugs illegally, telling defendant Zuckerberg, "Your [Facebook's] platform is still being used to circumvent the law, and allow people to buy highly addictive drugs without a prescription[.]" Representative McKinley noted that it happens all the time, and pointed out that Zuckerberg isn't fulfilling the promise he made to remove ads for illegal online pharmacies from Facebook's website, telling defendant Zuckerberg, "you didn't do it." "Opioids are still available on your site … without a prescription on your site." McKinley added, "Facebook is actually enabling an illegal activity, and in so doing, you are hurting people."[17]

F. CTO MIKE SCHROEPFER TESTIFIED BEFORE THE EUROPEAN PARLIAMENTARY COMMITTEE IN MAY 2018

347. On April 26, 2018, Facebook's Chief Technology Officer Mike Schroepfer ("Schroepfer") appeared before the European Parliamentary Committee to explain Facebook's response to a sequence of data, privacy, and fake news scandals, according to *Business Insider*. During the meeting, Schroepfer admitted that it was a mistake to not alert users when the Individual Defendants initially

[17] Plaintiffs expressly incorporate by reference as though fully set forth herein the transcripts of the Congressional hearings held on April 10, 2018 and April 11, 2018, including Zuckerberg's testimony to both the House and Senate committees concerning Facebook's user privacy.

learned that Facebook's data had been sold to Cambridge Analytica in 2015, and Schroepfer apologized for the breach of users' trust. Schroepfer also stated that Facebook "not never, but rarely" read the terms and conditions of the application that improperly shared user data with Cambridge Analytica, *BBC News* reported.

348. The Parliamentary committee criticized Facebook practices regarding political advertising. Damian Collins ("Collins"), the chair of the DCMSC accused Facebook of having tools on its platform that work for the advertiser more than they work for the consumer. Schroepfer responded, "we were slow to understand the impact of this at the time" and promised to make political advertising far more transparent in the future, yet admitted that there was currently no way for people to opt out of it entirely, reported *BBC News*.

349. A Conservative Member of Parliament ("MP") Julian Knight described Facebook as a "morality free zone," while Paul Farrelly, a MP from the Labour Party, quoted journalist Matt Taibbi in describing Facebook as "a great vampire squid wrapped around the face of humanity, relentlessly jamming its blood funnel into anything that smells like money," reported the Register.

350. Schroepfer's appearance before the parliamentary committee left dozens of questions unanswered, and "the evidence presented by Schroepfer lacked many of the important details that we need," Collins said. The MP committee once again urged Zuckerberg to appear and testify before the committee, but he refused

a second time.

G. DEFENDANT ZUCKERBERG RELUCTANTLY TESTIFIED BEFORE THE EU PARLIAMENTARY COMMITTEE IN MAY 2018

351. When he finally appeared before the committee on May 22, 2018, European Parliament officials laid into Zuckerberg for Facebook's data privacy failings and raised the prospect of breaking up the social network, which some suggested had amassed an unfair share of power online.

352. The hearing's format allowed Zuckerberg to listen to questions from a dozen EU officials and then answer them in one statement afterward. Instead of directly answering many of the questions, Zuckerberg limited his response to the talking points he had already made during two days of testimony before the U.S. Congress the previous month.

353. The questions included: (i) what steps Facebook is taking to avoid future data "leaks" and to combat so-called fake news; (ii) whether Facebook will allow users to truly opt-out of targeted advertising; and (iii) whether Facebook has an anticompetitive stranglehold on the social media market. Other questions included: (i) what data Facebook collects on non-Facebook users; (ii) whether Facebook can promise that personal data collected for "security purposes" won't be used for targeted advertising; and (iii) whether Facebook would consider showing the public how its algorithms work.

354. Many of the EU officials at the May 22 hearing, including MP Guy

Verhofstadt, appeared skeptical of Zuckerberg's promises to do better. Verhofstadt, a former prime minister of Belgium, said:

> You have to ask yourself how you will be remembered, as one of the three internet giants, along with Steve Jobs and Bill Gates, who have enriched our world and our society, or on the other hand, as the genius who created a digital monster that is destroying our democracy and our society?

355. Under new EU General Data Protection Regulation ("GDPR"), which went into effect in May, 2018, Facebook and other technology companies could be fined up to four percent (4%) of their global revenue for privacy breaches. For Facebook, this could mean a fine of more than $1.5 billion.

356. On June 30, 2018, Facebook provided the House Energy and Commerce Committee with seven hundred forty-seven (747) pages of written responses to the questions that defendant Zuckerberg had been asked by the Committee during the hearing on April 11, 2018, but claimed he did not know the answers. Notably, of just six questions that the committee members had asked defendant Zuckerberg to answer concerning Facebook's Board, not one was directly answered in the Facebook responses:

> The Honorable Anna G. Eshoo:
> Isn't Facebook's Board complicit after years of transgressions and apologies by management?
>
> Facebook: We recognize that we have made mistakes, and we are committed to learning from this experience to secure our platform further and make our community safer for everyone going forward. As our CEO Mark Zuckerberg has said, when you are building

something unprecedented like Facebook, there are going to be mistakes. What people should hold us accountable for is learning from the mistakes and continually doing better—and, at the end of the day, making sure that we're building things that people like and that make their lives better.

Particularly in the past few months, we've realized that we need to take a broader view of our responsibility to our community. Part of that effort is continuing our ongoing efforts to identify ways that we can improve our privacy practices.

We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find.

We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook.

We explain the services we offer in language that's easier to read. We've also updated our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products.

The Honorable Anna G. Eshoo:
Does your board want you to resign? Not addressing security is immature behavior?

Facebook: We recognize that we have made mistakes, and we are committed to learning from this experience to secure our platform further and make our community safer for everyone going forward.

As our CEO Mark Zuckerberg has said, when you are building something unprecedented like Facebook, there are going to be mistakes. What people should hold us accountable for is learning from the

> mistakes and continually doing better—and, at the end of the day, making sure that we're building things that people like and that make their lives better.
>
> Particularly in the past few months, we've realized that we need to take a broader view of our responsibility to our community. Part of that effort is continuing our ongoing efforts to identify ways that we can improve our privacy practices.
>
> We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find.
>
> We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook.
>
> We explain the services we offer in language that's easier to read. We've also updated our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products.

357. In Facebook's written responses, Defendants confirmed that they had not taken action against any third-party apps for similar data-sharing and extrication practices as Kogan and Cambridge Analytica, and only went after those that posed a threat to Facebook's competitive position. In response to a request for "a list of developers that Facebook has taken legal action against for violations of Facebook's developer policy[,]" Facebook responded:

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process.

We also use tools like cease-and-desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets.

In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data.

We have invested significant resources in these efforts. Facebook is presently investigating apps that had access to large amounts of information before we changed our platform policies in 2014 to significantly reduce the data apps could access.

As of early June 2018, around 200 apps (from a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, and myPersonality) have been suspended—pending a thorough investigation into whether they did in fact misuse any data.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

H. FACEBOOK HAS BEEN REPEATEDLY FINED FOR VIOLATIONS OF FOREIGN PRIVACY LAWS, AND RECENT REPORTS SUGGEST THE VIOLATIONS ARE ONGOING

358. On March 31, 2015, a team of researchers tapped by Belgium's data

protection regulator to probe Facebook's privacy policy changes released an updated report accusing the company of violating European Union privacy law by tracking the activities of nonusers. According to version 1.2 of the report prepared by the Interdisciplinary Center for Law and ICT at the University of Leuven in Belgium, which was first released in February 2015, Facebook violated the EU's 2002 e-privacy directive by carrying out tracking practices that are even more expansive than the researchers had initially discovered.

359. In their first draft of the report, which is titled "From Social Media Service to Advertising Network: A Critical Analysis of Facebook's Revised Polices and Terms," the researchers revealed that while Facebook provides users with "high-level information" about its tracking practices, the collection and use of device information from users that is laid out in the company's most recent privacy policy fails to comply with EU privacy laws that require free and informed prior consent before storing or accessing information on an individual's device.

360. The updated report added the discovery that Facebook also tracks nonusers in a way that the researchers allege violates the laws' notice and consent requirements. "Facebook places cookies whenever someone visits a webpage belonging to the facebook.com domain, even if the visitor is not a Facebook user," the report said. "This means that Facebook tracks its users across websites even if they do not make use of social plug-ins, and even if they are not logged in, and

Facebook tracking is not limited to Facebook users."

361. Facebook's Chief Technology Officer, Mike Schroepfer, admitted in a May 30, 2018 interview with *Recode* that Facebook obtains information about non-users via cookies and that this data cannot be recaptured or deleted, stating, "in many cases you have cookie data from a device or from a browser, but I don't know which person this is associated with, and so it's pretty hard to get that data back for an individual."

362. According to the Belgian researchers' report, Facebook places a cookie on nonusers' devices that contains a unique identifier and has an expiration date of two years, and uses a "range of additional cookies" for visitors who are already users of the site. Once these cookies have been set, "Facebook will in principle receive the cookies during every subsequent visit to a website containing a Facebook social plug-in" such as the site's "like" button, which is currently present on more than thirteen (13) million sites, the report noted. The cookies deliver to Facebook a wealth of information about users' activities, such as the URL of webpages they have visited and information about the browser and operating system, the report added.

363. The report concludes that Facebook's practice violates the EU's e-privacy directive by taking users' silence to mean that they want to be tracked across third-party websites for ad targeting purposes, and by failing to inform

nonusers that their information may be gathered when they interact with a Facebook plug-in on a third-party site. While Facebook has claimed that the cookies it sets on nonusers' browsers are for security purposes, which are generally allowed under an exemption to the e-privacy directive, the report noted that the exemption does not cover the use of cookies for the security of websites or services that have not been explicitly requested by the user. "As a result, Facebook's tracking of nonusers, even if the data is not used for ad targeting or other purposes, violates … the e-privacy directive," the report concluded.

1. The European Commission Found the WhatsApp Acquisition Violated the EU Merger Regulation and Fined Facebook €110 Million

364. On March 12, 2018, WhatsApp attorneys signed an "undertaking" with the Information Commissioner responsible for enforcement of the Irish DPA, acknowledging that WhatsApp's "shar[ing] any personal data with the Facebook family of companies" would be a violation of the DPA because WhatsApp had: (i) "not identif[ied] a lawful basis of processing for any such sharing of personal data;" (ii) "fail[e]d to provide adequate fair processing information to users in relation to any such sharing of personal data;" and (iii) [i]n relation to existing users, such sharing … involved the processing of personal data for a purpose that is incompatible with the purpose for which such data were obtained." WhatsApp

"commit[ed]" not to engage in these practices only with respect to users in the European Union, and WhatsApp and Facebook continue to share the personal data of U.S. users with each other and with other third-party companies.

365. On May 18, 2017, the European Commission announced in a press release that it had fined Facebook €110 million "for providing incorrect or misleading information during the Commission's 2014 investigation under the EU Merger Regulation of Facebook's acquisition of WhatsApp." The press release explained:

> When Facebook notified the acquisition of WhatsApp in 2014, it informed the Commission that it would be unable to establish reliable automated matching between Facebook users' accounts and WhatsApp users' accounts. It stated this both in the notification form and in a reply to a request of information from the Commission. However, in August 2016, WhatsApp announced updates to its terms of service and privacy policy, including the possibility of linking WhatsApp users' phone numbers with Facebook users' identities.

366. The Commission found that, "contrary to Facebook's statements in the 2014 merger review process, the technical possibility of automatically matching Facebook and WhatsApp users' identities already existed in 2014, and that Facebook staff were aware of such a possibility." The Commission said the decision was "based on a number of elements going beyond automated user matching" and was "unrelated to either ongoing national antitrust procedures or privacy, data protection or consumer protection issues," but noted that those issues

"may arise following the August 2016 update of WhatsApp terms of service and privacy policy."

367. In its reply to the Commission's Statement of Objections, Facebook acknowledged its infringement of the rules.

2. The German Supreme Court Declared Facebook's "Friend Finder" Feature Unlawful in 2016

368. In February 2016, the German Supreme Court declared the Friend Finder feature on Facebook to be unlawful. The court found that the service, which allows the social networking giant to access users' contacts and send emails to non-users, was not adequately explained to consumers and amounted to harassing advertising.

369. Facebook's users did not provide the same information to Facebook that was ultimately used for targeting advertisements – while it was developed with user data, this data was aggregated, and ultimately new information was generated through Facebook's algorithm that was used for targeting purposes. Because this new information generated through Facebook's algorithm was not the same information that Facebook users had provided, they did not (and could not) know the information existed, let alone was being shared or used for any purpose. Facebook's users did not, because they could not, consent to such information being shared with third parties or used for targeted advertising. Thus, Facebook's

users did not implicitly or explicitly consent to Facebook's practices.

3. The Spanish Agency for Data Protection Fined Facebook €1.2 Million Euros in 2017

370. On September 11, 2017, the Spanish Agency for Data Protection ("AEPD") announced that it had fined Facebook €1.2 million for violating data protection regulations following its investigation to determine whether the data processing carried out by Facebook complied with the data protection regulations. The AEPD stated that its investigation made it possible to verify that Facebook does not inform its users in a comprehensive and clear way about the data that it will collect and the treatments that it will carry out with such data, but that it is limited to giving some examples. In particular, the AEPD found that Facebook collects other data derived from the interaction carried out by users on the platform and on third-party sites without them being able to clearly perceive the information that Facebook collects about them or with what purpose they are going to use it.

371. The AEPD also found that the privacy policy of Facebook (i) contains generic and unclear expressions and (ii) requires access to a multitude of different links to know it. Further, the AEPD concluded that Facebook makes an inaccurate reference to the use it will make of the data it collects, such that a Facebook user with an average knowledge of the new technologies does not become aware of the data collection or storage and subsequent treatment, or what the data collection will

be used for.

4. The French Data Protection Authority Fined Facebook its Maximum Allowable Fine in 2017

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

5. A German Court Found Facebook's Default Settings are Illegal and Facebook's Terms of Service are Invalid to Obtain Consent in 2018

373. On February 12, 2018, a German court found that Facebook's failure to obtain users' informed consent before collecting their data was illegal. The Berlin Regional Court found that Facebook flouted Germany's data protection law by turning data sharing settings on by default. One pre-activated setting on Facebook's smartphone app shared users' locations to the people they are chatting with, the German court said. Per the German court's ruling, Facebook also pre-ticked a box authorizing search engines to show links to user profiles in search results, making it easier for anyone to find someone's personal profile.

374. The court found that eight clauses in Facebook's terms of service were invalid, including a declaration that users consented to the Company using their names and profile pictures "for commercial, sponsored or related content" or sending their data to the United States.

6. Facebook Was Ordered to Stop Tracking Internet Usage and Faces Up to €100 Million in Fines

375. On February 16, 2018, a Belgian court ordered Facebook to stop tracking Belgian citizens' online activity on third-party websites — or face up to €100 million ($125 million) in fines. Facebook tracks the movements of visitors to outside websites by installing cookies, social plug-ins like its "like" button, or so-called pixels, which are invisible to the naked eye, the Belgian Privacy Commission said. The software tracks even those who do not have Facebook accounts, the privacy watchdog alleged in a suit filed in 2015.

376. The Brussels Court of First Instance sided with the Belgian Privacy Commission, ruling that Facebook "insufficiently" discloses what kind of data it collects, what it does with the data and how long it stores it. Facebook does not do enough to get users' consent, the court said in a Dutch-language statement. The court threatened Facebook with fines of up to €250,000 a day, or up to €100 million in total, if it does not stop tracking Belgians and delete all data it has already gathered using the methods.

VI. THE INDIVIDUAL DEFENDANTS VIOLATED SECTION 14(A) OF THE EXCHANGE ACT AND SEC RULE 14A-9 BY ISSUING MATERIALLY MISLEADING PROXY STATEMENTS IN 2016, 2017 AND 2018

377. Defendants violated Section 14(a) of the Exchange Act and SEC Rule 14a-9 by causing Facebook to issue proxy statements that failed to disclose the Cambridge Analytica incident, or the seriously deficient internal controls and privacy policies that Facebook maintained which caused Facebook to violate user privacy laws and damage Facebook's reputation. Defendants' failure to disclose these and other material facts likewise constitutes a breach of trust, and of their fiduciary duties owed to Facebook.

378. The Exchange Act requires publicly-traded companies to disclose to shareholders "material information," the kind of information that an investor would want to know to protect their investment. The SEC issued guidance on public reporting of cybersecurity incidents, noting that the commission "encourages companies to continue to use Form 8-K or Form 6-K to disclose material information promptly, including disclosure pertaining to cybersecurity matters."

379. In 2016, 2017 and 2018, Facebook did not mention the material information described herein and, as a result, convinced shareholders to approve Board-endorsed proposals and reject other proposals that the Board recommended voting against.

THE BOARD ISSUED THE MATERIALLY MISLEADING PROXY STATEMENTS IN RECOMMENDING A VOTE AGAINST SHAREHOLDER PROPOSALS ON THE BASIS OF THE DIRECTORS' MISSTATEMENTS ABOUT FACEBOOK'S PRIVACY PRACTICES AND BOARD OVERSIGHT

A.

380. Facebook's Board, including all of the Individual Defendants, caused Facebook to issue and file with the SEC materially misleading Proxy Statements soliciting their vote against various matters proposed by shareholders.

381. In soliciting a "no" vote on various shareholder proposals, the Proxy Statements contained misrepresentations concerning the Board's role in risk oversight. For example, on page 16 of the 2018 Proxy Statement, the Individual Defendants stated:

> **"Board Role in Risk Oversight"**
>
> Our board of directors as a whole has responsibility for overseeing our risk management and believes that a thorough and strategic approach to risk oversight is critical. 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 regular reports from our management team, including senior personnel that lead a variety of functions across the business, and from our internal audit department, as well as input from external advisors, as appropriate. These reports are designed to provide timely visibility to the board of directors and its committees about the identification and assessment of key risks, our risk mitigation strategies, and ongoing developments.
>
> 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, legal, and regulatory risk exposures, which span a variety of areas including

> litigation, regulatory compliance, reputational and policy matters, platform integrity efforts, financial reporting, cybersecurity, and international operations. 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 corporate governance and 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.

382. The Proxy Statements misled shareholders to vote against "Stockholder Proposals" meant to improve the Board's governance, failing to disclose negative, true facts about the Individual Defendants' performance described above.

B.

THE BOARD ISSUED THE MATERIALLY MISLEADING PROXY STATEMENT IN SOLICITING THE DIRECTORS' RE-ELECTION TO FACEBOOK'S BOARD AND COMPENSATION PACKAGES

383. The Individual Defendants violated Section 14(a) of the Exchange Act and SEC Rule 14a-9, thereby breaching their duty of candor owed to Facebook and its shareholders, by causing Facebook to issue Proxy Statements soliciting their re-election to the Board, failing to disclose the Cambridge Analytica incident and deliberately concealing Facebook's advertising practices and corporate policies which allowed and perpetuated Facebook's violations of user privacy and other laws. Defendants' failure to disclose those material facts likewise constitutes a

breach of their fiduciary duties.

384. Defendants also violated Section 14(a) of the Exchange Act and SEC Rule 14a-9 by causing Facebook to issue Proxy Statements soliciting approval of compensation packages, failing to disclose the Cambridge Analytica incident which caused serious harm and damages to Facebook or the seriously deficient privacy policies that allowed it to occur. Defendants' failure to disclose those material facts likewise constitutes a breach of their fiduciary duties and, in particular, their duty of candor.

385. The 2016 Proxy Statement, the 2017 Proxy Statement, and the 2018 Proxy Statement (collectively, the "Proxy Statements") omitted any disclosures regarding (i) the Cambridge Analytica leak; (ii) the Individual Defendants' knowledge that Facebook's internal controls and systems were inadequate and ineffective to protect user information; (iii) the Individual Defendants' knowledge of data security failures that had actually materialized and had not been disclosed; (iv) the fact that Facebook's internal controls and systems were inadequate to ensure that the company complied with applicable notification and disclosure requirements concerning the Cambridge Analytica leak; (v) the fact that the Individual Defendants failed to maintain appropriate policies and procedures to detect and prevent data security leaks and to protect user information; and (vi) the fact that the Individual Defendants failed to appropriately address Facebook's

privacy practices and misleading claims regarding same as required by the Consent Decree; and (vii) the fact that, as a result of the foregoing, Facebook may be in violation of the Consent Decree.

386. The Proxy Statements harmed Facebook by interfering with the proper governance on its behalf that follows stockholders' informed voting of directors. As a result of the false or misleading statements in the Proxy Statements, Facebook stockholders voted to re-elect all of the Individual Defendants to the Board and approve their compensation packages.

387. The statements in the Proxy Statements conveyed that Facebook's corporate governance structure was "effective" and provided "oversight of management and Board accountability." In reality, Facebook's corporate government structure allowed senior executives and the Board to sidestep real accountability and instead continue perpetuating the data security practices that led to the Cambridge Analytica leak, and fail to disclose or notify users of the leak.

388. The Proxy Statements, which contained materially misleading statements and thus deprived shareholders of adequate information necessary to make a reasonably informed decision, caused Facebook's stockholders to re-elect all of the Individual Defendants to the Board and approve their compensation while they were breaching their fiduciary duties to Facebook and deliberately concealing material information concerning the Cambridge Analytica leak and its

effects on Facebook's business and reputation.

VII. DEFENDANTS VIOLATED SECTION 10(B) OF THE EXCHANGE ACT AND SEC RULE 10B-5 BY KNOWINGLY OR RECKLESSLY ISSUING MATERIALLY FALSE AND MISLEADING STATEMENTS

389. In breach of their fiduciary duties to Facebook and its shareholders, and in violation of Section 10(b) of the Exchange Act and SEC Rule 10b-5, the Individual Defendants issued, and caused Facebook to issue, statements that, in light of the practices detailed above, were materially false or misleading when made. The Individual Defendants' misrepresentations artificially inflated the price of Facebook shares, causing the company to purchase shares at artificially inflated prices, through its significant stock repurchase program.

390. On November 18, 2016, with full knowledge of the exfiltration and unauthorized use of user data and the undisclosed deviation of its policies, as described above, the Board authorized Facebook to repurchase $6 billion of its own shares of common stock. The share repurchases were the first in Facebook's history since becoming a public company.

391. Between 2017 and March 31, 2018, with the Board's authorization and consent, Facebook repurchased billions worth of Facebook stock. According to Facebook's 2017 Annual Report, Facebook repurchased approximately 13 million Class A common shares for an aggregate amount of approximately $2.07

billion in 2017 alone. In repurchasing these shares, the Individual Defendants falsely signaled to the public that they believed Facebook shares were undervalued and that the repurchases were the best use of Facebook's cash. The share repurchases also had the effect of growing Facebook's earnings per share—as share repurchases lower the number of shares outstanding, on which earnings per share are based—as well as its return on assets, return on equity, and other metrics. Together, these actions helped inflate Facebook's share price.

392. Since the Board did not have a separate Finance Committee, the entire Board was charged with the responsibility for recommending and approving securities repurchases. All Board members approved the repurchase transactions.

393. During the time of the repurchase transactions, the Individual Defendants knowingly or recklessly made materially false or misleading statements and/or failed to disclose material information regarding Facebook's user privacy practices, including: (i) the failure to disclose that Facebook had already experienced the exfiltration and unauthorized use of data impacting millions of Facebook users; (ii) that Facebook had intentionally deviated from its own policy supposedly implemented in 2015 to prevent access to user information; and (iii) that Facebook had no internal processes in place to control, monitor or retrieve user data that had been sent from Facebook servers. To the contrary, as revealed by Facebook's former platform operations manager responsible for policing data

breaches by third-party software developers, Facebook had no such controls, and millions of Facebook users had their data harvested by third parties without their knowledge.

394. The Individual Defendants also made false or misleading statements or omissions relating to its internal controls and risks in Facebook's SEC filings. For example, Facebook's 2015, 2016 and 2017 Annual Reports, signed by the Individual Defendants, each contain approximately twenty (20) pages of risk disclosures, yet the only reference to the unauthorized use of user information refers to the mere risk of it happening in the future, obfuscating the fact that such unauthorized use had already occurred and on a massive scale impacting tens of millions of Facebook users. The Annual Reports falsely contain certifications that Facebook's internal controls are effective. The SEC filings also falsely represented that Facebook maintained robust privacy policies and a risk management system to protect user data.

395. The Individual Defendants' statements (including those contained in Facebook's SEC filings described above) were materially false and misleading, and failed to disclose material information, for the reasons stated above, including the fact that Facebook had already: (i) experienced the unauthorized access and use of user information, (ii) deviated from its own policy to restrict access to user information, and (iii) failed to implement and maintain adequate risk controls at the

company.

396. In repurchasing shares in connection with the stock repurchase program, Facebook relied on Defendants' false or misleading statements, either directly or through the "fraud on the market" doctrine.

397. Facebook justifiably expected the Individual Defendants to disclose material information as required by law and SEC regulations in Facebook's periodic filings with the SEC. Facebook would not have repurchased its securities at artificially inflated prices had the Individual Defendants disclosed all material information then known to them, as detailed in this Complaint. Thus, reliance by Facebook should be presumed with respect to the Individual Defendants' omissions of material information.

398. Additionally, the "fraud on the market" presumption applies to the Individual Defendants' misstatements of material fact or failures to disclose material facts.

399. As a result of the foregoing, the market for Facebook's common stock promptly digested current information regarding Facebook from all publicly-available sources and reflected such information in the price of Facebook's stock. The foregoing facts indicate the existence of an efficient market for trading of Facebook stock and support application of the fraud-on-the-market doctrine

400. Facebook relied on the integrity of the market price for the repurchase of its stock and is entitled to a presumption of reliance with respect to the Individual Defendants' misstatements and omissions alleged in this Complaint.

401. Had Facebook known of the material adverse information not disclosed by the Individual Defendants or been aware of the truth behind the Individual Defendants' material misstatements, the Company would not have repurchased Facebook stock at artificially inflated prices.

402. The Individual Defendants, because of their positions of control and authority as officers or directors of Facebook, were able to -- and did -- control the content of the various SEC filings and other public statements pertaining to Facebook during the Relevant Period. Each Individual Defendant was provided with copies of the documents alleged in this Complaint to be false or misleading prior to or shortly after their issuance or had the ability or opportunity to prevent their issuance or to cause them to be corrected. Accordingly, each Individual Defendant is responsible for the accuracy of the public reports, releases, and other statements detailed in this Complaint and is therefore primarily liable for the misrepresentations in them or misleading omissions from them.

403. The price of Facebook's common stock was artificially inflated as a result of the Individual Defendants' materially false and misleading statements and

omissions identified above. The Individual Defendants engaged in a scheme to deceive the market and a course of conduct that operated as a fraud or deceit on Facebook, which repurchased shares at artificially-inflated prices. When the Individual Defendants' prior misrepresentations and fraudulent conduct were disclosed and became apparent to the market, the price of Facebook stock fell as the prior artificial inflation dissipated. As a result of its purchases of Facebook shares, the Company suffered damages under the federal securities laws.

VIII. CERTAIN DEFENDANTS SOLD THEIR FACEBOOK STOCK WHILE IN POSSESSION OF MATERIAL, NONPUBLIC INFORMATION

404. During the relevant period, certain of the Individual Defendants took advantage of the artificial inflation of Facebook's shares caused by the Individual Defendants' false or misleading statements and omissions that failed to disclose the Cambridge Analytica incident or the nature and extent to which Facebook's internal controls and policies had permitted the breach to occur. Specifically, Zuckerberg, Sandberg and Koum collectively sold or otherwise disposed of nearly $1.5 billion worth of their personally-held shares of Facebook stock during that time, all while in the possession of material, non-public information. At the time of these stock transactions in 2018, defendants Zuckerberg, Sandberg and Koum knew about or recklessly disregarded material, non-public information regarding the Cambridge Analytica scandal and Facebook's advertising practices, violations

of user privacy and data security laws, and other damages to Facebook caused by the Individual Defendants' actions (or conscious inaction) in connection with the practices described above.

405. For example, the IRS summons indicates that Facebook executives testified under oath about their communications and presentations to the Board beginning in at least 2009 regarding "advertising operations and revenues[.]"

406. Further, a former Facebook employee testified under oath that he had participated in a sale of stock by Facebook employees and had seen a valuation in connection with that permitted sale. According to the employee, whose name is redacted from the documents obtained by Plaintiff in this case, a valuation amount was communicated to all employees who were eligible to sell their stock.

407. All of the Individual Defendants knew (or recklessly disregarded that) these and other relevant facts were necessary to make the Individual Defendants' statements truthful and not misleading, but were not disclosed by the Individual Defendants. While these and other material facts were concealed from Facebook shareholders and the public, defendants Zuckerberg, Sandberg and Koum sold or otherwise disposed of Facebook common stock on the basis of that information, thereby breaching their fiduciary duties. In particular,

a. Zuckerberg sold 5,423,200 of his Facebook shares for proceeds of over $978 million.

b. Sandberg sold 196,684 of her Facebook shares for proceeds of over $35 million.

c. Koum sold 2,485,347 of his Facebook shares for proceeds of over $442 million.

408. The Exchange Act requires publicly traded companies to disclose to shareholders "material information," the kind of information that an investor would want to know to protect their investment. The SEC issued guidance on public reporting of cybersecurity incidents, noting that the Commission "encourages companies to continue to use Form 8-K or Form 6-K to disclose material information promptly, including disclosure pertaining to cybersecurity matters." In the 2017 Proxy Statement and 2018 Proxy Statement, Facebook did not mention the Cambridge Analytica incident, nor did Facebook mention the incident in any of its Form 8-K or other filings with the SEC. Instead, Facebook made general statements in its most recent proxy statement and annual report on Form 10-K about potential -- not actual -- user privacy and data security risks, and certified that its internal controls were adequate and complied with applicable laws (which necessarily include the Consent Decree). By trading while in possession of this material, non-public information, defendants Zuckerberg, Sandberg and Koum breached their fiduciary duties owed to the Company and its shareholders.

IX. DAMAGES TO FACEBOOK

409. As set forth above, the Individual Defendants' misconduct has wrought extreme financial and reputational damage to Facebook. The reputational damage suffered by Facebook is especially harmful to Facebook because the Company is built on customer trust.

410. The Individual Defendants breached this trust by acting in direct contravention of Facebook's publicly-touted credo. This reputational harm undoubtedly translates into long-term damage to the company.

411. The illegal practices and the Individual Defendants' gross failures to timely address, remedy, or disclose them also severely damaged Facebook's reputation within the business community and in the capital markets, as evidenced by, for example, the more than $50 billion loss in market capitalization after the Cambridge Analytica debacle (and Defendants' knowledge of or conscious disregard of it) were revealed. Further, in determining whether to use, conduct business with, and/or invest in Facebook, Facebook's customers and current and potential investors consider the company's ability to (i) protect its users' personal information and (ii) implement adequate controls to ensure practices that may violate user privacy are timely discovered and properly addressed. Facebook's failure to satisfy customer and investor concerns in this regard has harmed Facebook, as customers are less likely to use websites that knowingly permit or

encourage unscrupulous behavior, and investors are less likely to invest in companies that lack internal controls and fail to timely disclose material information. Thus, Facebook's ability to attract customers and investors is now impaired.

412. Further, as a direct and proximate result of the Individual Defendants' actions, Facebook has expended (and will continue to expend) significant additional money, including: (i) 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 (ii) costs incurred from the substantial compensation and benefits paid to the Individual Defendants who are responsible for the scheme.

413. On May 7, 2018, Facebook announced a major "restructuring" that will involve reorganization of its executives into three branches: (1) family of applications, which include Instagram, Messenger, WhatsApp, and Facebook's mobile app, led by Chief Product Officer Chris Cox; (2) central product services, which include advertisements, product management, and analytics, led by Vice President of Growth Javier Olivan; and (3) new platforms and infrastructure, which include augmented reality and virtual reality, blockchain and data privacy, led by Chief Technology Officer Mike Schroepfer.

1. The Board Approved Executive Compensation Practices That Encouraged the Unlawful Activity

414. In 2017, Facebook's Compensation & Governance Committee created a new "Equity Subcommittee" comprised of Sandberg and Facebook's Chief Financial Officer, Wehner, which has the "authority to review and approve grants of restricted stock units to employees and consultants" that is traditionally granted to the Board.

415. According to the 2018 Proxy Statement, Facebook's

> [e]xecutive compensation is based on contributions to number of advertisers, delivery of a strategic long-range plan, growth in user engagement, recruiting and developing teams to drive product development in 'new initiatives.' (2018 Proxy Statement at 24) (emphasis added).

Accordingly, by creating the Equity Subcommittee, which is comprised entirely of members of management who determine their own compensation based on metrics that encourage Facebook's unlawful business strategy, the Compensation & Governance Committee members have effectively ceded their oversight responsibilities to the very members of management who are responsible wrongdoers, while at the same time rewarding them for achieving performance goals that encourage the same wrongdoing and advertising practices based on violating user privacy and other laws.

416. Accordingly, there is significant doubt that the non-management Individual Defendants are disinterested because they face a substantial likelihood

of liability for their breaches of fiduciary duties, including their duties of good faith, fair dealing, and loyalty, as well as other violations of law.

417. The entire Board had the duty to ensure Facebook's privacy practices were designed to protect user information and disclose any violations of user privacy in accordance with applicable law. Facebook's internal controls and systems had the ability to detect and report suspicious activity at the developer level, yet failed to prevent violations of user privacy on multiple occasions, in violation of various applicable laws, regulations, and the FTC Consent Decree. The Board's duty was heightened by the fact that the FTC imposed affirmative obligations with respect to Facebook's user privacy practices in the Consent Decree.

418. The Board failed to fulfill its duty to detect and prevent violations of user privacy, and its failure is even more egregious in light of the many blatant warnings both before and during the relevant period that Facebook's privacy policies did not comply with applicable laws, and moreover, that the same practices which violated the law and user trust were Facebook's primary source of revenue.

419. During a May 27, 2015 presentation to the IRS, a Facebook representative indicated that "[Facebook] built 'forecasts,' from internal and external data, projecting [Facebook]'s [REDACTED] on a country-by-country

basis, so that Facebook could look at the forecasts, 'U.S. versus international.'" The representative stated that she has seen both year-long and three-year forecasts, and the IRS subsequently asked Facebook to provide all Documents constituting, reflecting or referring to any such "forecasts" of growth of [redacted], created, obtained or circulated from 2008 until 2012. If, as the IRS disclosures suggest, Facebook forecasted growth based on national and international rights to exploit Facebook's "platform technology," there can be no doubt that the Board knew of such exploitation of user data, and that it has been a core aspect of Facebook's business since well before the company's initial public offering in 2012.

420. In the June 8, 2016 summons, the IRS noted that a former Facebook executive who was examined under oath by the IRS on May 17, 2016

> "(a) made quarterly presentations to [Facebook]'s Board of Directors regarding user growth, projected and actual; (b) other executives of [Facebook] also made quarterly presentations to [Facebook]'s Board of Directors on topics or areas covered by the divisions they supervised; and (c) quarterly financials were presented to the Board of Directors as part of the quarterly board meetings."

421. Given the Board's awareness and deliberate concealment of the extent to which Facebook's business model and revenue depends upon its targeted advertisements, which requires the Company to collect, store, and share massive amounts of user data, and Facebook's failure to disclose or notify users of these

practices, it is clear the Board either deliberately or recklessly permitted Facebook to pursue profit at the expense of complying with the law.

422. The Individual Defendants directed, authorized, and oversaw the misconduct alleged herein, and they regularly monitored Facebook's user and revenue growth. Zuckerberg was personally involved in developing Facebook's platform and was responsible for its implementation to a degree far beyond his supervisory role as Facebook's CEO. In that role, Zuckerberg specifically instructed Facebook employees to prepare for, and circumvent, the blocks that he anticipated other websites would implement.

423. The Individual Defendants maintained executive compensation practices that improperly incentivized Facebook's growth, and the illegal activity, throughout the relevant period.

424. The Board's actions and decisions are not entitled to the presumption of the business judgment rule because the Individual Defendants failed to act in good faith and put their own personal and financial interests above those of Facebook and its shareholders.

2. The Board Failed to Comply with the Consent Decree and Has Exposed Facebook to Further Sanctions

425. The Individual Defendants were aware of, yet disregarded, their affirmative obligations to oversee Facebook's compliance with the Consent Decree

entered into with the FTC.

426. Because a majority of the directors face a substantial risk of liability for Facebook's violations of law, or at a minimum, for exposing Facebook to sanctions for violating the Consent Decree, demand is futile.

427. Section VII of the Consent Decree provides, in relevant part, that:

> [Facebook] shall deliver a copy of this order to all current and future principals, officers, directors, and managers; (2) all current and future employees, agents, and representatives having supervisory responsibilities relating to the subject matter of this order, and (3) any business entity resulting from any change in structure…. [Facebook] shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

428. Thus, each of the Individual Defendants received the Consent Decree and therefore had knowledge of the issues addressed therein and Facebook's affirmative obligations under the agreement. Notwithstanding their receipt and knowledge of the Consent Decree, the Individual Defendants failed to ensure Facebook complied with the Consent Decree.

429. Defendants Andreessen, Bowles and Desmond-Hellmann are members of Facebook's Audit Committee, which is responsible for overseeing Facebook's legal and regulatory risk exposure. Defendant Bowles is the Chairman of the Audit Committee and a financial expert, as defined under the SEC rule.

430. The members of Facebook's Audit Committee failed to meet their obligations as provided in the Audit Committee Charter, in addition to their duties imposed by law, because despite the numerous regulatory fines, investigations, and reports finding fundamental failings in Facebook's internal controls, they did not cause Facebook to remediate those control deficiencies. The Audit Committee's deliberate failure of oversight constituted breaches of their fiduciary duties to Facebook and has resulted in significant harm to the Company.

431. Further, the Audit Committee members were charged with assisting the Board in overseeing the integrity of Facebook's financial statements and the adequacy and reliability of disclosures to its stockholders, including the company's internal controls.

432. But Facebook's internal and disclosure controls were deficient, causing Facebook to issue materially false and misleading information regarding the company's practices. The Audit Committee was directly responsible for approving Facebook's materially false and misleading SEC filings, including the 2017 Proxy Statement and 2018 Proxy Statement.

433. The Audit Committee clearly failed in ensuring that Facebook's internal controls and procedures were sufficient to comply with applicable data protection and privacy laws.

434. In the Consent Decree, the FTC said Facebook told users that third-

party applications they installed would have access to only as much information as the applications needed to operate — but, the FTC said, the applications took far more. The FTC also alleged that personal information labeled as to be shared only with friends had been shared with third-party apps when a friend installed the applications, and accused Facebook of sharing personal information with advertisers. Yet, from 2013-2017, PwC certified that Facebook was operating an effective privacy program during that time period. "Facebook's privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information," PwC said in its assessor reports.

435. All of the Defendants failed to exercise any oversight over the insider sales transactions and failed to implement reasonable internal controls with respect to them.

COUNT I

Breach of Fiduciary Duty
(Against All Individual Defendants)

436. Plaintiff incorporates by reference and reallege each of the foregoing allegations as though fully set forth in this paragraph.

437. Each of the Individual Defendants owed and owe fiduciary duties to Facebook and its stockholders. By reason of their fiduciary relationships, the Individual Defendants specifically owed and owe Facebook the highest obligation of good faith, fair dealing, loyalty, and due care in the administration and

management of the affairs of the company, including its financial reporting, internal controls, and compensation practices.

438. Additionally, the Individual Defendants have affirmative obligations pursuant to the Consent Decree, as well as specific fiduciary duties as defined by the charters of various Board committees that, had such obligations and duties been discharged by the Individual Defendants, would have necessarily prevented the misconduct and the consequent harm to Facebook alleged in this Complaint.

439. Each of the Individual Defendants consciously and deliberately breached their fiduciary duties of candor, good faith, loyalty, and reasonable inquiry to Facebook and its stockholders by failing to act to ensure Facebook maintained adequate internal controls to comply with the Consent Decree and other applicable laws.

440. Each of the Individual Defendants had actual or constructive knowledge that they had caused Facebook to improperly misrepresent the nature of its advertising services, user privacy practices, and the extent of the its data sharing operations, and the Individual Defendants failed to correct Facebook's public statements. The Individual Defendants had actual knowledge of the misstatements and omissions of material facts set forth in this Complaint, or acted with reckless disregard for the truth, in that they failed to ascertain and to disclose such facts, even though such facts were available to them. Such material misrepresentations

and omissions were committed knowingly or recklessly and for the purpose and effect of increasing Facebook's revenues at the artificially inflating the price of Facebook's securities.

441. The Individual Defendants breached their fiduciary duties to Facebook by their actions and inactions, including, without limitation, by: (i) implementing and overseeing (a) Facebook's illegal business strategy of pursuing profits and revenue growth through violations of various laws and (b) conduct which was unethical, conduct that was designed to achieve an improper result, or conduct that was designed to achieve an improper purpose that was not in the Facebook's best interests; (ii) suppressing, concealing, and engaging in conduct designed to suppress, conceal, hide, or avoid detection or disclosure of information about any illegal activity or wrongdoing; (iii) omitting and failing to disclose material information or facts concerning illegal activity or wrongdoing in any public statements, or in connection with any request for information in any investigation, inquiry, or litigation by any government entity or regulator, and in discovery in any civil or criminal litigation; (iv) consciously permitting, allowing, and encouraging business practices that were unfair and violated the expectations and trust of Facebook's stockholders, users of Facebook's social networking website, smartphone users and users of mobile devices, U.S. citizens, government officials, and the public at large; (v) turning a blind eye to Facebook's illegal

activity and any persons who were employees, attorneys, and advisors or had any similar relationship with Facebook who engaged in wrongdoing or any illegal activity relating to their position, responsibilities and duties respecting the company, pursued profits or revenue growth, or who obtained any personal financial gain, at the expense of any of Facebook's users, stockholders, or any other person, or instead of complying, causing or failing to act or prevent others from failing to comply or to act to cause Facebook's compliance with applicable laws; (vi) by failing to be reasonably informed about the source of Facebook's revenues and the nature of its core advertising business; (vii) by failing to implement policies and procedures for enforcement of any Facebook policies, or failing to be reasonably informed about Facebook policies and procedures for enforcement, or any Facebook policies that violated the law or that were not enforced, or any employee actions and activities at Facebook that violated the law and company policy; (viii) failing to ensure that Facebook was in compliance with duties or obligations set forth in any agreements with U.S. and foreign governments and any regulators, or by allowing or permitting Facebook's policies and any activities or taking of any actions that failed to comply with such duties or obligations, including, without limitation, the Consent Decree entered in 2011; and (viii) failing to monitor and oversee low-level employee misconduct, either by (a) failing to implement a reasonable system of internal controls and reporting

procedures designed to detect and prevent wrongdoing; or (b) failing to adequately supervise and monitor Facebook's internal controls and reporting systems and taking no action or inadequate action upon receiving red flag warnings of deficiencies in Facebook's internal controls or of illegal activity occurring at the company.

442. The Individual Defendants, individually and in concert, engaged in the above- referenced conduct in intentional, reckless, or grossly negligent breaches of the fiduciary duties they owed to Facebook to protect its rights and interests.

443. Each of the Individual Defendants approved, signed, and willfully made and participated in issuing misleading statements, including in Facebook's public filings with the SEC, which contained omissions and misrepresentations that such Individual Defendants knew were misleading and failed to disclose material facts and information related to Facebook's core advertising business, advertising services, policies, practices, and internal controls, including relating to user privacy, information, and data security.

444. Each of the Individual Defendants deliberately concealed this information for improper purposes and failed to disclose material facts or to correct Facebook's public statements as necessary so as to not be misleading, or alternatively, failed to be reasonably informed about Facebook's business and

failed to fully inform themselves sufficiently when making, signing, and approving public statements and prior to making decisions as directors and officers, either of which is sufficient to render them personally liable to the company for breaching their fiduciary duties.

445. The Individual Defendants' actions detailed in this Complaint were not a good-faith exercise of prudent business judgment to protect and promote Facebook's corporate interests.

446. As a direct and proximate result of the Individual Defendants' breaches of their fiduciary obligations, Facebook has sustained and continues to sustain significant harm and damages.

447. As a result of the misconduct alleged in this Complaint, the Individual Defendants are liable to Facebook for its damages as referred to herein including, inter alia, the likely fine by the FTC of $3-5 billion.

448. During the relevant period, the Individual Defendants were unjustly enriched by their receipt of bonuses, stock options, stock, or similar compensation from Facebook that was tied to Facebook's financial performance, or otherwise received compensation that was unjust in light of the Defendants' bad faith conduct, violations of Facebook's Terms of Service, and self-dealing.

449. Plaintiff, as a shareholder and representative of Facebook, seeks restitution from the Individual Defendants and seeks an order of this Court

disgorging all profits, benefits, and other compensation—including any salary, options, performance-based compensation, and stock— obtained by them due to their wrongful conduct alleged in this Complaint.

450. The Individual Defendants' actions and conduct described herein were not only a breach of their fiduciary duties, but also constitute violations of law for which they are personally liable, separately and apart from their liability for breaches of fiduciary duties owed to Facebook.

COUNT II

Contribution and Indemnification (Against All Defendants)

451. Plaintiff incorporates by reference and realleges each of the foregoing allegations as though fully set forth in this paragraph.

452. This claim is brought derivatively on behalf of Facebook against the Individual Defendants for contribution and indemnification.

453. Facebook is named as a defendant in shareholder class actions filed beginning on or about March 20, 2018, asserting claims under the federal securities laws for, *inter alia*, false and misleading statements related to the Facebook's user privacy practices. In the event Facebook is found liable for violating the federal securities laws, the Company's liability will arise, in whole or in part, from the intentional, knowing, or reckless acts or omissions of some or all of the Individual Defendants as alleged herein. Facebook is entitled to receive contribution from the

Individual Defendants in connection with the securities fraud class action against the Company.

454. Facebook is also named as a defendant in other putative class actions filed on behalf of certain Facebook users, asserting claims under various states' laws for, *inter alia*, violations of privacy. In the event Facebook is found liable for violating those laws, Facebook's liability will arise, in whole or in part, from the intentional, knowing, or reckless acts or omissions of some or all of the Individual Defendants as alleged herein. Facebook is entitled to receive contribution from the Individual Defendants in connection with the class actions commenced against the Company.

455. Accordingly, Facebook is entitled to all appropriate contribution or indemnification from the Individual Defendants.

COUNT III

Misappropriation of Information and Breach of Fiduciary Duty for Insider Sales (Against Defendants Zuckerberg, Sandberg and Koum)

456. Plaintiff incorporates by reference and realleges each of the foregoing allegations as though fully set forth in this paragraph.

457. At the time of the stock sales set forth above, Zuckerberg, Sandberg and Koum knew or recklessly disregarded the information described in this Complaint regarding the breach and illicit data sharing and sold Facebook common

stock on the basis of that information.

458. The information described above was non-public information concerning Facebook's unlawful conduct associated with its business strategy to generate revenues through targeted advertising. The information was a proprietary asset belonging to Facebook which defendants Zuckerberg, Sandberg and Koum used for their own benefit when they sold Facebook common stock.

459. The sales of defendants Zuckerberg, Sandberg and Koum's shares of Facebook common stock while in possession and control of this material adverse non-public information was a breach of their fiduciary duties of loyalty and good faith.

460. Because the use of Facebook's proprietary information for their own gain constitutes a breach of the fiduciary duties owed by defendants Zuckerberg, Sandberg and Koum to the Company, Facebook is entitled to the imposition of a constructive trust on any profits they obtained thereby.

COUNT IV

Breach of Duty of Candor
(Against the Individual Defendants)

461. Plaintiff incorporates by reference and realleges each of the foregoing allegations as though fully set forth in this paragraph,

462. The Individual Defendants negligently issued, caused to be issued, and participated in the issuance of materially misleading written statements to

stockholders that were contained in the Proxy Statements and in the supplements thereto.

463. The Proxy Statements contained proposals to Facebook's stockholders urging them to (i) re-elect the members of the Board, (ii) approve executive compensation, (iii) approve director compensation, (iv) approve adoption of an amended and restated certificate of incorporation, and (v) vote against various stockholder proposals for Facebook's Board, including proposals: (a) to initiate and adopt a recapitalization plan and to take necessary steps to change voting requirements, including in Facebook's charter and bylaws; (b) for the Board to issue a report discussing the merits of establishing a Risk Oversight Board Committee; (c) for Facebook to appoint an independent Chair of the Board; and (d) for Facebook to issue a report to shareholders regarding the efficacy of Facebook's enforcement of its terms of service relating to content policies and assessing content-related risks. The Proxy Statements recommended a vote against each of the stockholder proposals, but misstated or failed to disclose any facts whatsoever (i) regarding the Cambridge Analytica scandal, including the fact that the Individual Defendants learned of the circumstances thereof and related issues in 2015 and believed that Facebook would face significant reputational harm if the truth were revealed; (ii) that Facebook's policies allowed certain third parties to access Facebook information, including user data and that of their friends, despite

representations that the company's policies prohibited such practices; (iii) that Facebook obtained information about Facebook users and non-users from other sources besides Facebook's website; (iv) that Facebook had failed to enforce its platform policies or correct deficiencies in its internal controls that were known to the Board when the Proxy Statements were filed, including its inability to track user data once it left Facebook's servers; and (v) that Facebook's corporate governance structure was materially deficient. Thus, the soliciting materials for the Proxy Statements were materially false and misleading. By reasons of the conduct alleged in this Complaint, the Individual Defendants breached their duty of candor owed to Facebook and its stockholders. As a direct and proximate result of the Individual Defendants' wrongful conduct, they misled or deceived Facebook stockholders by making misleading statements that were an essential link in stockholders heeding Facebook's recommendation to re-elect the directors who are members of the current Board, vote in favor of the Board's proposals, and vote against stockholder proposals identified above.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs request that the Court award a judgment as follows:

A. Determination that this action is a proper derivative action maintainable under the law;

B. Declaring that the Individual Defendants have breached their fiduciary duties to Facebook;

C. Determining and awarding to Facebook the damages sustained by it as a result of the violations set forth above from each Individual Defendant, jointly and severally, together with prejudgment and post-judgment interest thereon;

D. Directing Facebook to take all necessary actions to reform and improve its corporate governance and internal procedures to comply with applicable laws and to protect the Company and its stockholders from a repeat of the damaging events described in this Complaint, including putting forward for a stockholder vote resolutions for amendments to Facebook's by-laws or articles of incorporation, and taking such other actions as may be necessary to place before stockholders for a vote the following corporate governance policies:

i. a proposal to strengthen Board oversight and supervision of Facebook's data security practices;

ii. a proposal to strengthen Facebook's disclosure controls to ensure material information is adequately and timely disclosed to the SEC and the public; and

iii. a proposal to strengthen the Board's supervision of

operations and develop and implement procedures for greater stockholder input into the policies and guidelines of the Board;

E. Extraordinary equitable or injunctive relief as permitted by law or equity, including attaching, impounding, imposing a constructive trust on, or otherwise restricting the Individual Defendants' assets so as to assure that Plaintiff, on behalf of Facebook, has an effective remedy;

F. Awarding to Facebook restitution from the Individual Defendants, and each of them, and ordering disgorgement of all profits, benefits, and other compensation obtained by the Individual Defendants, including the proceeds of insider transactions made in violation of state securities laws;

G. Declaring that the 2017 Proxy Statement and the 2018 Proxy Statement contained materially false and misleading statements;

H. Awarding to Plaintiff costs and disbursements related to this action, including reasonable attorneys' fees, consultant and expert fees, costs, and expenses; and

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

CIARDI CIARDI & ASTIN

/s/ Daniel K. Astin
Daniel K. Astin (#4068)
Joseph J. McMahon, Jr. (#4819)
1204 N. King Street
Wilmington, Delaware 19801
(302) 658-1100

Attorneys for Plaintiff Robert A. Feuer

Dated: May 1, 2019

OF COUNSEL:

CIARDI, CIARDI & ASTIN
Albert A. Ciardi III
Walter W. Gouldsbury III
One Commerce Square
2005 Market Street, Suite 3500
Philadelphia, PA 19103
(215) 557-3550

GREENFIELD & GOODMAN LLC
Richard D. Greenfield
250 Hudson Street, 8th Floor
New York, NY 10013
(917) 495-4446