

No. 23-980

In the Supreme Court of the United States

FACEBOOK, INC., ET AL., PETITIONERS

v.

AMALGAMATED BANK, ET AL.

*ON WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT*

**JOINT APPENDIX
VOLUME 1 (PAGES 1-409)**

KANNON K. SHANMUGAM
*Paul, Weiss, Rifkind,
Wharton & Garrison LLP
2001 K Street, N.W.
Washington, DC 20006
(202) 223-7300
kshanmugam@paulweiss.com
Counsel of Record
for Petitioners*

KEVIN K. RUSSELL
*Goldstein, Russell
& Woofter LLP
1701 Pennsylvania Avenue,
N.W., Suite 200
Washington, DC 20006
(202) 240-8433
krussell@goldsteinrussell.com
Counsel of Record
for Respondent*

PETITION FOR A WRIT OF CERTIORARI FILED: MARCH 4, 2024
CERTIORARI GRANTED: JUNE 10, 2024

TABLE OF CONTENTS

VOLUME 1

	Page
Third amended complaint, October 16, 2020 (D. Ct. Dkt. 142)	1

VOLUME 2

Facebook, Inc. Form 10-K for fiscal year 2016, February 2, 2017 (D. Ct. Dkt. 133-1)	410
Order granting motion to dismiss complaint, September 25, 2019 (D. Ct. Dkt. 118)	550
Harry Davies, <i>Ted Cruz Using Firm that Harvested Data on Millions of Unwitting Facebook Users</i> , Guardian, December 11, 2015 (D. Ct. Dkt. 146-9)	616
Emma Roller, <i>Is It Ted Cruz's Party —Or Marco Rubio's?</i> , N.Y. Times, December 15, 2015 (D. Ct. Dkt. 146-10)	625
Paul Grewal, Facebook Newsroom, <i>Suspending Cambridge Analytica and SCL Group from Facebook</i> , March 16, 2018 (D. Ct. Dkt. 130-12)	631
Carole Cadwalladr & Emma Graham-Harison, <i>Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach</i> , Guardian, March 17, 2018 (D. Ct. Dkt. 146-21)	634
Complaint, <i>SEC v. Facebook, Inc.</i> , Civ. No. 19-4241 (N.D. Cal. July 24, 2019) (D. Ct. Dkt. 125-16)	642
Consent to entry of final judgment, <i>SEC v. Facebook, Inc.</i> , Civ. No. 19-4241 (N.D. Cal. July 24, 2019) (D. Ct. Dkt. 126-17)	661

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION**

In re FACEBOOK, INC. SECURITIES LITIGATION	Master File No. 5:18-cv-01725-EJD <u>CLASS ACTION</u>
This Document Relates To: ALL ACTIONS.	THIRD AMENDED CONSOLIDATED CLASS ACTION COMPLAINT FOR VIOLATIONS OF THE FEDERAL SECURITIES LAWS DEMAND FOR JURY TRIAL

* * *

Plaintiff Amalgamated Bank, as Trustee for the Long View LargeCap 1000 Growth Index Fund, LongView Quantitative LargeCap Fund, and LongView Quant LargeCap Equity VEBA Fund (“Amalgamated”), and Public Employees’ Retirement System of Mississippi (“Mississippi,” and, together with Amalgamated, “Lead Plaintiffs”), by and through their respective undersigned attorneys, on behalf of themselves and the Class (as defined below) of investors in the publicly-traded common stock of Facebook, Inc. (“Facebook” or the “Company”), allege the following in support of their claims for violation of the Securities Exchange Act of 1934 (“1934 Act”) and

Rule 10b-5 promulgated thereunder against Facebook and certain of its officers and directors.¹

I. Introduction

1. This securities class action arises from defendants' materially false and misleading statements and omissions concerning Facebook's privacy and data protection practices and the impact of defendants' misconduct on Facebook's business and financial condition. It is brought on behalf of all persons who purchased Facebook common stock between February 3, 2017 and July 25, 2018, inclusive (the "Class Period"), against Facebook and three of its officers and/or directors: Chief Executive Officer ("CEO") Mark Zuckerberg ("Zuckerberg"), Chief Operating Officer ("COO") Sheryl K. Sandberg ("Sandberg") and Chief Financial Officer ("CFO") David M. Wehner ("Wehner") (collectively, "defendants"). When the full truth concerning defendants' misrepresentations was revealed, including misconduct that Zuckerberg has admitted was a "major breach of trust," Facebook's stock price

¹ This Third Amended Complaint is filed pursuant to the Court's September 16, 2020 Order (ECF No. 141). In amending their complaint, Lead Plaintiffs reserve all rights and allegations under their prior complaint. Nothing herein is intended to waive, in whole or in part, any previously asserted claims, arguments or allegations. Except as to allegations concerning themselves and their transactions in Facebook stock, Lead Plaintiffs' allegations are based on an investigation conducted by Lead Counsel, including: (i) review of the Company's filings with the SEC and other government agencies; (ii) information on the Company's website and in media and analyst reports and other public statements; and (iii) information from other sources believed to be reliable, as described herein. Lead Plaintiffs believe that substantial additional evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery.

declined precipitously, causing the loss of billions of dollars in shareholder value.²

2. Facebook derives virtually all of its revenue from monetizing the personal information—data—that it collects from the users of its social media platforms. It does so through the sale of “targeted advertising” that is based on Facebook users’ personal information, including their online activities, the pages they visit, the posts they “liked,” and the people they “friended.” While Facebook users generally understood that the Company was using their personal data in order to tailor the ads that they would see, they trusted Facebook to keep that personal data private, not to share it directly with third parties, without informed consent, and to act in accordance with defendants’ public statements regarding Facebook’s protection of user privacy and user control over data. Defendants frequently acknowledged that maintaining Facebook’s users’ trust was critical to the Company’s continued growth and financial success.

3. Unbeknownst to users—and investors—their trust in Facebook was misplaced. In contrast to defendants’ public statements, Facebook was deliberately sharing user data with hundreds of third parties, including third-party app developers and multi-national corporations such as Apple, Amazon, Blackberry, Microsoft and Samsung, who had been “whitelisted” for access to users’ data. The entities Facebook whitelisted also included known or suspected national security threats, such as Huawei (a Chinese technology company with deep ties to China’s government) and Mail.Ru Group (a Kremlin-connected technology conglomerate), as well as known pri-

² F8 2018 Developer Conference Tr. at 9 (May 1, 2018).

vacy threats, such as apps created by Global Science Research (“GSR”). The facts show that Cambridge Analytica Ltd. (“Cambridge Analytica”) was also whitelisted for continued access to users’ friend data even after defendants publicly represented this access had been shut down. As another court has already found, Facebook did not “come close to disclosing [this] massive information-sharing program,” and users did not consent to this use of their data. *In re Facebook, Inc. Consumer Privacy User Profile Litig.*, 2019 WL 4261048, at *14 (N.D. Cal. Sept. 9, 2019) (the “Consumer Case”).

4. During the Class Period, defendants knew or willfully blinded themselves to the fact that sensitive user information for approximately 87 million Facebook users had been provided to a third-party political consulting firm called Cambridge Analytica, and remained at risk of being used and abused. Indeed, the data was misused by Cambridge Analytica to build psychological profiles of Facebook users that became the basis for political advertising designed to trigger some of the worst characteristics in people, such as paranoia and racial bias.

5. On December 11, 2015, *The Guardian* reported that Cambridge Analytica may have obtained Facebook user data for use in political campaigns.³ Defendants responded to the article with feigned surprise and assured users, investors, regulators and the public that they would “require” any compromised data to be deleted, that violators would be punished, and that Facebook would swiftly halt any misuse of its users’ data. For example, a Company spokesman told *The Guardian*: “[W]e will take swift

³ Harry Davies, *Ted Cruz using firm that harvested data on millions of unwitting Facebook users*, *Guardian* (Dec. 11, 2015) (“Dec. 2015 *Guardian* article”).

action against companies that [violate Facebook’s privacy policies], including banning those companies from Facebook and requiring them to destroy all improperly collected data.” Facebook would use variations of this statement over and over thereafter, including during the Class Period, whenever questions were raised about users’ control over their data or Facebook’s ability to protect its users’ data.

6. Behind the scenes, however, Facebook’s primary concern was minimizing the public relations fallout from the scandal. Facebook did not publicly confirm that Cambridge Analytica had obtained user data (to the contrary, as discussed below, during the Class Period Facebook was still pointing to statements on Cambridge Analytica’s website stating that Cambridge Analytica did *not* use Facebook data).⁴ Nor did defendants reveal that just before *The Guardian* story broke, Facebook had hired the co-founder of GSR, the company that had funneled the user data to Cambridge Analytica, and put him to work at Facebook’s Menlo Park headquarters, where he remained employed throughout the Class Period.

7. In the wake of *The Guardian* article, Facebook exchanged a few emails with Cambridge Analytica during the December 2015-January 2016 time period about purloined data, which Facebook would later call a “confirmation” or “certification” of deletion. Yet, on June 11, 2016, Facebook learned from GSR that Cambridge Analytica’s January 2016 “certification” was a fraud and quickly moved to cover up the fact that Cambridge Analytica was still in possession of the data.

8. Facebook did not notify the public or government regulators of the lost data, or alert the users whose data

⁴ All emphasis added throughout unless otherwise noted.

had been compromised. In addition, because the data provided to Cambridge Analytica was in a format that was easily shared with others, defendants knew that the representations of GSR and Cambridge Analytica, even if reliable (and they were not), were insufficient to assure that the user data was not still at risk of being misused. Zuckerberg later acknowledged his responsibility for these failures, admitting “we didn’t do enough,” which was a “huge mistake [and] [i]t was my mistake.”⁵

9. Since this action was commenced, additional facts have been revealed demonstrating that defendants could not reasonably rely upon the bare assertions of GSR and Cambridge Analytica. Newly uncovered documents show that as early as September 2015, Facebook personnel were referring to Cambridge Analytica as “sketchy (to say the least),” and that in 2015 Facebook determined that both GSR and Cambridge Analytica had violated Facebook’s terms of use. It has also been revealed that Facebook learned that both GSR and Cambridge Analytica had repeatedly lied to Facebook regarding the scope and type of user data they possessed. And internally, Facebook ignored multiple red flags revealing that the Cambridge Analytica data was still being used by Cambridge Analytica itself to develop political advertisements that it placed on Facebook, leaving no doubt that the data had not been deleted and the certifications to the contrary were incorrect. Yet, by summer 2016, Facebook was set to make \$75-\$85 million in advertising revenue from Cambridge Analytica, which was Donald Trump’s (“Trump”) campaign ad buyer on Facebook at the time. Far from requiring any (non-fraudulent) “certifications” of deletion

⁵ Toby Shapshak, ‘It Was My Mistake’ Zuckerberg Admits, While Facebook ‘Didn’t Do Enough To Prevent Abuse,’ *Forbes* (Apr. 4, 2018).

during this time, Facebook “embedded” its own employees to work, literally, inside the Cambridge Analytica data center that was running the Trump campaign’s digital operations in San Antonio, Texas. And Facebook even gave Cambridge Analytica a promotion—from being a “sketchy” company (as of December 2015) to being a “Preferred Marketing Developer” (as of summer 2016). Such are the privileges conferred upon companies pursuant to Zuckerberg’s and Sandberg’s selective policy enforcement model—a type of coin-operated policy enforcement model that slows to inoperable speeds so long as the policy violator keeps making deposits above \$250,000. Cambridge Analytica’s \$75-\$85 million in ad buys exceeded that threshold by several orders of magnitude.

10. Knowing Cambridge Analytica continued to violate Facebook’s (publicly stated) privacy policies while working to support the 2016 Trump campaign, and knowing that Cambridge Analytica had given Facebook a fraudulent deletion “certification” *so that* it could continue violating Facebook’s (publicly stated) privacy policies, Facebook repeatedly went on the record to assure users and investors that Facebook’s 17-month-long investigation into Cambridge Analytica had not uncovered a scintilla of wrongdoing:

- Facebook went on the record, on March 4, 2017, to publish false results of its Cambridge Analytica investigation, in statements to *The Guardian*, which reported: “A Facebook spokesperson said: ‘Our investigation to date has **not uncovered anything that suggests** wrongdoing with respect to Cambridge Analytica’s work on the Leave and Trump campaigns.’”

- Facebook went on the record, on March 5, 2017, to repeat the same false results of its Cambridge Analytica investigation, in statements to *The Daily Mail*, which reported this quote from a Facebook spokesperson: ““Our investigation to date has **not uncovered anything that suggests** wrongdoing with respect to Cambridge Analytica’s work on the Leave and Trump campaigns.””
- Facebook went on the record, on March 30, 2017, with *The Intercept*: ““Our investigation to date has **not uncovered anything that suggests** wrongdoing,’ a Facebook spokesperson told *The Intercept*,” in a report that concerned the Trump campaign and some related subjects.

These statements were all false—as Facebook’s “spokesperson” knew, having specifically referenced Facebook’s “investigation,” which uncovered far more than mere “suggestions” of wrongdoing by Cambridge Analytica.” *See* §VI.D.-K.

11. In addition, there is no dispute that by December 2015 defendants knew that significant amounts of sensitive user data had been transferred to third parties in violation of its stated policies. Defendants also knew that this created huge—and undisclosed—risks for the Company. Facebook’s ability to generate revenue depended on users’ willingness to post—and share—data on which ads were based. If user engagement declined, or if users became less willing to share their data, Facebook’s ability to generate revenue would diminish. And the number one thing that could cause users to disengage or refuse to share their data was a lack of trust that the Company was

protecting their information. Zuckerberg himself has admitted that “the No. 1 thing that people care about is privacy and the handling of their data.”⁶

12. Despite their knowledge of these risks, defendants decided to conceal and deny them in public statements, including in documents filed with the United States Securities and Exchange Commission (“SEC”) during the Class Period. In their periodic SEC filings, defendants set forth a number of “risk factors,” including the risk of harm to Facebook’s business if third parties obtained user data. Facebook, however, described these risks as merely hypothetical, stating that “*if* developers fail to adopt or adhere to adequate data security practices . . . our users’ data *may be* improperly accessed” and “*if*” that happened there “*could*” be harm to Facebook’s business. In reality, defendants knew that these risks were not hypothetical because they knew that multiple third parties—Cambridge Analytica and others—had *in fact* improperly gained access to user data and used it in ways not consented to or authorized by those users. *See* §IV.C.-E. And Cambridge Analytica kept misusing the data throughout the 2016 political season, after it gave Facebook a fraudulent “certification” or “confirmation” of deletion—a fraud that Facebook discovered no later than June 11, 2016.

13. Defendants reinforced their false and misleading risk disclosures through other misrepresentations during the Class Period. In February and March 2017, defendants responded to press inquiries regarding the status of

⁶ Kara Swisher and Kurt Wagner, *Here’s the transcript of Recode’s interview with Facebook CEO Mark Zuckerberg about the Cambridge Analytica controversy and more*, Recode (Mar. 22, 2018).

their “investigation” into Cambridge Analytica by: (i) referring reporters to Cambridge Analytica’s website statement that it supposedly “does not use data from Facebook”; and (ii) telling reporters that Facebook’s “investigation to date [into Cambridge] had not uncovered anything that suggests wrongdoing.” These statements were false. As Zuckerberg later admitted, Facebook had known since 2015 that Cambridge Analytica used data from Facebook and had done so in violation of Facebook’s policies, and Cambridge Analytica kept misusing the data throughout the 2016 political season, as noted. *See* §IV.C.-K.

14. On July 24, 2019, following an investigation that lasted more than a year, the SEC announced a \$100 million settlement with Facebook over charges that the Company had made materially false and misleading risk disclosures in its filings with the SEC, including from the start of the Class Period until at least March 2018.⁷ *See* Complaint, *SEC v. Facebook, Inc.*, 3:19-cv-04241-JD (N.D. Cal. July 24, 2019) (ECF No. 1) (the “SEC Complaint”). The SEC concluded that: “Facebook knew, or should have known, that its Risk Factor disclosures in its annual reports . . . and in its quarterly reports . . . were materially misleading.”⁸ These materially false statements acted as a “fraud or deceit upon purchasers” of Facebook stock during the Class Period.⁹

⁷ Press Release, *Facebook to Pay \$100 Million for Misleading Investors About the Risks It Faced From Misuse of User Data*, Securities & Exchange Commission (July 24, 2019).

⁸ *See* SEC Complaint at ¶44; *see also id.* at ¶¶47-49 (Facebook made misleading statements to the press in February and March 2017).

⁹ *Id.* at ¶53.

15. Defendants also made representations regarding the privacy and security of user data on Facebook during the Class Period. For example, defendants assured the public that Facebook users had control of their data and Facebook was not sharing sensitive user data with third parties. *See, e.g.*, §IV.L.1. (Sandberg: “***you are controlling who you share with***”; Zuckerberg: when you share on Facebook “***you have complete control*** over who sees it and how you share it”); *see also* §VI.A. These statements were materially false and misleading. In reality, users had no control over their data because behind the scenes Facebook was engaged in a “massive information-sharing program” that was deliberately concealed from users and investors, who did not begin to learn the truth until March 2018. *Facebook*, 2019 WL 4261048, at *14 (Consumer Case).

16. Remarkably, Facebook engaged in these activities for years (including throughout the Class Period) even though Zuckerberg had assured users on April 30, 2014 that Facebook would stop allowing third parties to collect data about users’ friends, which Facebook stated in a press release was “a really important step for giving people power and control over how they share their data with apps” and gave people “more control over their data.”¹⁰ In contrast to Zuckerberg’s promises, the data of more than 87 million people that was ultimately transferred to Cambridge Analytica was collected ***after*** Zuckerberg and Facebook assured users that third parties such as GSR would no longer be able to obtain users’ friends’ data. *See* §IV.B.-E.

¹⁰ Complaint for Civil Penalties, Injunction, and Other Relief, *United States of America v. Facebook*, No. 19-cv-2184 (D.D.C. July 24, 2019) (ECF No. 1) (the “FTC Complaint”) at ¶98.

17. Indeed, it has now become clear that defendants’ “important” public announcement in April 2014 was an utter sham. Defendants exempted a wide array of “white-listed” app developers and corporate giants such as Google, Amazon, Samsung, Blackberry, Huawei (a Chinese technology company with deep ties to China’s government) and Mail.Ru Group (a Kremlin-connected technology conglomerate) from this prohibition on third-party access to user friend data. Defendants allowed these entities and hundreds more to override user privacy settings in order to get this data in secret. Recently obtained Facebook documents confirm the obvious: this widespread practice was conceived of, and approved by, Zuckerberg and Sandberg as part of Facebook’s “reciprocity” initiative—where Facebook secretly gave third parties access to its trove of user data in exchange for advertising revenues and other valuable business benefits. *See* §IV.C.

18. On July 24, 2019, the Federal Trade Commission (“FTC”) announced a “record-breaking **\$5 billion** penalty” against Facebook.¹¹ The FTC determined that from prior to the Class Period until at least June 2018, Facebook had violated the 2012 FTC Consent Decree by “**deceiving users about their ability to control the privacy of their information.**” The \$5 billion FTC penalty against Facebook is unprecedented and historic: it is 18 times greater than the largest ever previously imposed on any company for violating consumers’ privacy, and as the FTC noted it is “one of the largest penalties ever assessed by the U.S. government for any violation.”¹² *See* §V.A.2.

¹¹ Press Release, *FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, Federal Trade Commission (July 24, 2019).

¹² *Id.*

19. In addition to false statements regarding Cambridge Analytica, the risks facing the Company, and the ability of users to control their data, defendants made numerous other false and misleading statements and omissions during the Class Period, including misrepresentations and omissions concerning: (i) the Company's efforts to investigate and contain the data exposed to Cambridge Analytica (*e.g.*, §V.E.); (ii) Facebook's response to other incidents where data had been exposed to third parties or used in violation of user's privacy settings (§§VI.E., H., J., M.); (iii) Facebook's compliance with regulatory requirements governing user privacy, including the 2012 FTC Consent Decree (§§VI.G., I.); and (iv) the impact of Facebook's privacy violations on its business (§§VI.K.-L.).

20. At the same time as defendants were making false statements and concealing material risks from the market they were selling billions of dollars' worth of Facebook shares. During the Class Period, Zuckerberg sold approximately 30,000 Facebook shares for proceeds of more **\$5.2 billion**, while Sandberg sold \$389 million worth of Facebook stock and Wehner \$21 million. These sales exceeded defendants' pre-Class Period sales, and included particularly large sales during the first quarter of 2018—before Facebook's failure to address the Cambridge Analytica breach became public, as did reports of numerous other false statements by the Company regarding privacy, security and user control over data.

21. On March 17, 2018, *The Guardian* reported that Facebook had delayed taking action to address the Cambridge Analytica data breach, and that Facebook user

data was potentially still in the hands of Cambridge Analytica and other third parties.¹³ In an article published the same day, *The New York Times* reported that Facebook’s failure to comply with its privacy policies was “one of the largest data leaks in the social network’s history.”¹⁴

22. These disclosures sent shockwaves through the market and caused the price of Facebook’s common stock to drop nearly 7% on Monday, March 19, 2018, the first trading day after the news broke. In the days that followed, the U.S. Congress and British Parliament called for inquiries, multiple former Facebook insiders came forward with accounts of repeated warnings that had been given and ignored by Zuckerberg and other members of management, and calls for users to disengage from the platform—#DeleteFacebook—took off.

23. By March 27, 2018, Facebook’s stock was trading as low as \$152/share, a drop of nearly 18% in value from its price just before news of the Cambridge Analytica scandal broke, reflecting a loss of more than \$100 billion in market capitalization. A March 2018 report by one of the world’s leading corporate governance and proxy advisors, Institutional Shareholder Services (“ISS”), stated that Facebook’s “failure to protect its users’ privacy has

¹³ Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, *Guardian* (Mar. 17, 2018); Carole Cadwalladr (@carolecadwalla), TWITTER (Mar. 22, 2018).

¹⁴ Matthew Rosenberg, Nicholas Confessore & Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, *N.Y. Times* (Mar. 17, 2018).

eroded the level of trust among users, calling into question the company’s business model and its governance.”¹⁵

24. Meanwhile, defendants embarked on an orchestrated apology tour, repeatedly admitting their failure to protect user privacy or live up to their prior assurances. These were not mere expressions of regret. On the contrary, Zuckerberg himself signed full page advertisements in several U.S. and U.K. newspapers conceding that Facebook’s response to the Cambridge Analytica data breach was a “**breach of trust**,” and apologizing that “we didn’t do more at the time.”¹⁶ In other public statements, Zuckerberg took “responsibility” for this breach of trust and told reporters that Facebook’s actions in response to the Cambridge Analytica scandal were “clearly a mistake . . . I’m not trying to say it was the right thing to do.”¹⁷

25. Despite their public admissions of fault, defendants rushed to assure investors that the disclosures had only minor impacts on user engagement and would not have a material effect on the Company’s financial performance. For example, Zuckerberg testified to Congress in April 2018 that Facebook had seen no dramatic declines in the number of Facebook users and no decrease in user interaction on Facebook whatsoever, and when Facebook reported its results for the first quarter on 2018 on April 25, 2018, defendants said that user activity had increased,

¹⁵ Oshni Arachchi, *Trouble in Tech: A Crisis of Trust in Social Media*, ISS-Ethix (Mar. 28 2018) at 3.

¹⁶ Sheena McKenzie, *Facebook’s Mark Zuckerberg says sorry in full-page newspaper ads*, CNN (Mar. 25, 2018).

¹⁷ Kara Swisher and Kurt Wagner, *Here’s the transcript of Recode’s interview with Facebook CEO Mark Zuckerberg about the Cambridge Analytica controversy and more*, Recode (Mar. 22, 2018).

advertising effects were *de minimis*, and any incremental spending occasioned by changes the Company made to address Cambridge Analytica matters were already reflected in the quarterly results.¹⁸ *See also* §VI.L. (discussing additional false statements).

26. Buoyed by the favorable earnings report for the first quarter of 2018 and the purported lack of financial impact resulting from the Cambridge Analytica scandal, Facebook's stock price immediately climbed by more than 9% following the earnings report. Facebook's stock price continued to climb thereafter. By July, Facebook's stock price was trading well above \$200 per share.

27. On July 25, 2018, the Company reported its earnings results for the second quarter of 2018, stunning investors when Facebook finally revealed that its privacy misconduct had in fact hit the Company's bottom line and seriously impacted its business. Defendants reported a significant decline in users in Europe, zero user growth in the United States, decelerating worldwide growth of active users (*i.e.*, those most responsible for generating data used in targeted advertising), lower than expected revenues and earnings, ballooning expenses affecting profitability, and reduced guidance going forward. All of this was a direct result of the disclosures concerning Facebook's true privacy practices. Indeed, Zuckerberg opened the July 25, 2018 investor conference call by discussing "the investments we've made over the last six months to improve safety, security and privacy across our services," which had "significantly impact[ed] our profitability."¹⁹

¹⁸ Q1 2018 Facebook, Inc. Earnings Call Tr. at 15 (Apr. 25, 2018).

¹⁹ Q2 2018 Facebook, Inc. Earnings Call Tr. at 3 (July 25, 2018).

28. Market reaction to the Company's earnings report for the second quarter of 2018 and conference call was swift and severe, causing the price of Facebook's common stock to drop by nearly 19% on July 26, 2018, for a staggering single-day loss of approximately \$100 billion in market capitalization. This was the ***largest such one-day drop in U.S. history***. By July 27, 2018, Facebook stock had fallen by 21%, shedding approximately \$112 billion in market capitalization. This action seeks to recover for the enormous damages suffered by Facebook investors.

II. Parties

A. Plaintiffs

29. Amalgamated is an investment bank with over \$4 billion in assets that serves thousands of labor unions, nonprofits, social impact enterprises, political organizations, foundations and individuals. Amalgamated has been offering investment management services since 1973, and has over \$40 billion in assets under management and custody. Amalgamated is the trustee for the LongView LargeCap 1000 Growth Index Fund, the LongView Quantitative LargeCap Fund and the LongView Quant LargeCap Equity VEBA Fund, each of which purchased Facebook common stock during the Class Period and were damaged thereby, as set forth in the certification attached hereto as Ex. A and incorporated herein by reference.

30. Mississippi (or "PERS") is a public retirement system that serves the state of Mississippi. Founded in 1952, PERS provides retirement benefits for individuals working in Mississippi's state government, public schools, universities, community colleges, municipalities, counties, legislature, highway patrol, and other public entities. It currently has over 300,000 members, including over

100,000 retiree and beneficiary members, and approximately \$26.5 billion in assets under management. Mississippi purchased Facebook common stock during the Class Period and was damaged thereby, as set forth in the previously-filed certification and the schedule attached hereto as Ex. B, which are each incorporated herein by reference.

31. Ernestine Bennett, Fan Yuan, Fern Helms and James Kacouris are the plaintiffs in putative class actions filed against Facebook and its officers and directors that have been consolidated into this proceeding. Like the other members of the proposed Class, each of these plaintiffs alleges in their respective complaints that they purchased Facebook common stock at the artificially-inflated prices prevailing in the market during the Class Period and were damaged thereby.

B. Defendants

32. Defendant Facebook is a Delaware corporation with its principal place of business located in Menlo Park, California, where it owns and leases 3 million square feet of office buildings and 130 acres of land for future expansion. Facebook's common stock is traded under the ticker "FB" on the NASDAQ Global Select Market ("NASDAQ"), an efficient market. As of December 31, 2017, the Company had 25,105 employees. In its FY17 report on SEC Form 10-K, the Company stated: "We use our investor.fb.com and newsroom.fb.com websites as well as Mark Zuckerberg's Facebook Page (<https://www.facebook.com/zuck>) as means of disclosing

material non-public information and for complying with our disclosure requirements under Regulation FD.”²⁰

33. Defendant Zuckerberg founded Facebook in 2003 and is its CEO and Chairman of the Board. Zuckerberg controls Facebook. The Company has two classes of common stock, giving Zuckerberg the ability to control more than half of the voting power of the company. Because Zuckerberg controls a majority of the company’s voting power, Facebook is considered a “controlled company” pursuant to corporate governance rules for NASDAQ-listed companies. As a result, FB does not need to have a majority of independent directors, a compensation committee, or an independent nominating function (directors are responsible for nominating members to the company’s board). Zuckerberg personally appointed more than half of Facebook’s Board of Directors, including himself, and has the authority to make major decisions by himself.

34. As set forth herein, defendant Zuckerberg controlled the Company, had knowledge of or access to inside information concerning Facebook, including the conduct described below and had a duty to disseminate accurate information concerning Facebook and to correct any misleading statements, which he violated in making the misrepresentations and omissions alleged herein. Indeed, defendant Zuckerberg was personally involved in developing Facebook’s data security platform and, according to his own admissions, personally responsible for the data security breach and other facts, transactions and circumstances alleged herein. For example, Zuckerberg has publicly stated that he is “responsible for what happens

²⁰ As used herein, “FY” means the Company’s fiscal year, and “Q” means the Company’s fiscal quarter (*e.g.*, FY17 means fiscal year 2017, and 1Q17 means the first fiscal quarter of 2017).

on our platform”²¹ and testified that “I started Facebook, I run it, and I’m responsible for what happens here.”²² Zuckerberg also specifically admitted responsibility and apologized for the Cambridge Analytica data breach, testifying that the situation “was a big mistake. And it was my mistake. And I’m sorry.”²³ During the Class Period, Zuckerberg sold 29,680,150 shares, netting gross proceeds of \$5,330,078,471.

35. Defendant Sandberg is, and at all relevant times was, COO of Facebook. Since she was appointed COO in March 2008, Sandberg has run the Company’s business operations and is Zuckerberg’s “right hand” in running the Company. Sandberg has served on Facebook’s Board of Directors since June 2012. As set forth herein, Sandberg controlled the Company, had knowledge of or access to inside information concerning Facebook, including the conduct described below and had a duty to disseminate accurate information concerning Facebook and to correct any misleading statements, which she violated in making the misrepresentations and omissions alleged herein. Indeed, Sandberg has asserted that she is responsible for “controls on the Company” relating to data security and she holds herself “responsible for the [controls] we didn’t have.”²⁴ “[W]e run the company,” Sandberg has said.²⁵

²¹ Kif Leswing, *Mark Zuckerberg and Sheryl Sandberg respond to Cambridge Analytica scandal*, Business Insider (Mar. 21, 2018).

²² Committee Hearing Transcript, Senate Commerce, Sci. and Transp. Comm. and Senate Judiciary Comm. Joint Hearing on Facebook (“Committee Hearing Transcript”) (Apr. 10, 2018) at 6.

²³ *Id.*

²⁴ *Full video and transcript: Facebook COO Sheryl Sandberg and CTO Mike Schroepfer at Code 2018*, Recode (May 30, 2018).

²⁵ *Id.*

During the Class Period, Sandberg sold 2,589,000 shares, netting gross proceeds of \$389,943,538.

36. Defendant Wehner is, and at all relevant times was, CFO of Facebook. Since he was appointed CFO in June 2014, Wehner has run the finance, facilities and information technology functions at Facebook. From November 2012 to June 2014, Wehner served as Facebook's Vice President, Corporate Finance and Business Planning. As set forth herein, Wehner controlled the Company, had knowledge of or access to inside information concerning Facebook, including the conduct described below and had a duty to disseminate accurate information concerning Facebook and to correct any misleading statements, which he violated in making the misrepresentations and omissions alleged herein. During the Class Period, Wehner sold 130,201 shares, netting gross proceeds of \$21,417,346.

37. Defendants Zuckerberg, Sandberg and Wehner are collectively referred to herein as the "Executive Defendants." The Executive Defendants made, or caused to be made, false statements that caused the price of Facebook common stock to be artificially inflated during the Class Period.

III. JURISDICTION AND VENUE

38. The claims asserted herein arise under and pursuant to §§10(b), 20(a) and 20A of the 1934 Act, 15 U.S.C. §§78j(b), 78t(a) and 78t-1, and Rule 10b-5, 17 C.F.R. §240.10b-5, promulgated thereunder by the SEC.

39. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. §1331 and §27 of the 1934 Act.

40. Venue is proper in this District pursuant to §27 of the 1934 Act and 28 U.S.C. §1391(b). Facebook maintains its headquarters in Menlo Park, California, and many of the acts charged herein, including the preparation and dissemination of materially false and misleading information, occurred in substantial part in this District.

41. In connection with the acts alleged in this complaint, defendants, directly or indirectly, used the means and instrumentalities of interstate commerce, including, but not limited to, the mails, interstate telephone communications and the facilities of the national securities markets.

IV. Background and Overview of Defendants' Fraud Scheme

A. Facebook's Business

42. Facebook is the world's largest social networking company. The Company offers products and platforms such as facebook.com, Instagram, Messenger, WhatsApp and Oculus, which are designed to facilitate connection and information sharing between users through mobile devices and personal computers. Facebook was founded in 2004 by its current CEO Zuckerberg, who according to Facebook's SEC filings is the Company's "chief operating decision-maker."

43. The Company operates by monitoring both users and non-users, tracking their internet activity and retaining personal data.

1. Facebook's Business Depends on Monetizing User Data

44. Facebook's main asset is the vast treasure-trove of user personal data that it has amassed since its founding.

The Company generates substantially all of its tens of billions of dollars in revenue by selling access to its users' data, including through the sale of advertisements that are "targeted" towards particular users based on the users' personal data. In FY17, Facebook reported \$40.6 billion in revenue, with \$39.9 billion or over 98%, coming from targeting advertising and marketing placement. In FY18, Facebook's revenue ballooned to \$55.8 billion, with \$55.01 billion or 98.6% generated by ads.²⁶

45. Facebook stated in its FY18 Form 10-K that it was able to generate this revenue because its "ads enable marketers to reach people based on a variety of factors including age, gender, location, interests, and behaviors." As one *Seeking Alpha* author explained in a March 19, 2018 report: "Facebook's business model relies on its high traffic, but its real "moat" is its exclusive control over a vast array of very detailed user data that allows micro-targeting advertising."²⁷

46. Facebook sells targeted advertising not only on its primary platform, but also on applications, or "apps," developed by third parties and integrated into Facebook's platform. These apps represent a significant source of revenue to Facebook. For example, game apps, like Candy Crush or Farmville, generate large revenues for Facebook based on the ads that are placed in front of users as they play the game. These apps also help attract new users to, and engage existing users on, the Facebook platform.

²⁶ As used herein, "FY" means the Company's fiscal year, and "Q" means the Company's fiscal quarter (*e.g.*, FY18 means fiscal year 2018, and 1Q18 means the first fiscal quarter of 2018).

²⁷ Erich Reimer, *The Cambridge Analytica Mishap Is Serious For Facebook*, *Seeking Alpha* (Mar. 19, 2018).

47. During and prior to the Class Period, Facebook relied heavily on the addition of apps to increase user engagement. “User engagement” or “engagement” is a key metric for Facebook. It is measured by counting user’s active reactions to content posted on Facebook—*i.e.*, whether users “Like” a Post, or click on an image or leave a comment. Facebook engages in extensive analysis of user activity and reports this information to advertisers.

48. Facebook has acknowledged that its financial performance depends on its success in attracting active users to its platform. As the Company stated in its FY17 report on Form 10-K: “The size of our user base and our users’ level of engagement are critical to our success. Our financial performance has been and will continue to be significantly determined by our success in adding, retaining, and engaging active users of our products, particularly for Facebook and Instagram.” Simply put, engaged users generate more advertising revenue for Facebook. Indeed, as Facebook explained in its FY17 annual report: “Trends in the number of users affect our revenue and financial results by influencing the number of ads we are able to show, the value of our ads to marketers, the volume of Payments transactions, as well as our expenses and capital expenditures.”

49. As discussed in more detail below, to encourage third-party app developers to develop new apps for the platform, Facebook provided them with access to user’s content and data, including information that users believed was private. According to Sandy Parakilas (“Parakilas”), a former Facebook operations manager responsible for privacy issues, “one of the main ways to get

developers interested in building apps was through offering them access to this [user] data.’”²⁸

2. Facebook’s Success Depends on User Trust, Which Defendants Cultivated by Stating Users Controlled Their Data

50. As defendants have repeatedly acknowledged, Facebook’s reputation as a trustworthy platform for sharing personal information is essential to the Company’s success.²⁹ Indeed, if unable to attract new users or keep existing ones, Facebook would fail or be significantly less profitable. To cultivate this critical user trust, defendants repeatedly assured the public that the Company respected privacy and that users sharing on Facebook had control over their personal data.

51. For example, as Sandberg stated on March 22, 2018 in a CNBC Interview, users’ belief that their personal data is protected, “goes to the core of our service” and maintaining users’ belief that their data was safe is

²⁸ Paul Lewis, *‘Utterly Horrifying’: ex-Facebook insider says covert data harvesting was routine*, Guardian (Mar. 20, 2018).

²⁹ For example, Facebook’s Form 10-K for the fiscal year ended December 31, 2017 stated: “If people do not perceive our products to be . . . trustworthy, we may not be able to attract or retain users . . .”; see also Mark Zuckerberg, *Our Commitment to the Facebook Community*, Facebook Newsroom (Nov. 29, 2011) (Zuckerberg describing how people share on Facebook because they have “complete control over who they share with at all times”); see also Kara Swisher and Kurt Wagner, *Here’s the transcript of Recode’s interview with Facebook CEO Mark Zuckerberg about the Cambridge Analytica controversy and more*, Recode (Mar. 22, 2018); *CNBC Exclusive: CNBC Transcript: Sheryl Sandberg Sits Down with CNBC’s Julia Boorstin Today*, CNBC (Mar. 22, 2018).

“the most important thing we can do for running this company.”³⁰ Zuckerberg has likewise stressed that “[t]he No. 1 thing that people care about is privacy and the handling of their data So I think *it’s a pretty big deal*.”³¹ Further, Sandberg represented in October 2017 that “[w]hen [users] share on Facebook, you need to know that no one is going to steal your data, no one is going to get your data that shouldn’t have it . . . and that you are controlling who you share with.”³²

52. Likewise, Zuckerberg has publicly touted how “[p]rotecting the privacy of the people on Facebook is of utmost importance to us.”³³ Zuckerberg has also specifically represented that Facebook users “have control over how [their] information is shared” on Facebook; “we do not share [users] personal information with people or services [they] don’t want;” and “we do not and never will sell any of [Facebook’s users] information to anyone.”³⁴ Sandberg has likewise spoken publicly about Facebook’s privacy controls, stating for example that “[p]rivacy is of the

³⁰ *CNBC Exclusive: CNBC Transcript: Sheryl Sandberg Sits Down with CNBC’s Julia Boorstin Today*, CNBC (Mar. 22, 2018).

³¹ Kara Swisher and Kurt Wagner, *Here’s the transcript of Recode’s interview with Facebook CEO Mark Zuckerberg about the Cambridge Analytica controversy and more*, Recode (Mar. 22, 2018).

³² Gideon Lichfield, *Watch Sheryl Sandberg’s technique for shielding Facebook from hard questions*, Quartz at Work (Oct. 13, 2017).

³³ Graham Ruddick, *Facebook forces Admiral to pull plan to price car insurance based on posts*, Guardian (Nov. 2, 2016).

³⁴ Mark Zuckerberg, *From Facebook, answering privacy concerns with new settings*, Wash. Post (May 24, 2010); see also Facebook Data Policy (Jan. 30, 2015); Anita Balakrishnan, Sara Salinas & Matt Hunter, *Mark Zuckerberg has been talking about privacy for 15 years—here’s almost everything he’s said*, CNBC (Mar. 21, 2018).

utmost concern and importance to Facebook and it's important to us that the people who use our service know that we are very protective of them. It is their data, they have control of it, they share it.”³⁵ As detailed below, Defendants' statements were false.

B. In 2012, Facebook Agreed to an Extraordinary 20-Year FTC Consent Decree Due to Repeated Failures to Protect User Privacy

53. In contrast to their public assurances, defendants repeatedly disregarded user privacy and data control in order to promote growth and increase profits. This approach has led to repeated regulatory violations and other problems.

54. On November 29, 2011, the FTC announced that Facebook had agreed to settle “charges that it deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public.”³⁶ These charges included the fact that Facebook had represented that third-party apps on its platforms would only have access to user data “that they needed to operate” when, in fact, “the apps

³⁵ Press Association, *Facebook's Sheryl Sandberg defends targeted ads*, *Guardian* (Apr. 22, 2014); Gideon Lichfield, *Watch Sheryl Sandberg's technique for shielding Facebook from hard questions*, *Quartz at Work* (Oct. 13, 2017).

³⁶ *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises*, Federal Trade Commission (Nov. 29, 2011). See also Jacqui Cheng, *FTC complaint says Facebook's privacy changes are deceptive*, *Ars Technica* (Dec. 21, 2009); Ryan Singel, *Facebook Privacy Changes Break the Law, Privacy Groups Tell FTC*, *Wired* (Dec. 17, 2009).

could access nearly all of users' personal data—data the apps didn't need."³⁷

55. The FTC had alleged that Facebook told its users that:³⁸

(a) they could restrict access to information by selecting a "Friends Only" setting when, in fact, that setting "did not prevent their information from being shared with third-party applications their friends used";

(b) their photos and videos would be inaccessible to others once their accounts were deactivated or deleted when, in fact, Facebook had "allowed access to the content, even after users had deactivated or deleted their accounts"; and

(c) the Company "complied with the U.S.-EU Safe Harbor Framework that governs data transfer between the U.S. and the European Union" when, in fact: "It didn't."

56. The November 2011 FTC press release about the settlement stated that Facebook had agreed "to take several steps to make sure it lives up to its promises in the future, including giving consumers clear and prominent notice *and obtaining consumers' express consent before their information is shared beyond the privacy settings they have established.*" According to the FTC, the settlement "bar[red] Facebook from making any further deceptive privacy claims, require[d] that the company get consumers' approval before it changes the way it shares

³⁷ *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises*, Federal Trade Commission (Nov. 29, 2011).

³⁸ *Id.*

their data, and it require[d] that Facebook obtain periodic assessments of its privacy practices by independent, third-party auditors for the next 20 years.”³⁹

57. On August 10, 2012, Facebook and the FTC formally agreed to settle the FTC’s charges and entered into the Consent Decree (the “FTC Consent Decree” or “Consent Decree”) that would govern Facebook’s conduct for the subsequent 20 years.⁴⁰

58. Part I of the Consent Decree provided that Facebook, “in connection with any product or service . . . shall not misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information, including, but not limited to: . . . (B) the extent to which a consumer can control the privacy of any covered information maintained by [Facebook] and the steps a consumer must take to implement such controls; [and] (C) the extent to which [Facebook] makes or has made covered information accessible to third parties”⁴¹

59. Part IV of the Consent Decree additionally ordered Facebook to “establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to: (1) address privacy risks related to the development and management of new and existing products and services for consumers; and (2) protect the privacy and confidentiality of covered information.”⁴²

³⁹ *Id.*

⁴⁰ John Leibowitz, J. Thomas Rosch, et al., *Decision and Order*, Federal Trade Commission (Aug. 10, 2012).

⁴¹ *Id.*

⁴² *Id.*

60. As David Vladeck, the former FTC Director who worked on the agency’s enforcement action against Facebook, explained, “[t]he **FTC consent decree put Facebook on notice**” that its representations concerning its privacy practices needed to be completely accurate and that any representations would receive significant regulatory scrutiny.⁴³

61. As described in more detail in §§IV.C., IV.G.1. and V.A.2., *infra*, in 2019 following an extensive investigation, the FTC charged Facebook with violating Parts I.B, I.C, and IV of the Consent Decree by, *inter alia*, “**misrepresenting the extent to which users could control the privacy of any covered information maintained by [Facebook]**” based on conduct extending through the Class Period, including Facebook’s practice of whitelisting third parties for continued access to user friends’ data without the knowledge or consent of the users. Indeed, Facebook even overrode users’ privacy settings in order to provide whitelisted third parties with access to use friend data.⁴⁴

62. In July 2019, Facebook settled the FTC’s charges by paying a record-breaking \$5 billion penalty, which constituted the “largest ever imposed on any company for violating consumers’ privacy” and was “almost 20 times greater than the largest privacy or data security penalty ever imposed worldwide.”⁴⁵

⁴³ David C. Vladeck, *Facebook, Cambridge Analytica, and the Regulator’s Dilemma: Clueless or Venal?*, Harv. L. Rev. (Apr. 4, 2018).

⁴⁴ FTC Complaint at ¶¶43-48.

⁴⁵ *Id.*

C. Defendants Immediately Violated the FTC Consent Decree by Continuing to Secretly Share User Friends' Data

63. Despite the 2012 FTC Consent Decree, Facebook secretly continued giving third-party app developers access to user friends' data regardless of how users set their Privacy Settings.⁴⁶

1. Reciprocity: Facebook Gave Third Parties Access to User Friends' Data in Exchange for Data, Money or Other Business Benefits

64. In 2013, defendants acknowledged internally that it was improper for Facebook to give third-party app developers to access user friends' data. As an internal Facebook document dating from August 2013 explains: "Users should not be able to act as a proxy to access personal information about friends that have not expressed any intent in using the app."⁴⁷

65. Defendants' belated acknowledgement was long overdue. As the 2019 FTC Complaint charges: "Facebook knew or should have known that its conduct violated the 2012 [Consent Decree] because it was *engaging in the very same conduct that the [FTC] alleged was deceptive in Count One of the original Complaint that led to the 2012 [Consent Decree]*."⁴⁸

⁴⁶ FTC Complaint at ¶¶37-50. As explained below, the FTC determined this conduct to have violated the FTC Consent Decree because "Facebook represented to consumers that they could control the privacy of their data by using desktop and mobile privacy settings to limit the information Facebook could share"—but "[i]n fact, Facebook did not limit its sharing of consumer information."

⁴⁷ *Id.* at ¶81.

⁴⁸ *Id.* at ¶9.

66. The problem for Facebook was that completely cutting off this practice—and providing users with actual control over their data—would significantly limit Facebook’s ability to profit from its vast store of user data. Defendants did not want to completely give up on monetizing this data.

67. Accordingly, defendants—including Zuckerberg and Sandberg—decided to continue providing access to user friend data to a wide array of third parties who would, in exchange, provide reciprocal value to Facebook. As discussed below, and confirmed in internal Facebook documents, this “reciprocity” became the “fundamental principle that govern[ed]” the Facebook platform from 2014 and continued through mid-2018.

68. The way it worked was that defendants would exchange user friend data as consideration for a reciprocal exchange of value with third-party app developers and other companies who were “whitelisted” for secret access to user friend data.

69. In this way, defendants engaged in selling user friend data in exchange for reciprocal benefits. For defendants, “reciprocity” came in various forms, including an exchange of data between a whitelisted app developer and Facebook, by Facebook requiring the third party to spend substantial sums on advertising at Facebook or by a third party enhancing Facebook’s brand and platform to make it more attractive to users, as in the case of the dozens of major phone device makers that Facebook whitelisted during the Class Period.

70. Indeed, as noted by *Slate*, Facebook’s whitelisting “private agreements were conditional on the third party sending over its own valuable user data to Facebook, or on the company making big advertising purchases with

Facebook,” which constitutes a “business in selling or bartering data.”⁴⁹

2. Facebook’s Internal Documents Confirm Defendants’ Decision to Exchange Data for Reciprocal Value

71. Internal Facebook documents made public in connection with litigation between Facebook and an app developer, Six4Three, LLC (the “Six4Three Documents”)⁵⁰ confirm that defendants supplied user friend data in exchange for reciprocal value. For example, an internal Facebook memo explaining the policies for Facebook’s Platform 3.0 rollout (which indicates that the memo was created in the period from mid-2013 to early 2014), states.⁵¹

The fundamental principle that governs Platform usage is a simple concept: reciprocity. Reciprocity involves an equitable value exchange between a 3rd party developer and Facebook. This value exchange involves one of the following from developers: high-quality experiences that FB users can use to tell great stories to their friends and family on FB and/or monetary value in the form of revenue sharing or direct payment. In return, Facebook offers a developers [sic] access to our Platform.

The memo also states: “During app review, we examine the APIs that the app uses in order to determine what

⁴⁹ Elena Botella, *Facebook Earns \$132.80 From Your Data Per Year*, Slate (Nov. 15, 2018).

⁵⁰ *Six4Three, LLC v. Facebook, Inc., Mark Zuckerberg et al.*, No. CIV 533328 (Cal. Super. Ct. San Mateo Cnty.) (Hon. V. Richard Swope) (the “Six4Three Litigation”).

⁵¹ Six4Three Documents, Ex. 43 at FB-01220345.

[is] the appropriate level of reciprocity. The guideline for this review is ‘take data, give data.’”⁵²

72. Facebook emails dating from September 2013 also note that “the capability will remain to give access features which are publicly deprecated [*i.e.*, discontinued] but available to whitelisted apps.”⁵³ This included “apps that have been whitelisted for . . . friends_”⁵⁴ and listed Netflix as an example.⁵⁵

73. Facebook directly linked third parties’ access to data to the amount a third party was spending on advertising at Facebook. For example, an email string dating from September 2013 shows Ime Archibong, Facebook’s Director of Global Product Partnerships, and Konstantinos Papamiltiadis, Facebook’s Director of Developer Platforms and Programs, discussing the fact that Facebook was requiring third-party app developers to “spend on [advertising at Facebook] **at least \$250K a year to maintain access to the data.**” Otherwise, they would “[c]ommunicate in one-go to all apps that don’t spend that those permission[s] will be revoked.”⁵⁶

74. Zuckerberg and Sandberg were involved in the decision to exchange user friends’ data for reciprocal value from third parties. For example, internal Facebook documents dating from October 30, 2012 shows Facebook employees stating that “we’ve been having **a series of conversations w/ Mark [*i.e.*, Zuckerberg]** for months about

⁵² *Id.* at FB-01220349.

⁵³ Six4Three Documents, Ex. 80 at FB-000061439.

⁵⁴ *Id.*

⁵⁵ *Id.* at FB-000061437.

⁵⁶ Six4Three Documents, Ex. 79 at FB-000061251.

the Platform Business Model.”⁵⁷ These discussions included the fact that Facebook would “remove/**whitelist access** to the Stream APIs and Search APIs and potentially other APIs that might leak the friend graph” and that “[w]e are going to require that all platform partners agree to data reciprocity.”⁵⁸

75. Zuckerberg and Sandberg were on an email exchange dated November 9, 2012 where they each approved the use of “reciprocity” in order to increase the value of Facebook. Zuckerberg stated: “***I think we should go with full reciprocity***” in order to “***increase the value of our network . . . [by] . . . increas[ing] sharing back into Facebook.***”⁵⁹ Sandberg responded: “I like full reciprocity and this is the heart of why.”⁶⁰

76. The Six4Three Documents also include an internal Facebook email exchange on November 2012 in which a Facebook employee suggested that his team “identify our top 20 developers and put together a straw man for how we will enforce reciprocity with each of them. We need this for the meeting with Mark [Zuckerberg] on Monday to help ground the discussion about what ‘full reciprocity’ actually means”⁶¹ The same day, those employees discussed whether the team would classify the developers who would be required to engage in reciprocity with Facebook by “a specific criterion (*e.g.*, MAU)” or “based on the . . . partners which Mark [Zuckerberg] focuses on.” Mike Vernal (“Vernal”) responded that the team should

⁵⁷ Six4Three Documents, Ex. 45 at FB-00423235-36.

⁵⁸ *Id.* at FB-00423236.

⁵⁹ Six4Three Documents, Ex. 48 at FB-01155756.

⁶⁰ *Id.*

⁶¹ Six4Three Documents, Ex. 175 at FB-00947599.

focus on “*the apps that Mark [Zuckerberg] knows, loves, and is concerned about.*”⁶²

77. Additional internal Facebook emails show that Zuckerberg was actively involved in granular decisions to grant or ban third parties from having access to users’ friends’ data. An internal Facebook email exchange dating from January 2013 shows that Zuckerberg specifically approved shutting down Twitter’s “friends API access” because Twitter, a competitor, had launched the “Vine” video app that allowed users to “find friends via FB.” As such, Facebook staff wrote, “Unless anyone raises objections, we will shut down their friends API access today.” Zuckerberg replied: “Yup, go for it.”⁶³

78. As for Tinder, which was whitelisted, Zuckerberg wrote about the reasons why a Tinder co-founder wanted to meet with him, stating: “He probably just wants to make sure we won’t turn off their API.”⁶⁴ Of course, Facebook “whitelisted” this dating app so they continued to get secret access to users’ friends’ data.

79. Similarly, the Six4Three Documents show that Facebook made decisions about how to deal with developers who were angry about changes to the platform (*i.e.*, restriction of their access to user friends’ data) based on the apps’ spending and personal relationships with Zuckerberg and Sandberg. In December 2013, a Facebook employee wrote: “There are also comms plans in the works for working with developers who are high ad spenders and

⁶² *Id.* at FB-00947598.

⁶³ Six4Three Documents, Ex. 44 at FB-00934373.

⁶⁴ Angel Au-Yeung, *Facebook CEO Mark Zuckerberg Dismissed Tinder Cofounder As Irrelevant But Still Let Dating App Get Special Access To Users’ Data*, *Forbes* (Nov. 7, 2019).

friends of Mark/Sheryl [*i.e.*, Zuckerberg and Sandberg].”⁶⁵

80. Indeed, reports show that Facebook used “whitelisting” as a bargaining chip with third parties while presenting the more restrictive policies to the public as privacy enhancements. Before Facebook supposedly cut off third parties’ access to users’ friends’ data, an internal Facebook email shows the Company divided apps into “three buckets: existing competitors, possible future competitors, [or] developers that we have alignment with on business models.”⁶⁶ Facebook employees internally complained that this plan to “group apps into buckets based on how scared we are of them” made them feel “unethical” and “like a bad person.”⁶⁷ After Facebook supposedly cut off access to friends’ data, and announced that change publicly (*see* §IV.D., *infra*), the developers who fell into the “alignment” bucket were able to regain access privately by agreeing to make mobile advertising purchases or provide reciprocal user data from their sites. Facebook executives who worked on the plan reportedly referred to it as the “Switcharoo Plan.”

81. Facebook employees pointed to Zuckerberg as being intimately involved in the discussions and decision-making around these changes to the platform. For instance, in an October 2013 instant message conversation among Facebook employees, Douglas Purdy wrote: “[W]e have spent hours and hours with [**Z**]uck, etc. about this.”⁶⁸

⁶⁵ Six4Three Documents, Ex. 198 at FB-00194154.

⁶⁶ Katie Paul & Mark Hosenball, *Facebook executives planned ‘switcharoo’ on data policy change: court filings*, Reuters (Nov. 6, 2019).

⁶⁷ Six4Three Documents, Ex. 109 at FB-01363612-13.

⁶⁸ Six4Three Documents, Ex. 113 at FB-01353433.

Similarly, another Facebook employee wrote in 2013 that he shared his concerns about changes to the platform “in every single meeting I have with . . . *Zuck*.”⁶⁹

D. Cambridge Analytica and GSR Harvest Facebook Users’ “Likes” and Personal Information for Political and Commercial Purposes

1. Background on Cambridge Analytica’s “Psychographics,” Relationship to Facebook “Likes” Data, and Parties Involved in the Data Misappropriation

82. Cambridge Analytica offered political campaigns the opportunity to weaponize social media data as a voter manipulation tool. In 2014, the company began looking to Facebook for the underlying data necessary to provide such services.

83. By early 2014, Alexander Nix (“Nix”), Cambridge Analytica’s CEO, learned about a research paper by a Cambridge University academic named Michal Kosinski (“Kosinski”), titled “Private traits and attributes are predictable from digital records of human behavior.”⁷⁰ The paper found that Facebook users’ “likes” could be used to successfully predict an individual’s personality traits according to the “OCEAN” scale, a psychometric model that measures an individual’s openness to experiences, conscientiousness, extraversion, agreeableness, and neuroticism. The paper warned that the “[l]ikes” data “may have

⁶⁹ Six4Three Documents, Ex. 114 at FB-01364691.

⁷⁰ Michael Kosinski, David Stillwell, & Thore Graepel, *Private traits and attributes are predictable from digital records of human behavior*, PNAS, 110 (Apr. 9, 2013) at 5802 (“Kosinski Paper”); see also Complaint, *In the Matter of Cambridge Analytica, LLC*, No. 9383 (July 24 2019) (“FTC Cambridge Complaint”) at ¶7 (timing of discovery by Nix).

considerable negative implications, because it can easily be applied to large numbers of people without obtaining their individual consent and without them noticing.”⁷¹ Nix was interested in this research paper because Cambridge Analytica intended to offer voter profiling, microtargeting and other marketing services to U.S. campaigns and other U.S.-based clients.⁷²

84. Christopher Wylie (“Wylie”) was a senior data scientist working for Nix in a Cambridge Analytica affiliate called SCL Elections, which was based in the U.K. Nix tasked Wylie to figure out how to obtain the Facebook “likes” data *and* data modelling that Nix wanted—data and modelling that Nix wanted for commercial purposes.

85. To that end, Wylie approached some professors at Cambridge University who were familiar with Kosinski’s paper about modelling Facebook “likes.” Wylie had spoken with a few professors who rejected Wylie’s proposals that they work with Cambridge Analytica to harvest and model Facebook “likes” for political-commercial purposes. But Aleksandr Kogan (“Kogan”) told Wylie that he would do the data harvesting project. Kogan told Wylie, in substance, “Well, I could do it. As long as you pay for the data and pay for costs, we can do it and figure out some kind of commercial deal after so let’s just see if

⁷¹ Kosinski Paper at 5805. The FTC weighed this kind of research—perhaps this very paper—in arriving at its decision to issue a \$5 billion penalty to Facebook: “Research suggests that *a user’s ‘likes’ of public Facebook pages* can be used to accurately predict that user’s personality traits, sometimes better than the user’s own friends and family.” FTC Complaint at ¶2.

⁷² FTS Cambridge Complaint at ¶9.

this works,” as Wylie testified.⁷³ And Kogan got to work on the Facebook “likes” data harvesting and modelling project with one of his colleagues at Cambridge University—a Ph.D. researcher named Joseph Chancellor (“Chancellor”).

86. Wylie has testified about the importance of Facebook’s data to Cambridge Analytica: “Facebook **data** and the acquisition, using Kogan’s **app** was **the foundational dataset** of the company [Cambridge Analytica]. That is how the algorithms were developed” to generate the psychographic profiles of Facebook users.⁷⁴

87. Kogan told 60 Minutes that he “**did everything**” on the Facebook data harvesting and modeling project with Chancellor, a post-doc researcher at Cambridge University.⁷⁵ “The two were co-founders and equal co-owners of Global Science Research, or GSR, the company that Cambridge Analytica hired to gather the user data and analyze it for psychological traits.”⁷⁶ Facebook eventually lured Chancellor away to work for Facebook at their Menlo Park headquarters. *See infra* §IV.E.

88. In April 2014—as Kogan and Chancellor were preparing to put their “Quiz App” into action—Facebook announced a change to the platform threatened their data harvesting project.

⁷³ Wylie testified to the House of Commons’ Digital, Culture, Media and Support Committee in the U.K. on March 27, 2018 (“Wylie U.K. Test.”) at Q1322.

⁷⁴ Wylie U.K. Test. at Q1305.

⁷⁵ Alex Pasternack, *A Facebook scientist tied to Cambridge Analytica has quietly left Facebook*, FastCompany (Sept. 6, 2018).

⁷⁶ *Id.*

2. In April 2014, Facebook Publicly Announced that Access to Users' Friends Data Would Be Prohibited

89. In April 2014, Facebook publicly announced that it was shutting down third parties' ability to access and collect user friends' data. On April 30, 2014, Zuckerberg himself made this announcement at Facebook's April 30, 2014 F8 Developers' Conference, where he acknowledged how "surpris[ing]" it can be "when friends share some of your data with an app," which he promised to "change."⁷⁷

90. Zuckerberg elaborated that Facebook was aware that users had grown "scared" to log in to apps via Facebook:⁷⁸

[W]e need to do everything we can to put people first and give people the tools they need to [be able to sign] in and trust your apps.

Now, we know that some people are scared of pressing this blue button [*i.e.*, the Facebook button]. You probably—a lot of you have maybe even had personal experiences where you felt this. It's some of *the most common feedback* that we get on our platform.

91. Zuckerberg stated that Facebook would shut-off third-party access to user friend data to ensure that "everyone has to choose to share their own data with an app themselves."⁷⁹ He stressed that this was "a really important step for giving people power and control over how

⁷⁷ Larry Magid, *Zuckerberg Pledges More User Control Of Facebook App Privacy—Unveils Anonymous Log-In*, Forbes (Apr. 30, 2014); *see also* FTC Complaint at ¶197.

⁷⁸ *Facebook's CEO Mark Zuckerberg F8 2014 Keynote (Full Transcript)*, Singiu Post (July 5, 2014).

⁷⁹ FTC Complaint at ¶197.

they share their data with apps.”⁸⁰ On April 30, 2014, Facebook issued a press release promising to give “*people more control*,” including “*more control over their data*.”⁸¹

92. As stated in the FTC Complaint, “in April 2014 . . . Facebook announced that it would stop allowing third-party developers to collect data [about friends].”⁸² As noted below, Zuckerberg and Facebook admitted that this fact was to be “taken as true” in any subsequent litigation by the FTC. Indeed, as also discussed below, Facebook admitted the same in its March 16, 2018 public statement announcing that Cambridge Analytica and SCL Group were being suspended from Facebook, stating, for example: “*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. This is just one of the many ways we give people the tools to *control their experience*.”⁸³

93. Despite what the FTC Complaint calls “these clear statements,” “Facebook continued to allow *millions* of third-party developers access to [user friends’ data] for at least another year.”⁸⁴ The FTC Complaint notes that “Fa-

⁸⁰ *Id.*

⁸¹ *Id.* at ¶98.

⁸² *Id.* at ¶8.

⁸³ See Paul Grewal, *Suspending Cambridge Analytica and SCL Group From Facebook*, Facebook Newsroom (Mar. 16, 2018).

⁸⁴ FTC Complaint at ¶164.

cebook did not disclose this fact to its users”—thereby depriving users of knowledge and the ability to consent to the disclosure of their data.⁸⁵

94. This conduct violated Parts I.B and I.C of the FTC Consent Decree, which prohibited Facebook from misrepresenting “the extent to which a consumer can control the privacy of [their personal information]” and “the extent to which [Facebook] makes or has made covered information accessible to third parties.”⁸⁶

3. Additional Changes Announced on April 30, 2014

95. Also on April 30, 2014, Facebook issued a press release and video tutorial about changes to the app log in procedures. The press release stated: “**Today**, we’re making additional improvements to Login based on people’s feedback.” It noted how “people tell us that some apps ask for too many permissions . . . [t]o address this, we’re extending our existing App Center and Open Graph review process to Login.” The press release also promised to give “people more control,” including “more control over their data.” The accompanying video tutorial stated:⁸⁷

⁸⁵ *Id.* at ¶100. To the contrary, in September 2015, Facebook launched a “Privacy Checkup” tool as a means to help users “be in control” of their data and included a list of apps that users had installed. But this tool failed to list the apps that had access to user data based on their friends’ consent and did not disclose that Facebook was continuing to share that data with “millions of third-party developers.” *Id.* at ¶¶101-105.

⁸⁶ *Id.*, Count I at ¶¶160-165.

⁸⁷ Jeff Sephar, *The New Facebook Login and Graph API 2.0*, Facebook for Developers (Apr. 30, 2014) (embedded video).

[P]ermissions are all about enhancing peoples’ experiences *in your app*. People shouldn’t feel frustrated or worried [about the permissions the app is seeking]. So, during the review process, we’ll make sure that your app is only requesting the permissions that *it really needs*. . . . We make sure to test your Facebook login info on a variety of devices to make sure that there are no crashes or error warnings. This may all seem *really obvious* but it’s gonna make a huge difference when building trust with your app’s audience.

96. The April 30, 2014, Facebook Log In announcement arose years after “*senior Facebook management employees* observed that third-party developers were making more than 800 billion calls to the API per month and noted that permissions for Affected Friends’ data were being *widely misused*.”⁸⁸ Senior executive Vernal (who “reported directly to CEO Zuckerberg”)⁸⁹ framed the issue in terms of being between a rock and a hard place: “I know there’s a constant tension between protecting users and respecting our developer community,” but “[w]e need to soften the punishment” on developers who do not comply with Facebook’s policies.⁹⁰ But another employee responded that “*56% of the time* when a user sees a platform permission dialogue, they don’t grant them” and that “[u]sers don’t trust us enough to handle bad apps.”⁹¹

⁸⁸ FTC Complaint at ¶185.

⁸⁹ Kurt Wagner, *Big-Time Facebook Executive Mike Vernal Is Headed to Sequoia*, Vox (Apr. 18, 2016).

⁹⁰ Six4Three Documents, Ex. 19 at FB-01062013-2014.

⁹¹ *Id.* at FB-01062012.

4. Facebook Initially Rejects Kogan’s Quiz App for Taking Data It Does Not Need—in Violation of Facebook Policies—Then Overrides Its Own Rejection

97. Kogan and Chancellor submitted the Quiz App to Facebook in the context of addressing user fears. On May 6, 2014, Kogan filed an app review application disclosing that the Quiz App wanted to seek users’ permission to download their birthdates, locations (current city) and “likes[.]”⁹² But the Quiz App was a single-use “quiz.” The app did not need to know where users lived and what they “liked.” Requesting data that it did not need was a red flag that the app would do something else with the data.

98. On May 7, 2014, Facebook’s app review process rejected the Quiz App. Facebook wrote to Kogan: “Your app is not using the data gained from this permission to enhance the in-app experience. Please refer to the documents on how to use permissions to create a high-quality, unique, *in-app* experience for the user.”⁹³ Facebook later said that it rejected the Quiz App on May 7, 2014 because it “was requesting more data than it needed to operate *and* did not need to use that data to enhance a user’s in-app experience.”⁹⁴ Facebook’s policy was clear at the

⁹² Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia, Office of the Privacy Commissioner of Canada (Apr. 25, 2019) (“Canada Report”) at ¶129.

⁹³ *Id.* at ¶130 (emphasis omitted).

⁹⁴ *Id.* at ¶136.

time: “Request only the data and publishing permissions your app needs.”⁹⁵

99. Facebook’s “partnership team” was responsible for rejecting Kogan’s Quiz App, as well as all other app rejection decisions at the time.⁹⁶ From 2011-2018, the team was run by Dan Rose (“Rose”), Facebook’s Vice President of Partnerships and Platform Marketing,⁹⁷ who reported directly to Sandberg, Facebook’s COO.⁹⁸

100. In fact, it took less than 24 hours for Rose’s partnership team to reject Kogan’s application to seek users’ “likes” and other personal data for a one-time quiz app, on the grounds that it violated Facebook’s stated developer policies.

101. Despite nominally rejecting Kogan’s application, Facebook nonetheless permitted the Quiz App to collect all the “likes” of the installing users **and** the “likes” of all the users’ friends after May 7, 2014. Facebook itself deliberately overrode its own policies. As a U.K. government report explains, “Facebook rejected [Kogan’s] request on 7 May **2014** but allowed Dr. Kogan to continue using version 1 of the API ***in a manner inconsistent*** with

⁹⁵ 2014 Facebook Platform Policy 7.4 (Oct. 22, 2014) (“FPP 7.4”) at 5; *see also* 2016 FPP (Aug. 28, 2016) (showing the policies did not change).

⁹⁶ Canada Report at ¶132 (“Facebook indicates that these apps’ access to friends’ information was subject to additional review and approval by Facebook’s partnership team.”)

⁹⁷ Geoffrey A. Fowler, *WSJ*(2/15) *Facebook’s Web of Frenemies*, Dow Jones & Co., Inc. (Feb. 16, 2011).

⁹⁸ Dawn C. Chmielewski, *Dan Rose, Facebook Executive Overseeing Partnerships, Is Leaving The Company*, *Deadline* (Aug. 22, 2018).

Facebook’s Developer Policy until May **2015**.”⁹⁹ And as Kogan later testified, “there was not even a signed agreement initially. They gave me the dataset without any agreement signed. It was just, ‘Here’s an email. Here’s the dataset.’”¹⁰⁰ Every “like” that the Quiz App collected for more than a year violated Facebook’s (stated) platform policy: “Request only the data and publishing permissions your app needs.”¹⁰¹ Facebook knew the app violated its own policies, as Facebook’s own “rejection” shows.

102. To explain the contradiction between Facebook’s words and actions, Kogan testified that Facebook’s publicly-stated policies were not Facebook’s actual policies. He also testified that “I don’t think they have a developer policy that is valid” and “For you to break a policy it has to exist and *really* be their policy. The reality is that Facebook’s policy is unlikely to be their policy.”¹⁰² Similarly, he testified: “I mean, if somebody has a document that is

⁹⁹ U.K. Information Commissioner’s Office, *Investigation into the use of data analytics in political campaigns: Investigation Update* (July 11, 2018) (“ICO Report”) at 23.

¹⁰⁰ Signed agreement did not improve matters. In 2014, GSR sent documents to Facebook purporting to give GSR the right to “disseminate, publish, transfer, append or merge with other databases, *sell, license* . . . and archive” any user data that it collected. Julia Carrie Wong, *Congress tried to crack Zuckerberg—but Facebook still has all the power*, Guardian (Apr. 10, 2018).

¹⁰¹ FPP 7.4 at 5; *see also* 2016 FPP (Aug. 28, 2016) (showing policies didn’t change).

¹⁰² Kogan testified to the House of Commons’ Digital, Culture, Media and Sport Committee in the U.K. on April 24, 2018 (“Kogan U.K. Test.”) at Q1966.

not their policy, you cannot break something that is not really your policy.”¹⁰³

5. Kogan’s Quiz App Harvests Data from Tens of Millions of Users and Their Friends After Defendants Promised that Access to User Friend Data Had Been Shut Down

103. As detailed in the sections that follow, it has now been revealed that the underlying Facebook user data obtained by Cambridge Analytica was taken from Facebook *after* Zuckerberg and Sandberg’s April 2014 announcement that third-party access to such data was no longer allowed. Specifically, the app designed by Kogan was not even submitted to Facebook until May 2014 and did not begin harvesting the Facebook user data sold to Cambridge Analytica until after that date.

104. In other words, Kogan was one of the app developers who was—unbeknownst to the public—secretly grandfathered into the third-party information sharing program that defendants had told the public was discontinued months earlier.

105. This fact is acknowledged in the June 2014 contract that Kogan and Chancellor (through GSR) signed with Cambridge Analytica’s parent company, which stated: “GS’s method relies on a pre-existing application functioning under Facebook’s old terms of service. New

¹⁰³ *Id.* at Q1967. Facebook’s own actions corroborate Kogan’s testimony and demonstrate that Facebook knew that Kogan’s app violated Facebook’s policy but permitted Kogan’s app to do so—Facebook’s partnership team “tested” his app via App Review, “rejected” his app, but then allowed the app to harvest users’ “likes” data and additional personal data in violation of its stated platform policies. Facebook’s data transfers via the Quiz App reveals the fact that it overrode its own decision to reject the Quiz App.

applications are not able to access friend networks and no other psychometric profiling applications exist under the old Facebook terms.”¹⁰⁴

106. Further, in its complaint filed in connection with its \$100 million settlement with Facebook, the SEC confirmed that Kogan collected the data sold to Cambridge Analytica *after* Zuckerberg had publicly announced that access to user friends’ data had been shut-off. The SEC Complaint states:¹⁰⁵

In the summer and early fall of 2014, a business entity [*i.e.*, GSR] created and controlled by the researcher [*i.e.*, Kogan] retained a surveying firm to recruit and pay approximately 270,000 Facebook users to download the researcher’s app and take the personality survey. This enabled . . . [Kogan] to collect Facebook data from both the 270,000 app users and many app users’ friends, which collectively amounted to tens of millions of Facebook users.

107. In sum, because Facebook was secretly giving Kogan continued access to user friends’ data in contravention of its public promises in April 2014 to shut-off that access, more than 87 million users had their data improperly harvested by Kogan without their knowledge or consent, which Kogan then sold to Cambridge Analytica.

108. As Roger McNamee (“McNamee”), an early investor in Facebook and mentor to Zuckerberg, stated, only “270,000 people signed up to take [Kogan’s] test”—

¹⁰⁴ See House of Commons, Dig., Culture, Media and Sport Comm.: *Disinformation and ‘fake news’: Interim Rep.*, Background papers submitted by Christopher Wylie (July 29, 2018) (“Chris Wylie Background Papers”) at 84 of 122; see also U.K. Parliamentary Committee, Interim Report at ¶105.

¹⁰⁵ SEC Complaint at ¶24.

but Kogan “was able to harvest data from 50 million people. And those people—all but the 270,000 who signed up for the test—**did not give any permission.**”¹⁰⁶

109. In fact, as detailed below, Kogan and Chancellor (through GSR) were also given whitelisted access to user friend data in May 2015—**after even** Facebook’s internal, secret deadline to purportedly shut down user friend data.

6. Cambridge Analytica’s Quiz App Starts the First Wave of Data Extraction from Facebook’s Servers to Create a Psychographic Model, and Psychographic Scores, Based on Facebook “Likes”

110. On May 9, 2014, Kogan emailed a Cambridge Analytica scientist a “good starting shopping list” of “traits that can be predicted now” and included the OCEAN traits among others. This email implies that Kogan would be able to access all the data that the Quiz App would need “**now,**” despite Facebook’s rejection of the app just two days earlier:¹⁰⁷

¹⁰⁶ Interview of Roger McNamee by Noel King, *Facebook Is Losing Users’ Trust, Tech Investor Says*, NPR (March 20, 2018).

¹⁰⁷ Matthew Rosenberg, Nicholas Confessore, Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. Times (Mar. 17, 2018) (embedded email).



111. By May 30, 2014, Kogan and Chancellor had founded GSR to put the Quiz App into action *and* Facebook had started sending data to the Quiz App, as Chris Wylie testified.¹⁰⁸

GSR is Kogan's company. There were several iterations of the Facebook harvesting project. It first started as a very *small pilot*, firstly to see, most simply, is this data matchable to an electoral register? One of the concerns was if you just collect somebody named John Smith, that could be anybody, so can you match that to this John Smith, on this street, in this city. We then *scaled out slightly to make sure that he could acquire data in the speed that he said that he could*. The first real pilot of it was a sample of

¹⁰⁸ Wylie U.K. Test. at Q1317.

10,000 people who joined the app. That was *in late May 2014*.


Because Facebook started to transfer its users' data by May 30, 2014, Rose's partnership team at Facebook must have overridden the app's app review rejection by this date at the latest.

112. As noted above, on June 4, 2014, GSR entered into a contract with an affiliate of Cambridge Analytica to download more data from Facebook's servers via the Quiz App. Nix signed the contract for the Cambridge Analytica affiliate.¹⁰⁹ Kogan and Chancellor signed for GSR.¹¹⁰

GD Data and Technology Subscription Agreement

The parties have signed this agreement on the date set out above.

SIGNED by 
DR ALEKSANDR KOGAN for and on
behalf of GLOBAL SCIENCE RESEARCH
LTD in the presence of:

Witness:
Signature : 
Name : Joseph Chancellor
Occupation : Co-Director, GSR
Address : 12 HAINSWORTH PLACE CB22 6

113. The contract shows that GSR would collect Facebook "**likes**" to create computer models that would assign personality scores to people who trusted the Facebook platform with their "likes." The "likes" were the key input to modelling personality scores, as the contract states that

¹⁰⁹ Chris Wylie Background Papers at 80-81 of 122.

¹¹⁰ Julie Carrie Wong, Paul Lewis Harry Davies, *How academic at centre of Facebook scandal tried—and failed—to spin personal data into gold*, Guardian (Apr. 24, 2018); FTS Cambridge Complaint at ¶¶14-15.

after the “likes” data are “collected, models are built” that “use Facebook likes to predict people’s personality scores.”¹¹¹

114. GSR and the Cambridge Analytica affiliate further recognized that the Quiz App was the sole psychometric profiling app that would give “access to friend” networks. The contract states, with regard to the Quiz App: “New applications are not able to access friend networks and no other psychometric profiling applications exist under the old Facebook terms.”

115. This fact is significant because it confirms that Cambridge Analytica could not have acquired all of the users’ subject “likes” from any *other source*.

116. The June 4, 2014 contract required GSR to harvest data from Facebook’s servers in a way that targeted Quiz App users (and their Facebook friends), but the scope of harvesting was limited to 11 U.S. states at the time. The contract further specified that that GSR would harvest Facebook profile data about the Quiz App installers (and their Facebook friends) who lived in 11 particular U.S. states, generate personality scores for these individuals, and then match these profiles to U.S. voter records provided to GSR by SCL Elections. GSR would then send these matched records along with the associated personality scores back to SCL Elections.¹¹²

¹¹¹ Chris Wylie Background Papers at 84 of 122.

¹¹² FTS Cambridge Complaint at ¶¶14-15.

7. Facebook “Throttles” the Rate of Data Transferred from Its Servers to GSR Via the Quiz App “Likes”

117. By July 26, 2014, GSR—*i.e.*, Kogan and Chancellor—were required to deliver to SCL psychographic profiles for 1.5 to 2 million people in the specified 11 U.S. states, and match their psychographic profiles to voter records. The contract required the transferred data to comprise, at a minimum, “raw data” sufficient to identify Facebook users’ in real life—first and last name, gender, and location. The contract also required GSR to deliver “modelled” big five OCEAN personality scores (five scores per person), modelled republican party support, modelled political involvement/enthusiasm score, and modelled political volatility scores. Facebook “likes” were the key input to all of these “modelled” data: GSR used the “likes” to train an algorithm that would assign personality scores to the “Facebook friends” who had never downloaded the Quiz App and as a result never disclosed to the app any “Facebook friends” responses to GSR’s personality quiz. The algorithm inferred responses, in much the same way that Facebook’s newsfeed algorithms infer what users would like to read out of the trillions of potential pieces of information circulating throughout the internet.

118. Kogan and Chancellor detailed the procedures they would follow in the contract:

Process Overview

The approach has several steps:¹¹³

1. GS generates an initial “seed sample” using online panels.

¹¹³ Chris Wylie Background Papers at 86 of 122.

2. GS uses its **battery of psychometric inventories** to investigate psychological, dispositional and/or attitudinal facets of the sampled respondents.
3. GS guides respondents through its **proprietary data harvesting technology** (GS Technology) and upon consent of the respondent, the GS Technology scrapes and retains the respondent's Facebook profile **and a quantity of data on that respondent's Facebook friends**.
4. The psychometric data from the seed sample, as well as the Facebook profile and Facebook friend data is run through a **proprietary set of algorithms that models** and predicts psychological, dispositional and or/attitudinal facets of each Facebook record.
5. The **output of step 4 is a series of scores for each record**.
6. GS receives a dataset from SCL and conducts a **matching exercise to append two million (2,000,000) records with GS scores**.
7. GS exports the matched records back to SCL.

119. In July 2014, Kogan and Chancellor ran into a problem at the third step of their process when they were harvesting data from Facebook about the Quiz App's users and their Facebook friends. Facebook engineers "throttled" the data that Facebook's servers were sending to the GSR's servers in the U.K.. Chris Wylie testified about this issue:¹¹⁴

Christopher Wylie: . . . I remember when—and I think this was around **July 2014**—Kogan was delayed for a couple of days because **Facebook had throttled the app, so that it could not pull as much data**.

¹¹⁴ Wylie U.K. Test. at Q1336.

There was some problem with pulling as much data at the same speed as before. He told me that he had a conversation with some engineers at Facebook. I was not in those conversations. This is what he told me at the time. Facebook would have known from that moment about the project, because he had a conversation with Facebook’s engineers, or at least that is what he told me. I do not know if that is entirely true or not, but that is what he told me.

GSR worked out this problem with Facebook’s engineers and transferred the resulting data to Cambridge Analytica (via Nix and SCL). The fact that Facebook’s engineers observed the Quiz App taking too much data is important because it shows—consistent with the app review rejection—that it was taking data the Quiz App did not need in violation of Facebook’s stated platform policies. And it shows the volume of data that the Quiz App did not need was so great that the data transfer alone set off internal alarm bells. But Facebook gave the Quiz App data that it did not need anyway.

8. Cambridge Analytica Puts the First Two Waves of Misappropriated Data to Commercial Use, Targeting “Neurotic” People with Ads that Violate Facebook’s (Stated) Ads Policies

120. On July 26, 2014—around the time that Facebook’s engineers throttled the data—Kogan revealed to Facebook that the Quiz App had a commercial purpose.¹¹⁵ Nix had agreed to pay the Kogan-Chancellor GSR company 75 cents for each voter record that they could match

¹¹⁵ Canada Report at ¶31 (“On July 26, 2014, Dr. Kogan updated the description of the [Quiz] App on Facebook removing the statement that it would not use the data collected for commercial purposes.”).

with OCEAN scores in the 11 U.S. states that they were targeting at the time.¹¹⁶ Cambridge Analytica started making money from the data over summer and fall 2014.

121. During that time, Cambridge Analytica’s biggest customers were a pair of political action committees (“PACs”) that paid Cambridge Analytica \$811,025 in fees.¹¹⁷ Cambridge Analytica was “owned almost entirely”¹¹⁸ by Mercer, who contributed \$1 million to each PAC that paid Cambridge Analytica’s fees.¹¹⁹ An advisor to one of those PACs later shared a presentation that Cambridge Analytica had made to one of those PACs, called the John Bolton Super PAC, with the media.¹²⁰

¹¹⁶ Chris Wylie Background Papers at 86 of 122. Nix then billed a variety of customers \$1.6 million during 2014 and into early 2015; his largest customer during this time was the John Bolton Super PAC (\$703,025 paid to Cambridge Analytica). *Vendor/Recipient Profile Cambridge Analytica*, opensecrets.org (2014); *Vendor/Recipient Profile Cambridge Analytica*, opensecrets.org (2016). The Bolton PAC’s largest donor was Robert Mercer (\$1,000,000) in 2014. *John Bolton Super PAC*, opensecrets.org (2014). Mercer funded the Cambridge Analytica Facebook data harvesting project and was the company’s majority shareholder. Wylie U.K. Test. at Q1273. Mercer’s ownership facilitated Cambridge Analytica’s U.S. political work because foreign nationals (like Nix) generally are not permitted to make donations in U.S. elections. *Foreign nationals*, Federal Election Commission of the United States of America (June 23, 2017).

¹¹⁷ *Vendor/Recipient Profile Cambridge Analytica*, opensecrets.org (2014).

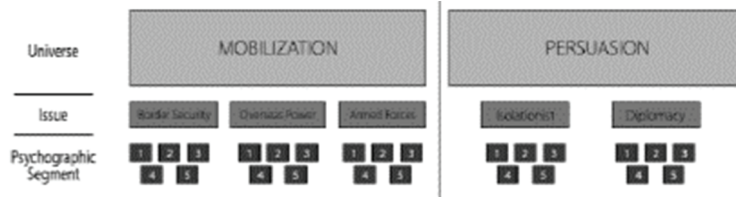
¹¹⁸ Matthew Rosenberg, Nicholas Confessore, Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. Times (Mar. 17, 2018).

¹¹⁹ *Ending Spending Action Fund*, opensecrets.org (2014) (Ending Spending); *John Bolton Super PAC*, opensecrets.org (2014).

¹²⁰ Alexander Zemlianichenko, *Inside John Bolton Super PAC’s deal with Cambridge Analytica*, The Center for Public Integrity (July 16, 2018); John Bolton Super Pac, *CA Political Psychographic*

That PAC supported a number of self-described conservative politicians.

122. Cambridge Analytica’s presentation to the PAC emphasized its psychographic targeting:



Finally, the issue groups have been subdivided according to psychographic personality traits, with voters divided into five segments according to their dominant personality traits, which are outlined in this document.

Each psychographic segment can be targeted on its own, or at the same time as a segment with the same number in a different issue cluster.

123. The five “dominant personality traits” are the OCEAN traits, per the presentation. The presentation described the OCEAN traits, explaining, for example, that “[p]eople with high neuroticism have long, intense reactions to stimuli.” The presentation then gave an example of person who Cambridge Analytica graded as highly neurotic: “Pamela’s friends would describe her as the life of the party, and she loves being around other people. On the inside, however, she has a lot of fears and worries about her security.” These fears and worries informed the kinds of ads that Cambridge Analytica would pay Facebook to send to Pamela.

Messaging Report, Cambridge Analytica (embedded 24-page presentation).

E. Facebook Transfers Approximately 17.1 Billion Facebook “Likes”—and the Users’ Names, Locations, and Other Personally Identifiable Facts—from Its Servers to GSR Via the Facebook Quiz App

1. In 2015 Cambridge Analytica Gets “White-listed” by Facebook for Continued Access to User Friend Data

124. Cambridge Analytica’s customers were pleased with the results that psychographic-segmented custom audiences and custom messaging delivered in 2014 with regard to the 11 U.S. states that they had targeted. This success underlay Cambridge Analytica’s next actions.

125. By January 31, 2015, with the U.S. presidential contests looming, Cambridge Analytica entered into a new contract with GSR to buy more data, this time focusing on Facebook users in the 39 states that Cambridge Analytica was not already using.¹²¹ GSR provided personality scores to SCL Elections for the remaining 39 U.S. states. This step required Facebook data from approximately 250,000-270,000 people who installed the Quiz App and a subset of their “*50-65 million*” Facebook friends—specifically, “*30 million identifiable*” users whom GSR could match to voter records.¹²² Cambridge Analytica paid GSR approximately £200,000 for that data and related services.¹²³ But Cambridge Analytica wanted more data. On or about April 30, 2015, Kogan and Chancellor’s GSR company supplemented their agreement with SCL Elections to that end.

¹²¹ FTS Cambridge Complaint at ¶127.

¹²² *Id.* at ¶126.

¹²³ Kogan U.K. Test. at Q1925.

126. The supplement called for GSR to harvest more data from Facebook’s servers—namely, whether the 30 million people who were the subject of the January 2015 agreement had “liked” any of 500 Facebook group pages that Cambridge Analytica had identified for GSR.¹²⁴ The data were for the upcoming U.S. presidential campaigns.¹²⁵ But harvesting all the 29-plus million “friends” likes with regard to the 500 pages presented yet another serious problem from GSR and Cambridge Analytica’s point of view.

127. As discussed above, Facebook had publicly announced that access to user friend data would be shut off on April 30, 2014. Internally, however, Facebook decided to nevertheless give existing app developers continued access to user friend data for another year without getting direct permission. The internal Facebook deadline to shut down this continued access was April 30, 2015.

128. But, even after the April 30, 2015 internal Facebook deadline passed, Facebook continued to grant GSR access to user friend data without the permission of those

¹²⁴ FTS Cambridge Complaint at ¶127.

¹²⁵ In 2015, a number of political candidates and organizations began preparing their campaigns for the upcoming U.S. presidential primaries and general election. Mercer supported Senator Ted Cruz early in the in the primaries and the Cruz campaign paid Cambridge Analytica \$5.8 million. *Sen. Ted Cruz—Texas*, opensecrets.org (2016) (Cruz expenditures). A political action committee that Mercer funded with Facebook Board Member Peter Thiel (\$1 million given) and others paid Cambridge Analytica \$5.6 million during this time. *Vendor/Recipient Profile Cambridge Analytica*, opensecrets.org (2016) (Cambridge Receipts); *Keep The Promise I/Make America Number 1*, opensecrets.org (2016) (donors to Keep The Promise I/Make America Number 1). The PAC was known as the “Keep The Promise I/Make America Number 1” PAC—Peter Thiel donated \$1,000,000 on October 26, 2016. *Id.*

friends. For example, after May 5, 2015, the Quiz App harvested 500 page “likes” from the 250,000-270,000 Facebook Quiz App installers and their 29 million-plus Facebook “friends.” Cambridge Analytica’s former Business Development Director Brittany Kaiser (“Kaiser”) testified about this subject:¹²⁶

[U.K. MP] Ian C. Lucas: We know that there was contact between Facebook and Cambridge Analytica about the use of data. I think it was in 2015, from memory. Did you know about that at the time?

[Former Cambridge Analytica employee] Brittany Kaiser: Yes. The first time that I heard anything about Facebook data, in writing or even in a personal conversation, which didn’t have to do with those personality quizzes, was late April 2015. Facebook had announced to all of its clients, and therefore to its clients’ clients, that it was going to close its personal data API, which allowed apps and their clients to have access to this data. Before the closing of this access, my chief data officer gave me and two of my colleagues a list of thousands of different groups on Facebook and asked us to **choose 500** of them that we thought having information of the individuals **who like** those groups **would be useful in our modelling** for our new commercial business, which I was helping grow. So we chose 500 of those groups and **turned that into what I suppose is now GSR**, although I wasn’t aware of who we were getting them from at the time, in order to get the data of those individuals **who liked the groups that we chose**. We received that data and **turned in**

¹²⁶ Kaiser testified to the House of Commons’ Digital, Culture, Media and Sport Committee in the U.K. on Apr. 17, 2018 (“Kaiser U.K. Test.”) at Q1595.

that request on 5 May, 2015. If Facebook actually closed that API in April, either a company contracted with Facebook was contravening their legal obligations or they were selling us old data—I am not sure.

129. Kaiser provided written testimony also confirming that, “in May 2015,” Facebook allowed Cambridge Analytica to harvest users’ friends data—in particular “data related to the people who had liked [certain] groups”—*after* Facebook had supposedly closed the “friends data” loophole.¹²⁷

130. Other facts corroborate Kaiser’s testimony. For example, the SEC Complaint confirmed this continued access in May 2015.¹²⁸ Canadian authorities investigated Facebook’s conduct in the Cambridge Analytica matter and likewise found: “*According to Facebook*, the [GSR] App ceased *receiving* information about [installing users’ “friends”] *in May 2015.*”¹²⁹

131. There is no dispute that by April 30, 2015, Defendants had purportedly shut down access to user friend data. So it should have been impossible for GSR to collect the third wave of data in May 2015. But, as discussed above, Facebook—with Zuckerberg and Sandberg’s knowledge and direct involvement—had a secret program in place that gave third parties, including app developers like GSR, whitelisted access to user friend data after the

¹²⁷ “Kaiser Stmt.” refers to the written statement Kaiser provided for the Fake News Inquiry to British Parliament on April 4, 2017. Kaiser Stmt. at 6.

¹²⁸ SEC Complaint at ¶25 (“By the end of May 2015, the researcher had transferred this information to Cambridge.”).

¹²⁹ Canada Report at ¶¶32, 113 (The report explains that the term “Affected Users” refers to the “friends” of users who had installed the app.).

publicly-announced purported April 30, 2014 cut-off date and the internal Facebook deadline of April 30, 2015.

132. Facebook testimony and internal documents demonstrate that Facebook did, in fact, “whitelist” a number of apps like Quiz App around the same time that Facebook whitelisted the Quiz App.¹³⁰

133. A Facebook policy manager, Allison Hendrix, gave testimony on this subject in the Six4Three Litigation.¹³¹ Hendrix was asked at her deposition to review a Facebook “standard form[]” titled “Private Extended API addendum” with parenthesis noting its version, “(v.01.29.20.15).”¹³² The contract at issue in that case, between Facebook and a company called “Nuance,” was dated March 16, 2015, a few weeks before Facebook whitelisted GSR’s Quiz App.

134. Facts show that the Nuance contract was similar to the contract of special privileges that Facebook extended to GSR with respect to the Quiz App. An investigation by *The Wall Street Journal* later confirmed that Nuance was one of the apps that Facebook whitelisted.¹³³ This means that the Nuance contract—one of Facebook’s “standard forms” as Hendrix testified—would have been

¹³⁰ See June 21, 2017, Highly Confidential Deposition Transcript of PMQ of Facebook, Inc., Allison Hendrix (“Hendrix Deposition”) in the Six4Three Litigation matter; see also Six4Three Documents, Ex. 93 at FB-00043884-89 (“Confidential” March 16, 2015, Facebook Private Extended API Addendum between Facebook, Inc. and Nuance Communications, Inc.).

¹³¹ Hendrix Deposition.

¹³² See *id.* at 228:16-25.

¹³³ Deepa Seetharaman & Kirsten Grind, *Facebook Gave Some Companies Special Access to Additional Data About Users’ Friends*, Wall St. J. (June 8, 2018).

substantially the same as the contract that GSR executed with Facebook to secure “friends data” after Facebook purportedly cut-off access on April 30, 2014—after that date, GSR would need secret APIs to get the “friends data.” The form whitelisting agreement defines the “Private Extended API[s]” as “a set of API’s provided by Facebook to Developer . . . **to retrieve data** or functionality that is **not generally available** under Platform,” which, in this case, included the “likes” of the “friends” of the people whom GSR paid to download and take a personality quiz via the Quiz App.

135. *The Wall Street Journal’s* investigation into whitelisting uncovered the fact that Facebook whitelisted a number of apps, reporting: “Facebook officials said the company struck a small number of deals with developers largely to improve the user experience.”¹³⁴ *See infra* §IV.C. The facts show that GSR’s Quiz App was one of the special apps that Facebook gave continued access to “friends data” after even its internal April 30, 2015 deadline to shut this access down completely.

136. Facebook’s standard whitelisting agreement shows that it tried to conceal the program:¹³⁵

Confidential Information. Developer agrees that ***the existence*** and content of the Private Extended APIs, the Private Extended API Guidelines and its

¹³⁴ Facebook made similar statements in response to written questions from the U.S. Senate. Yet, in responding to the question: “Do you know roughly how many executed Private Extended API Addendum agreements Facebook has entered into?” at her confidential deposition, Hendrix testified: “I don’t track the specific number, but I can tell you that there’s definitely many, many, many.” *See* Hendrix Deposition at 230:8-23.

¹³⁵ *See* Six4Three Documents, Ex. 93 at FB-00043885.

use of Private Extended APIs is deemed to be confidential information of FB and Developer will maintain the same in strict confidence and not to disclose the same to any third party (other than agents and contractors for the sole purpose of providing services to Developer hereunder) or use the same for any purpose other than its performance under the Agreement. The obligations contained in this paragraph ***will survive any termination or expiration*** of the Agreement.

In sum, Facebook “whitelisted” the GSR app and a number of similar apps then used form agreements to prevent GSR or anyone else from disclosing the existence of whitelisting. Critically, this was the data that Cambridge Analytica purchased from GSR.

2. Facebook Opens a Non-Public Investigation into Cambridge Analytica, Internally Calling the Company “Sketchy”

137. On September 22, 2015, Facebook began an internal investigation into Cambridge Analytica because this third party was flagged as receiving vast amounts of Facebook user data. Facebook’s internal communications show Facebook’s political team in Washington D.C. warned a group of Facebook employees, that a “sketchy (to say the least) data modeling company [Cambridge Analytica] has penetrated our market deeply”:¹³⁶

¹³⁶ Joint Consent Mot. Regarding Motion to Seal, *District of Columbia v. Facebook Inc.*, No. 2018 CA 008715 B (D.C. Super. Ct. July 25, 19), Ex. A (Sept. 2015-May 2016 Facebook email thread) (“Sept. 2015-May 2016 Facebook email thread”) at 1.

CREATED Sep 22, 2015 9:27 am by [REDACTED]

DESCRIPTION Hi [REDACTED] -

Our team has been spending a lot of time lately attempting to clarify to clients in the political space how our policies apply to pitches coming from vendors regarding matching social data to voter files. You'll recall TrendPo using scraped engager audiences last year to create custom audiences - we suspect many of these companies are doing similar types of scraping, the largest and most aggressive on the conservative side being Cambridge Analytica (<http://ca-political.org/what-we-do/>), a sketchy (to say the least) data modeling company that has penetrated our market deeply. Because the frequency with which this is coming up has increased drastically in the past few weeks, we'd like to work with your team to make sure we have clear channels between our teams. Specifically, we need answers to the following questions:

1. Can we develop template messaging to advise clients on how our policies apply to these types of services? Does this already exist? (I believe I remember enforcement relying on a few different policies last year).
2. Can you help us investigate what Cambridge specifically is actually doing?

138. Facebook redacted the name of the person (“H” and “I”) who wrote to open the investigation into Cambridge Analytica, but the substance of the message indicates that the person worked on Facebook’s political team in Washington DC.

139. Others on Facebook’s political team were involved in the investigation.¹³⁷

Sep 29, 2015 8:57 am
M [REDACTED]

[REDACTED] Following up on [REDACTED] task here - we are getting several pointed questions from the political partner space around what is in bounds versus what is out of bounds. Many companies seem to be on the edge-possibly over. Would it be worth setting up a call to chat through the boundaries? or can you take a look at the cited examples and weigh in on the methods/tolerance for them? Thank you!

Sep 29, 2015 7:16 am

140. Facebook’s platform policies team got involved in the investigation, writing that it would be very difficult for Cambridge Analytica to use Facebook users’ data for political purposes in a way that complied with Facebook’s policies “mainly because it seems to access data that isn’t explicitly being permitted” and triggers a violation of Facebook Platform Policy (FPP) 7.4: “Request only the data and publishing permissions your app needs.”¹³⁸ But the policy team in Menlo Park needed an “App ID” (an internal app identification number) to figure out what Cambridge Analytica was doing.¹³⁹

¹³⁷ *Id.*

¹³⁸ FPP 7.4 at 5.

¹³⁹ Sept. 2015-May 2016 Facebook email thread at 10.

Sep 30, 2015 8:02am
 M [REDACTED] [REDACTED]
 Hello, thanks for surfacing this very interesting question. To start: could you provide App IDs and App names for the apps that are engaging in this scraping of user data?

tldr--Need more info before can offer anything more definitive; but my hunch is that these apps' data-scraping activity is likely non-compliant (see FPPs cited below).

—

As for the website itself, I dug around a bit and couldn't find any very salient red flags. However, in light of our data-sensitivity-related policies, the following Facebook Platform Policies (FPPs) come to mind:

FPP3.9 - Don't sell, license, or purchase any data obtained from us or our services.
 FPP3.10 - Don't transfer any data that you receive from us (including anonymous, aggregate, or derived data) to any ad network, data broker or other advertising or monetization-related service.
 FPP7.4 - Request only the data and publishing permissions your app needs.

There are also more FPPs related to data stuff here: <https://developers.facebook.com/policy/#data>

As for your questions:
 (1) I don't believe we currently have any language/boilerplate messaging re: political analysis/data-scraping apps.
 (2) Please provide App IDs, I'd be happy to investigate their app's activity.
 (3) Without App IDs to dig deeper, I can't say exactly what they're doing, but my initial hunch is that "automatically linking emails in your database to FB accounts" would be against our policies (whether for FPP or otherwise), mainly because it seems to access data that isn't explicitly being permitted access by the user (see FPP7.4 above). It also brings to mind the following:

FPP3.11 - Don't put Facebook data in a search engine or directory, or include web search functionality on Facebook.

With all the above-mentioned FPPs in mind, I imagine it would be "very" difficult to engage in data-scraping activity as you described while still being compliant with FPPs.

141. Yet the Washington DC political team did not have the relevant App IDs:

Oct 13, 2015 11:36am
 H [REDACTED] I [REDACTED]
 It's difficult to get app ID's for these companies since they're usually one-off for clients and they're not volunteering them, but I'll dig a little.

H [REDACTED] [REDACTED]
 facebook | Instagram
U.S. Political and Advocacy | Washington, DC
 [REDACTED]@fb.com

This message shows that the “U.S. Political and Advocacy” team in Washington DC started the Cambridge Analytica investigation—“H” and “I” requested the Cambridge Analytica investigation. And the person whom Facebook anonymized as “M” and “N” was that person’s manager—as she was the manager of Facebook’s political sales team overall:

Dec 18, 2015 1:43pm
 M [REDACTED] [REDACTED]
 @ [REDACTED] [REDACTED], while we sort out the Cambridge Analytica/Research use of data question, can we parallel process two other elements to get ahead of future issues? On Friday, we chatted about equipping our team with a “plain English” description of what is in and out of bounds for data matching in the space. We often point people to the terms, but even having a little more general of a framework/what are the bright lines would equip our sales team in marked better.

There are facts that “M” and “N” was Katie Harbath (“Harbath”), who led a team at Facebook that sold ads and provided other services to Facebook’s Republican clients. ¶¶191, 268 n.282.

142. Facebook’s investigation into Cambridge Analytica’s data misuse continued.

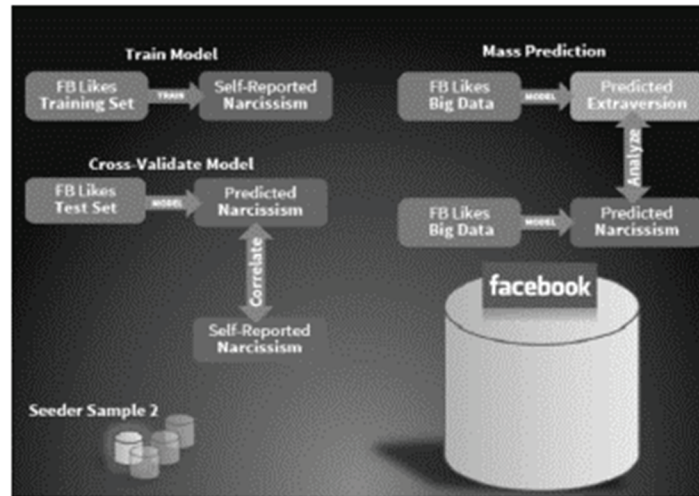
3. Facebook Meets with GSR’s Principals—Kogan and Chancellor—to Discuss What They Learned from the Work They Did for Cambridge Analytica

143. In late 2015, Chancellor and Kogan—GSR’s co-founders—were working together at Cambridge University. The two sat on a panel of four people at a workshop called “Big Data Methods for Social Science and Policy—Interdisciplinary Workshop Programme” held on September 24, 2015.¹⁴⁰

144. Kogan chaired the panel and the three others made presentations. Chancellor made a presentation that bears a strong resemblance to the work that he and Kogan did for Cambridge Analytica. Chancellor explained how he trained a computer model via machine learning to discern the relationship between: (1) survey respondents’ “FB Likes”; and (2) the survey responses that they reported. Chancellor validated the model and then used the model to find Facebook users with similar personality traits based upon their “FB Likes.”

¹⁴⁰ *Big Data Methods for Social Science and Policy—Interdisciplinary Workshop Programme*, Cambridge Centre for Data-Driven Discovery (Sept. 24, 2015).

145. Chancellor illustrated how the methodology worked in several slides, including this one:¹⁴¹



Chancellor also gave examples of the kinds of personality traits that the “FB Likes” model assessed, including the big five “OCEAN” personality characteristics. The presentation described, in substance, what he and Kogan had done for Cambridge Analytica over the preceding months.

146. Chancellor was not the only researcher working under Kogan who presented that day. Rui Sun also presented a paper—one that Kogan would later tell Facebook was based upon data that Facebook had transferred to GSR via the Quiz App. The paper “was prepared with a graduate student in [Kogan’s] lab, other academic collaborators, and members (current and former) of the Pro-

¹⁴¹ Joseph Chancellor, Presentation, *Combining Data- and Theory-Driven Approaches Using Large, Anonymous Datasets of Behavior*, University of Cambridge (2015).

tect and Care team at Facebook that contains data collected from the [Quiz App]” and the paper was “*reviewed and approved by Facebook’s internal review team.*”¹⁴²

147. In early November 2015—approximately six weeks after Kogan, Chancellor and Sun presented their Facebook “likes” based research at Cambridge University—Facebook paid Kogan to teach Facebook what he had learned from the Cambridge Analytica dataset.

148. Kogan told *60 Minutes* that Facebook paid him to present what GSR found from the Cambridge Analytica data to Facebook in November 2015: “I even did a consulting project with Facebook in November 2015, and what *I was teaching them* was lessons I learned from working with this dataset that we had collected for Cambridge Analytica, so I was explaining, “Here’s kinda *what we did*, and here’s what *we learned*, and here’s how you could apply it internally to help you with surveys and survey predictions and things like that.””¹⁴³ Kogan spent a full week teaching Facebook what he and Chancellor did on the Cambridge Analytica project—he “served as a paid consultant [to Facebook] for a week in November 2015.”¹⁴⁴

¹⁴² Stimson Letter at 31 of 40 (The “Stimson Letter” refers to the letter from Rebecca Stimson, Head of Public Policy, Facebook UK, to Damian Collins, Chair, Digital, Culture, Media and Sport Committee, United Kingdom House of Commons, dated May 14, 2018. Attached, at pages 29 and 33 are: June 11, 2016 GSR and Kogan certifications; June 24, 2016 settlement agreement with Kogan and GSR; and (undated) certification by SCL Elections Limited, but none from “Cambridge Analytica.”).

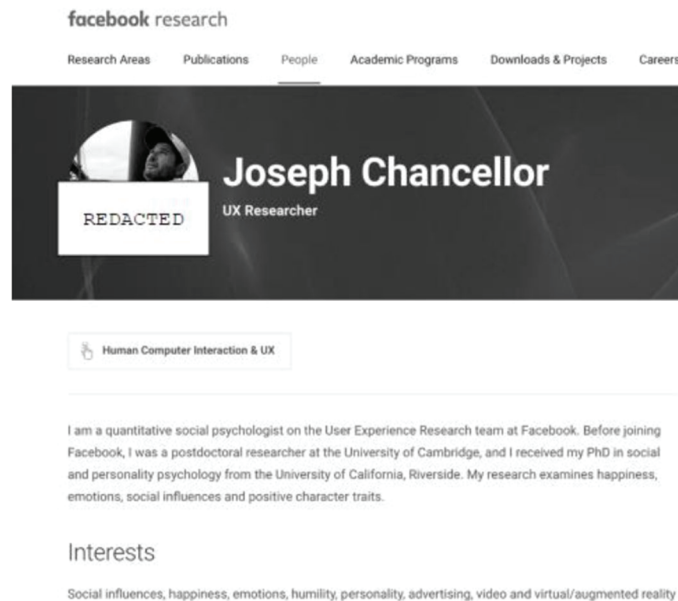
¹⁴³ Julie Carrie Wong, Paul Lewis Harry Davies, *How academic at centre of Facebook scandal tried—and failed—to spin personal data into gold*, *Guardian* (Apr. 24, 2018).

¹⁴⁴ Kate Bubacz, *Cambridge Analytica Data Scientist Aleksandr Kogan Wants You To Know He’s Not A Russian Spy*, *Buzzfeed* (Apr. 22, 2018).

Kogan and Chancellor “‘did everything together’” on the Cambridge Analytica project.¹⁴⁵

149. Following Kogan’s presentations to Facebook about the Cambridge Analytica dataset—presentations that Chancellor likely helped make—Facebook hired him. “Chancellor’s first day [as a full-time employee] at Facebook was November 9, 2015.”¹⁴⁶

150. Chancellor then shared his “facebook research” on a Facebook page:¹⁴⁷



¹⁴⁵ Julie Carrie Wong, Paul Lewis Harry Davies, *How academic at centre of Facebook scandal tried—and failed—to spin personal data into gold*, Guardian (Apr. 24, 2018).

¹⁴⁶ Facebook, Responses to U.S. Senate Select Committee on Intelligence, Questions for the Record addressed to Chairman Richard Burr (Oct. 26, 2018) at 2.

¹⁴⁷ Alex Pasternak, *A Facebook scientist tied to Cambridge Analytica has quietly left Facebook*, Fast Company (Sept. 6, 2018).

151. Chancellor’s resume demonstrates that Facebook paid him to do the same kinds of things working for Facebook as he did at GSR. His resume discloses that he worked with a number of internal Facebook teams, and taught courses on surveys (like those that the GSR Quiz App administered) and how to analyze them.¹⁴⁸ It shows he worked at the company’s headquarters in Menlo Park, and: (1) “Produced independent research for the Core App Monetization, Video, and Social VR product teams with research methods including interviews, intercepts, surveys, log analysis, and experiments”; (2) “Worked inside product teams and cross-functionally with design, product management, data science, content strategy, engineering, and marketing”; and (3) “Became a thought-leader within specific product areas, such as user sentiment to advertising and video ads, mentored new researchers, taught courses on visualization, SQL, data analysis, and survey analysis.”¹⁴⁹

4. The Guardian Links Cambridge Analytica and GSR on December 11, 2015 in Reporting “Millions” of Users’ Data Exposed, but GSR Minimizes the Subject Data to a “Couple Thousand” Anonymous Surveys

152. Facebook’s investigation into Cambridge Analytica stalled until December 11, 2015. Early that morning, *The Guardian* ran its first story on the Cambridge Analytica data harvesting matter, alleging that Cambridge Analytica had acquired millions of Facebook users’ “likes” for psychological modeling that Cruz’s presidential campaign was deploying to “gain an edge over Donald Trump”

¹⁴⁸ Resume for Joseph Chancellor, LinkedIn at 1.

¹⁴⁹ *Id.*

in the primaries, without the users' knowledge or consent.¹⁵⁰

153. Regarding the nature and volume of subject data, *The Guardian* reported:

In the race to advance data-driven electioneering strategies pioneered by successive Obama campaigns, Cruz has turned to Cambridge Analytica for its unparalleled offering of psychological data **based on a treasure trove of Facebook "likes"**, allowing it to match individuals' traits with existing voter datasets, such as who owned a gun.

* * *

Ted Cruz's presidential campaign is using psychological data based on research spanning **tens of millions** of Facebook users, harvested largely without their permission, to boost his surging White House run and gain an edge over Donald Trump and other Republican rivals, the Guardian can reveal.

* * *

[GSR/Kogan] used Amazon's crowdsourcing marketplace Mechanical Turk (MTurk) to access a large pool of Facebook profiles, hoovering up **tens of thousands** of individuals' demographic data—names, locations, birthdays, genders—as well as their Facebook "likes", which offer a range of personal insights.

* * *

Crucially, Kogan also captured the same data for each person's unwitting friends. For every individual recruited on MTurk, he harvested information about

¹⁵⁰ Dec. 2015 *Guardian* article.

their friends, meaning the dataset ballooned significantly in size. Research shows that in 2014, Facebook users had an average of around 340 friends.

154. Kogan disputed and minimized the issue, as reported by *The Guardian*.¹⁵¹

In an email, Kogan said he was unable to explain in detail where all the data came from, as he was restricted by various confidentiality agreements. He said SCL is no longer a client.

He said that *while GSR* often used MTurk for data collection, it “*never collected more than a couple thousand responses* on MTurk for any one project, or even across all projects for a single client—the *vast majority of our MTurk data collection as a company is in the form of surveys only.*” He said GSR stores Facebook data *anonymously*.

Kogan explained that separate from his university role, his private company undertook various commercial ventures relating to data analysis. He said that *when GSR collect Facebook data*, the terms detail the use that information collected will be put to and *make clear* to participants that they are *giving GSR full permission* to use the data and user contribution for any purpose.

155. Here, GSR’s comments contradict *The Guardian*’s allegations to the extent the allegations can be read to suggest that tens of millions of Facebook’s users’ data were harvested inappropriately, if at all. The Kogan/GSR remarks suggest that a “couple thousand” (about 2,000) users’ data were at issue, that they had given permission to GSR to collect largely “survey” data (not “likes”), and

¹⁵¹ *Id.*

that survey results were anonymized somehow. GSR said nothing about the kind of data—if any—that the company gave to SCL, noting that they were no longer a client. Thus, the only entity to go on the record in any substantive way—Kogan/GSR—painted a relatively benign picture of the amount and nature of data at issue.

156. Neither Cambridge Analytica, nor the Cruz campaign nor Facebook confirmed or denied any of the story’s allegations or any of Kogan’s statements. A Cruz campaign spokesperson suggested that nothing untoward had occurred: “***My understanding*** is all the information is acquired legally and ethically with the permission of the users when they sign up to Facebook.”¹⁵²

157. After the initial report ran in the morning of December 11, 2015, a Facebook spokesman went on the record, and *The Guardian* updated its story accordingly.¹⁵³

After this article was published, Facebook said the company was “carefully investigating this situation” regarding the Cruz campaign.

“[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,” a Facebook spokesman said in a statement to the Guardian.

¹⁵² *The Guardian* reported that Cambridge Analytica’s CEO, Nix, “did not respond to a request for comment.” When *The Guardian* first ran its story at 4:30 a.m. (PST), Facebook did not have a comment: “A spokeswoman for Facebook declined to comment.” *Id.*

¹⁵³ *Id.*

By the time that *The Guardian's* December 11, 2015 story ran, of course, Facebook had already known much of what Cambridge Analytica was doing. After *The Guardian* raised publicity about GSR and Cambridge Analytica, more information began to surface inside of Facebook.

5. Facebook's Investigation Expands as Numerous Facebook Employees Become Aware of the Investigation

158. Before *The Guardian* ran its report December 11, 2015 report, Facebook's communications team was evasive with *The Guardian*.¹⁵⁴

Before we published that story in 2015 [the December 11, 2015 story], I had approached Facebook's public relations representatives in London ***to inform them of the allegations***. I asked them a series of questions, including: "Is Facebook concerned that highly personal data about a large set of its users is now being exploited for experimental political campaigning purposes?" ***They didn't answer***. After declining to comment on the record, they emailed a few lines on background: "Facebook has a clear data use policy that makes it clear how the information people choose to add to Facebook is used." Their repetition of the word "clear" only made this feel more doubtful.

159. After *The Guardian* ran its report, Facebook swung into public relations ("PR") damage control. The same communication string that Facebook employees had opened about Cambridge Analytica on September 22, 2015 reflected the new status of the investigation to a "hi

¹⁵⁴ Harry Davies, *Facebook told me it would act swiftly on data misuse—in 2015*, *Guardian* (Mar. 26, 2018).

pri”—*i.e.*, high priority—issue, noting “[w]e need to figure this out ASAP,” as the following internal Facebook communications show:¹⁵⁵

Dec 11, 2015 10:06am
 C: [REDACTED]
 Hi everyone – this is hi pri at this point. This story just ran in the Guardian and is now prompting other media requests. We need to sort this out ASAP. Thank you!
 Dec 11, 2015 9:45am
 M: [REDACTED]
 [REDACTED] - Can you expedite the review of Cambridge Analytica or let us know what the next steps are? Unfortunately, this firm is now a PR issue as this story is on the front page of the Guardian website - <http://www.theguardian.com/> /senator-led-cruz-president-cam ... CC [REDACTED] [REDACTED] is fielding comms policy requests and concerns.

160. Facebook’s Cambridge Analytica investigation became high priority because it was now a “PR issue,” such that “comms policy” at Facebook was expressing “requests and concerns.” Facebook’s PR team started fielding internal PR issues at the same time. For example, Facebook’s PR message group reported the fact that Facebook’s research team worked with Kogan. In other words, it appeared as though Facebook had paid Kogan in the past for his expertise:

Dec 11, 2015 2:18pm
 M: [REDACTED]
 Also, importantly: according to the Wait, What thread and also an email from WW [REDACTED] [REDACTED] - it sounds like Facebook has worked with this “Aleksandr Kogan” on research with the Protect & Care team.
 Dec 11, 2015 1:04pm

The “Wait, What thread” specified in the above communication was shorthand for “Wait, What? Ask PR,” which was a PR message group that was visible to all Facebook employees.¹⁵⁶

161. Facebook’s communications team scrambled in response. One of *The Guardian* reporters working on the

¹⁵⁵ Sept. 2015-May 2016 Facebook email thread at 7.

¹⁵⁶ Sept. 2015-May 2016 Facebook email thread at 6. That month Facebook’s research (Protect and Care) team published a paper with “Aleksandr Spectre [who] previously published under the name Aleksandr Kogan.” *Id.* at 5; Maurice H. Yearwood, *et al.*, *On wealth and the diversity of friendships: High social class people around the world have fewer international friends*, *Personality and Individual Differences* 87, 224 (2015).

story would later recall: “[h]ours after the story was published, Facebook’s PRs got in touch seeking more information, and later that evening I heard from the mother-ship itself when *a senior*, California-based employee emailed a statement” to *The Guardian*.¹⁵⁷ Eliot Schrage was one of two senior, California-based employees who were responsible for Facebook’s communications and *The New York Times* reported that Schrage was an “architect of Facebook’s responses to a range of scandals” including “Cambridge Analytica.”¹⁵⁸

162. Schrage reported to Sandberg, who oversaw policy and communications.¹⁵⁹

¹⁵⁷ Harry Davies, *Facebook told me it would act swiftly on data misuse—in 2015*, *Guardian* (Mar. 26, 2018).

¹⁵⁸ *The New York Times* reported that Schrage was “an architect of Facebook’s responses to a range of scandals, including the rise of misinformation on the site and the misuse of user data by the political consulting firm Cambridge Analytica.” These facts demonstrate Sandberg and Schrage were involved in Facebook’s Cambridge Analytica investigation and its related public statements. Sheera Frenkel, *Facebook’s Head of Communications and Policy Is Leaving Company*, *N.Y. Times* (June 14, 2018).

¹⁵⁹ Schrage was the “VP of public policy and global communications.” Kurt Wagner & Rani Molla, *Mark Zuckerberg’s birthday photo shows the 20 Facebookers you should know not named Mark Zuckerberg*, *Vox* (May 16, 2017). That title corresponds to the “comms policy” requests and concerns that elevated Facebook’s internal Cambridge Analytica investigation to high priority status. ¶159. Sandberg later testified that she learned about the Cambridge Analytica matter when *The Guardian* reported it and it has been reported that Sandberg “overs[aw] Facebook’s policy and communications arms,” plausibly showing that her direct report (Schrage) would have been involved in managing Facebook’s response. Nicholas Confessore & Matthew Rosenberg, *Sheryl Sandberg Asked for Soros Research, Facebook Acknowledges*, *N.Y. Times* (Nov. 29, 2018). While both Sandberg and Schrage were “senior” communications/policy

163. Schrage would have been involved in the Cambridge Analytica investigation. Mark Zuckerberg’s testimony confirmed that he was involved in at least some discussions of Facebook’s decision not to notify the users that their data had been compromised, which confirms that he knew about Facebook’s investigation into Cambridge Analytica.¹⁶⁰

6. Facebook’s Investigation Discovers the “Likes” Model—“Solid Science”

164. Facebook employees and third parties got in touch with Facebook’s investigation team to share information about the parties involved in the data harvest, and to share information about the nature of the data harvest itself. For example, one of Kogan and Chancellor’s former colleagues at Cambridge University—Professor Michal Kosinski—offered to help Facebook with the investigation.¹⁶¹

people, Facebook’s comment to *The Guardian* on the record in the evening of December 11, 2015 was from a “spokesman,” which plausibly shows Schrage was more likely the senior person who provided the comment in comparison to Sandberg. ¶157. Sandberg and Schrage’s duties also involved reviewing internal weekly news summaries that included “[f]lags” of media reporting policy actions against developers. *See, e.g.*, Six4Three Documents, Ex. 58 at FB-01373378-380 (reporting to Sandberg, Schrage, Rose, Hendrix and others “Platform Weekly News—5/17/13,” with one of three “Flags” consisting of this information: “We took action against Social Roulette for violating Platform policies. This was picked up by TechCrunch, CNET and PC Mag.”).

¹⁶⁰ Committee Hearing Transcript at 63.

¹⁶¹ Sept. 2015-May 2016 Facebook email thread at 5; Maurice H. Yearwood, *et al.*, *On wealth and the diversity of friendships: High social class people around the world have fewer international friends*, *Personality and Individual Differences* 87, 224 (2015).

Dec 11, 2015 3:50pm
 A: [REDACTED]
 Hi – I'm a bit familiar with some of the context around the personality modeling stuff. As I understand it, it's inspired from <http://www.pnas.org/content/110/15/5802.abstract> which is solid science. I'm good friends with the lead author from that paper (Michal Kosinski) and he is not happy about how these guys are bringing his field of research into disrepute. He's offered to chat with people on our end and to give more context if that helps. edit: to be clear, the datasets mentioned in the Guardian article are different/collected differently to those in the PNAS research!
 Dec 11, 2015 3:22am

Here, Facebook's investigation discovered the significance of the “treasure trove of Facebook ‘likes’” that was one facet of *The Guardian's* core allegations.¹⁶² The message (above) linked to Kosinski's paper about “likes” modelling that warned that it “may have considerable negative implications, because it can easily be applied to large numbers of people without obtaining their individual consent and without them noticing.”¹⁶³

165. Facebook's investigation team also suspected GSR was selling data that would allow the buyers to identify the data subjects in real life—called, personally identifiable information or “PII”:¹⁶⁴

Dec 11, 2015 12:56pm
 H: [REDACTED]
 [REDACTED] – I just looked more deeply on the GSR website and it appears they *are* offering PII via their API:
 Reveal new depths of insight from your social media data with our API product, delivering the same consumer psychology insight provided by BrandAnalyzer at the individual level.
 *Enrich Your Social Media Data
 Augment social media data by appending deep psychological profiling, contextualized brand preferences, and more accurate consumer personas.

166. Others at Facebook joined the investigation, sharing what they knew about GSR's collection.¹⁶⁵

Dec 11, 2015 4:17pm
 W: [REDACTED]
 Hey team, A: [REDACTED] pointed me to this thread. Alex Kogan was my postdoc supervisor at Cambridge, although I left before he founded GSR. I have a cursory understanding on the basic principles behind GSR's products and data collection methods, if that helps. Feel free to ask me anything.
 Dec 11, 2015 3:50pm

¹⁶² Dec. 2015 *Guardian* article.

¹⁶³ Michal Kosinski, Academic Biography, Stanford Graduate School of Business; Kosinski Paper at 5805 (Apr. 9, 2013).

¹⁶⁴ Sept. 2015-May 2016 Facebook email thread at 5.

¹⁶⁵ *Id.* at 5.

7. Facebook Discovers that Facebook’s Own Decisions Allowing GSR to Violate Facebook’s Stated Policies Are at the Root of the Cambridge Analytica Data Harvest

167. On December 11, 2015, Facebook internally copied a large block of text from “the Guardian article on the supposed connection between SC and GSR”.¹⁶⁶

Dec 11, 2015 1:04pm
 F [REDACTED]
 The relevant part from the Guardian article on the supposed connection between SCL and GSR:

By summer 2014, Kogan’s company had created an expansive and powerful dataset. His business partner boasted on LinkedIn that their private outfit Global Science Research (GSR) “owns a massive data pool of 40+ million individuals across the United States – for each of whom we have generated detailed characteristic and trait profiles”.

Documents show SCL agreed to a contract with GSR, whereby it would pay its data collection costs in order to improve “match rates” against SCL’s existing datasets or to enhance GSR’s algorithm’s “national capacity to profile capacity of American citizens”.

In an email, Kogan said he was unable to explain in detail where all the data came from, as he was restricted by various confidentiality agreements. He said SCL is no longer a client.

He said that while GSR often used MTurk for data collection, it “never collected more than a couple thousand responses on MTurk for any one project, or even across all projects for a single client – the vast majority of our MTurk data collection as a company is in the form of surveys only”. He said GSR stores Facebook data anonymously.

Kogan explained that separate from his university role, his private company undertook various commercial ventures relating to data analysis. He said that when GSR collect Facebook data, the terms detail the use that information collected will be put to and make clear to participants that they are giving GSR full permission to use the data and user contribution for any purpose.

He said Cambridge University had “no knowledge of the clients or projects GSR had worked on” and that GSR has never used any data collected as part of his university activities.

168. As of 12:59 p.m. that day, Facebook’s investigation team was tracking down internal business and app identification numbers for Cambridge Analytica and GSR.¹⁶⁷

Dec 11, 2015 12:59pm
 S [REDACTED]
 Digging in more. [REDACTED] pulled this list of UIDs (first three are associated with Cambridge Analytica, last one is associated with GSR):
<https://fburl.com/18702435>. I tried to find an obvious connection among the group, but wasn’t able to (no shared apps, pages, etc. among ALL four). This means that the Cambridge Analytica/GSR connection remains unconfirmed.

With that said, we found a Business ID (id: 402906616566868) for Cambridge Analytica with one admin: YY [REDACTED] ZZ [REDACTED]. The business has a Page with 0 fans: <https://www.intern.facebook.com/cambridgeanalytica/>.

Lastly (and most interestingly), the business is associated with two other Pages: <https://www.intern.facebook.com/keepthepromise/> (a ted cruz page that links here: <http://www.keepthepromise1.com/about/>) AND <https://www.intern.facebook.com/PCIAA/> (property casualty insurers which links here: <http://www.pciaa.net/about-us/about-pci>). Both Pages have roughly 1k likes.

169. By 4:27 p.m. on December 11, 2015, Facebook official “D _____ E _____” reached out to Kogan about *The*

¹⁶⁶ *Id.* at 6.

¹⁶⁷ *Id.* at 6.

Guardian article, asking for an immediate response over email and to schedule a call with him. Kogan “privately” got in touch with Facebook’s investigation team “[w]ithin days”¹⁶⁸ of this request.¹⁶⁹

Dec 11, 2015 4:27pm
 [REDACTED] [REDACTED]
 Update: We are reaching out to Dr. Kogan and will schedule a call in addition to asking for immediate responses over email. Please be sure not to contact Dr. Kogan or discuss anything pertaining to this investigation if he contacts you. If he does contact you, please put him in touch with me directly.
 DevOps team - are [REDACTED] and [REDACTED] my poc for this investigation or should I include anyone else on any mtgs we schedule (want to make sure I'm looping in the right people)?

170. Within days of December 11, 2015, Facebook learned the name of the Quiz App from Kogan and was, therefore, able to track down its App ID number and history. As illustrated by the following example—pertaining to a different app—Facebook learned a lot about the Quiz App from its App ID:¹⁷⁰

Dec 17, 2015 5:17pm
 J [REDACTED] [REDACTED]
 That would be great! As [REDACTED] mentioned I've been digging into Nation Builder following our call with Strategic Media 21 though am struggling to fully understand the app based on online investigation alone. Here's what I've found:
 - NationBuilder (126739510711965), 132k MAP
 - Passed review for following permissions (https://our-astools.facebook.com/.../xrow/apps/submission-su.../f: user_events, publish_actions, rsvp_event, manage_pages)
 - Actively pulling these perms: <https://fburl.com/168831558>
 - In short the app seems to offer monthly subscription services for politicians, nonprofits, unions, etc building profiles based (in part) on information pulled from the person's activity on the client's Facebook Page. It then seems to offer correspondence services for the client's 'voter database,' including email blasts and text messages. From the 'How to connect to FB' FAQ page (http://nationbuilder.com/how_to_facebook_twitter_facebook).

171. The history of GSR’s Quiz App was far more troubling than that pertaining to the “NationBuilder” app—in the above example—because the Quiz App’s history revealed that Facebook allowed the app to violate its

¹⁶⁸ SEC Complaint at ¶4 (“Within days of the press report, both [Kogan] and Cambridge Analytica privately confirmed to Facebook that [Kogan] had transferred personality profiles based on Facebook user data to Cambridge Analytica.”).

¹⁶⁹ Sept. 2015-May 2016 Facebook email thread at 5.

¹⁷⁰ Sept. 2015-May 2016 Facebook email thread at 4.

platform policies *so that* it could download the data at issue from Facebook’s servers.

172. Whereas the “NationBuilder” app identified in the above example “[p]assed [app] review,” the Quiz App failed app review but was nonetheless allowed to harvest data that the app did not need anyway. *See* §IV.D.4.-8. The same “review” history would have flagged the fact that Facebook whitelisted the app. *See* §IV.E.1. And Facebook also was able to uncover the “perms” that apps were pulling, meaning Facebook could see what kinds of data the Quiz App users were giving “permissions”—whether legitimate or deceptively induced—to the Quiz App that the Quiz App could then use to pull data from Facebook’s servers about the users. Facebook could readily access all of the details it wanted about the information that the Quiz App was pulling because the Quiz App was pulling data from Facebook’s own servers—servers that Facebook engineers used to “throttle” the Quiz App previously.¹⁷¹

¹⁷¹ Facebook’s internal documents provided a number of illustrations of how the company could pull detailed information on thousands of apps at a time. *See, e.g.*, Six4Three Documents, Ex. 74 at FB-00061650 (Facebook internal communication addressing “private API usage”—*i.e.*, whitelisting—pulling historical monthly active user stats for 6,000 apps); Six4Three Documents, Ex. 80 at FB-00061439 (Facebook internal communication discussing “thorough audit on the apps that have been whitelisted for capabilities equivalent to the public APIs we will be deprecating, *i.e.*, apps that have been whitelisted”); Six4Three Documents, Ex. 72 at FB-00061223 (Facebook internal communication regarding large-scale app audit, noting “I have identified 110 apps out of a list of 1,100” to audit); Six4Three Documents, Ex. 77 at FB-01363528-531 (Facebook internal presentation noting that it would take “**2 weeks**” to audit “top 500” apps on Facebook, and showing a number of apps that cause “data leakage,” including a 12 apps whose monthly active uses are far lower than the number of data requests the app developers were making—for example, one app had

173. These reviews uncovered the Quiz App’s data download history—the three data transfer “waves,” the whitelisting and the app review rejection/override as detailed above.

174. Importantly, Facebook’s investigation into *The Guardian*’s December 11, 2015 report discovered that Kogan made misleading statements to *The Guardian*—and, by extension, to the public—about the nature of the data at issue:¹⁷²

- As Facebook knew, contrary to Kogan’s assurances to the public that “GSR stores Facebook data anonymously,” GSR collected Facebook users’ names, locations, gender and their Facebook user identification numbers.¹⁷³

334 thousand monthly active users but had pulled friends data from Facebook over 131 million times in preceding 30 days); Six4Three Documents, Ex. 78 at FB-01352120 (Facebook internal presentation summarizing data on 1.4 *million* apps, including number of monthly active users and number of calls app made to collect data from Facebook’s server via APIs over preceding 30 days) and *id.* at FB-01352144 (breaking down the number of apps requesting “friends” data on a daily basis—13,350 apps in total, with “0.9%” associated with Facebook Preferred Marketing Developers (“PMDs”) generating approximately 7 million impressions per day); Six4Three Documents, Ex. 146 (Facebook internal excel spreadsheet detailing and ranking apps, identifying app developers by name, and quantifying the total number of *minutes* each app had been used in the aggregate by Facebook users).

¹⁷² Kurt Wagner, *Here are the New York Times and Observer stories that pushed Facebook to suspend Trump’s data analytics company*, N.Y. Times (Mar. 17, 2018).

¹⁷³ Dec. 2015 *Guardian* article. Facebook gave the Facebook User ID datapoint to all developers. *See, e.g.*, Six4Three Documents, Ex. 43 at FB-01220350 (Facebook internal document stating that “anyone”—referring to any developer—can get “uid” without any re-

- As Facebook knew, contrary to Kogan’s assurances that GSR “never collected more than **a couple thousand** responses on MTurk”¹⁷⁴—the service GSR reportedly used to collect data from Facebook users—“for any one project, or even across all projects for a single client,” GSR collected personal information, from Facebook’s own servers, about **50-65 million** users. For the **30 million** users that GSR tied to U.S. voting records, GSR collected, on average, 570 “likes” per user—or approximately 17.1 billion “likes” in all.
- As Facebook knew, contrary to Kogan’s assurances that all of the affected users gave GSR “full permission” to collect the subject data, GSR lied to the users that GSR would only use the data for “research” and also lied to the users that GSR would not collect any personally identifiable information—in fact, the user identification numbers, name, gender, and location data are the opposite of “anonymous” data. Facebook’s security chief later admitted that Kogan “enticed several hundred

view—the “uid” datapoint refers to the Facebook User ID). Facebook’s servers transferred Facebook User IDs tied to all of the data that Kogan and Chancellor harvested via the Quiz App. *See, e.g.*, FTC Cambridge Complaint at ¶¶23-25 (stating the Quiz App “collected the Facebook User ID” along with a number of other datapoints from those who installed the app (250,000-270,000 people) and from all of their Facebook “friends” (50-65 million people)). Facebook’s internal communications show Facebook’s investigation suspected GSR was selling personally identifiable information before the team secured the Quiz App’s identification number. *See, e.g.*, Sept. 2015-May 2016 Facebook email thread at 6 (Facebook internal communication dated December 11, 2015 (between 12:00 p.m. and 12:56 p.m.) stating, “I just looked more deeply on the GSR website and it appears they ***are* offering PII**”—personally identifiable information—“via their API”).

¹⁷⁴ *See infra*. Dec. 2015 *Guardian* article.

thousand individuals to use Facebook to login to his personality quiz” but that Kogan “*lied to those users*” to get them to login.

175. But Facebook elected to conceal these facts from Facebook users and investors.

8. Cambridge Analytica Represents that It Received “Personality Score Data” from GSR, Which Facebook Confirms Violated Facebook’s Platform Policies

176. On December 17, 2015, Alex Tayler (“Tayler”), Chief Data Officer for Cambridge Analytica, wrote to Facebook executive Allison Hendrix (“Hendrix”) asking for confirmation that Cambridge Analytica had not breached Facebook’s terms of service.¹⁷⁵

177. Facebook responded that Cambridge Analytica *had* violated Facebook’s policies and terms. Indeed, on December 18, 2015, Facebook’s Hendrix replied and confirmed that Cambridge Analytica’s had violated Facebook’s policies and terms. Hendrix also confirmed Cambridge Analytica’s prior statements that it had “received *personality score data* from Dr. Kogan” and that Cambridge Analytica had funded Kogan’s work:¹⁷⁶

Thank you again for taking the time to speak with me last week and providing additional information into *Dr. Kogan’s development of the GSR app which was*

¹⁷⁵ See Mike Butcher, *Cambridge Analytica email chain with Facebook sheds new light on data misuse scandal*, TechCrunch (Jan. 17, 2020) (“Jan. 2020 *TechCrunch* article”). *TechCrunch* reported: “This entire exchange was then forwarded by executives from the N6A PR agency to Cambridge Analytica executives and was, in turn, obtained by Kaiser on 23 January 2016.”

¹⁷⁶ *Id.*

funded by Cambridge Analytica (via SCL Elections). As discussed, we don't allow any information obtained from Facebook to be purchased or sold, and we have strict friend data policies that prohibit using friend data for any purpose other than improving a person's experience in your app. From our conversations, ***it is clear that these policies*** have been violated.

You have ***told us that you received personality score data from Dr. Kogan that was derived from Facebook data, and that those scores were assigned to individuals included in lists that you maintained***. Because that data was improperly derived from data obtained from the Facebook Platform, and then transferred to Cambridge Analytica in violation of our terms, we need you to take any and all steps necessary to completely and thoroughly delete that information as well as any data derived from such data, and to provide us with confirmation of the same.

178. On January 18, 2016, Cambridge Analytica emailed Facebook that it would delete the personality score data.

179. By that date, approximately 30 people at Facebook knew about the company's investigation into Cambridge Analytica, including senior management in "Facebook's communications, legal, operations, policy, privacy, and research groups."¹⁷⁷ They all also knew that Cambridge Analytica had violated the Facebook's platform policies. Facebook chose to conceal all of these facts as it prepared for the presidential election, which Sandberg

¹⁷⁷ SEC Complaint at ¶30

compared to the “Super Bowl” in terms of advertising dollars and user engagement.

9. Sandberg Compares the 2016 Presidential Election to the World Cup, Super Bowl and Olympics in Terms of Ad Spend as the Primaries Continue to Unfold

180. With the Cambridge Analytica data harvest fresh in mind, Facebook’s senior management continued to discuss use of Facebook data for political campaigns with the investment community. On January 27, 2016, for example, Facebook held a public conference call with securities analysts and investors. An analyst asked Sandberg, “Sheryl, could you talk about political advertising? And, how you think about the attractiveness of—and any anecdotes you have on Facebook as a platform for political campaigns?”¹⁷⁸ Sandberg responded:

In terms of the elections, it’s important to note that we’re large and diversified, so no one vertical drives our business. ***Yes, the 2016 election is a big deal in terms of ad spend. But, so is the World Cup. So, is Super Bowl every year. So are events like the Olympics.***

We are excited about the kind of targeting we’re able to offer for our ads platform. We believe we have precision that doesn’t exist on any other platforms. So, for example, using Facebook and Instagram ads, you can target by congressional district, you can target by interest, you can target by demographics, or any combination of those. And, we’re seeing politicians at all levels really take advantage of that targeting.

¹⁷⁸ Q4 2015 Facebook Inc. Earnings Call Tr. at 16 (Jan. 27, 2016).

It's also probably worth saying that we're pretty excited about what's happening with the elections organically on Facebook. Facebook is really the new town hall and connecting the people who are running for office, both at the national and the local level with people directly has been really important. Every member of congress in the United States is now on Facebook. We're seeing some of them post every vote and explain why they are doing votes. We're seeing a bunch of the candidates for president get on Facebook themselves and interact, taking questions from their potential voters directly. And, we think that kind of direct engagement where people can hold their elected officials accountable, and elected officials can speak directly to constituents is a really important part of our mission, and ***we're excited about the 2016 election and what's happening there.***

181. On February 9, 2016, Sandberg attended a Goldman Sachs Technology Conference where she discussed "election issues," and stated:¹⁷⁹

So we think it's incredibly important. From the ad side, ***this is a big advertising event***, but we have a very diverse space, and no one event drives our ad revenue. There's also Super Bowl and World Cup. But we do have a pretty compelling ad offering in the market. We're the only place where you can target not just by gender, life's interests, but you can target by congressional district. And so we see people increasingly using our ad platform to do a kind of targeting that only we can do.

¹⁷⁹ Facebook Inc. at Goldman Sachs Tech. Conference Tr. at 5-6 (Feb. 09, 2016).

182. On March 2, 2016, Sandberg and Rose attended the Morgan Stanley Technology, Media & Telecom Conference. One participant discussed the U.S. presidential elections and asked how campaigns were using Facebook. Sandberg responded by explaining, among other things:¹⁸⁰

Well, I think it's very exciting, the election, certainly from Facebook's perspective because there's lots of interesting content being generated and shared on Facebook. It's an incredible platform for people to connect and they are connecting with politicians. [There are] conversations going on amongst friends about the election and so there's tons of interactions.

We have seen I think it's 75 million, 76 million people interact on Facebook around the election. So there's an incredible amount of engagement going on. . . .

On the ad side, I think it's—we just have a very diversified business from an ads perspective. So no one vertical, whether that be politics, is going to drive the business. ***But I think on an engagement side we are really excited about what we are seeing. And Dan, (multiple speakers) you work with a lot of the public figures.***

Rose followed up by reinforcing the significance of the 2016 election to Facebook:¹⁸¹

Yes, it's interesting, there's no question that this election cycle, the candidates have really

¹⁸⁰ Facebook Inc. at Morgan Stanley Tech., Media & Telecom Conference Tr. at 8 (Mar. 02, 2016).

¹⁸¹ *Id.*

taken to Facebook as a way to reach their constituents. It's also the case that outside of the US this has been happening for a while. And even in the last cycle Obama was famously very social media savvy and used social media better than his opponents.

F. Facebook, the Trump Campaign, and Cambridge Analytica Get to Work on the 2016 Presidential Election

1. Cambridge Analytica Continues to Model and Work with the Misappropriated Facebook Data, Admitting in Internal Documents that the 30 Million Users' Data Were the Key Ingredient of Its Secret Sauce—Psychographic Scoring

183. Because Facebook did not check whether Cambridge Analytica deleted the data it had improperly received, Cambridge Analytica simply kept the data and was able to continue working with it. Indeed, Facebook knew or should have known that Cambridge Analytica—a known “bad actor”—was not likely to simply delete highly valuable data that took nearly an entire year for Cambridge Analytica to harvest.

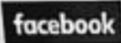


184. Thus, Cambridge Analytica simply carried on using the stolen data. According to accounts from Kaiser, a whistleblower and Cambridge Analytica's former Director of Business Development, Kaiser provided testimony to U.K. officials investigating the Cambridge Analytica scandal: “In March 2016 . . . I had an email from one of our senior data scientists responding to a question that said that we were actually using Facebook-like data in our modelling.”¹⁸² Kaiser's written testimony states that she

¹⁸² Kaiser U.K. Test. at Q1597.

“found another email dating from March 2016 in which another of our senior data scientists confirmed in writing that we were using some *Facebook likes for modeling*, two months after we confirmed that these data were deleted.”¹⁸³

185. On or about April 20, 2016, Cambridge Analytica—likely Tayler or Nix—made a presentation to a client titled: “Data-Driven Political Campaigning: Winning in 2016.” Kaiser shared images of this document in a documentary about the Cambridge Analytica matter, titled *The Great Hack*. In one slide, Cambridge Analytica touts “Our Data Makes Us Different,” which includes several data sources, including these three sources, which Cambridge Analytica presented on the “Our Data Makes Us Different” page of its presentation:

Of all the data Cambridge Analytica possessed, only one data

	Facebook Social Network (Graph Database Containing 30M Individuals)
	Facebook Likes (570 Data Points For 30M Individuals)
	Psychographic Inventories (10 Data Points For 30M Individuals)

source contained exactly 30 million users’ “likes”—namely, Facebook. The fact that Facebook transferred, on average, 570 “likes” per user shows Facebook transferred approximately **17.1 billion** “likes” to the Quiz App,

¹⁸³ Kaiser Stmt. at 6.

for sale to Cambridge Analytica. Those 30 million individuals' Facebook data precisely match the number of "Psychographic Inventories" that Cambridge Analytica was still using. In other words, Cambridge Analytica kept using the misappropriated data.

186. These facts—showing an exact 30-million-person match between the Facebook "likes" and "social graph" (*i.e.*, a data graph of each users' Facebook friends network) with the psychographic inventories—show that Cambridge Analytica lied to Facebook that it had merely received "psychographic scoring" from GSR. It also obviously received Facebook "likes" data. This also shows that Cambridge Analytica was still using the Facebook data, which took it a year to amass in three separate waves and which underpinned its commercial value.

187. Over the March-May 2016 period, Cambridge Analytica courted the Trump campaign as a client as the Cruz primary campaign wound down. Around that same time, Zuckerberg and Sandberg invited approximately 12 prominent conservative leaders to meet with them at Facebook's headquarters in Menlo Park.

2. Zuckerberg and Sandberg Instruct Facebook's Senior Policy/Political Ad Sales Executives to Set Up a Meeting with Prominent Conservatives

188. Zuckerberg and Sandberg followed the 2016 presidential campaign closely and, in May 2016, instructed their political team in Washington DC to strengthen Facebook's relationship with conservative causes. Facebook's Vice President of Public Policy, Joel Kaplan ("Kaplan"), "tapped a small team of Republicans, including [Katie] Harbath, to organize a visit for prominent conservatives" (about 12 total) with Zuckerberg and

Sandberg and other senior Facebook executives at the company’s headquarters.¹⁸⁴ Kaplan was part of “an elite group” of senior executives at Facebook, and had strong ties to Sandberg and reported to Schrage.¹⁸⁵ Harbath reported to Kaplan.

189. Kaplan and Harbath set up the meetings among Zuckerberg, Sandberg and prominent conservatives for May 18, 2016. The point of the meetings was to assure conservative voices that Facebook took their concerns about political bias seriously.

190. At a conference that Sandberg later attended with Kaplan in Washington DC, Sandberg explained that the May 18, 2016 meetings at the company’s headquarters were broader than just one issue. Among other things, the meeting attendees talked about how they were using Facebook “to get their voice out.”¹⁸⁶ Sandberg said “this really matters to us—it is a political time—and we’re proud of the role we play in elections.”¹⁸⁷ A senior Trump campaign official, Barry Bennett (“Bennett”), attended

¹⁸⁴ Craig Timberg, *How conservatives learned to wield power inside Facebook*, Wash. Post (Feb. 20, 2020).

¹⁸⁵ Taylor Hatmaker, *Facebook has other ties to Definers, the GOP-led opposition research group*, TechCrunch (Nov. 16, 2018) (“Having attended Harvard together, Kaplan and Sandberg are close. At Facebook, Kaplan reported to Communications and Public Policy VP Elliot Schrage . . . Schrage reported to Sandberg, though Kaplan was often looped into high-level decision making as well as part of ‘an elite group’ of senior executives at the company.”).

¹⁸⁶ *Facebook and Technological Innovation*, AEI Institute, C-SPAN (June 22, 2016) at 5:30-5:40 (Joel Kaplan in attendance).

¹⁸⁷ *Id.*

the May 18, 2016 meetings, where Facebook senior executives offered the Trump campaign special training.¹⁸⁸ Bennett had previously served as the manager of Ben Carson’s campaign while that campaign employed Cambridge Analytica. Bennett remarked a day after the May 18, 2016 meetings: “Great meeting & first step at Facebook today. Facebook is committed to being an open platform for all political views. More work to be done!”¹⁸⁹

191. Kaplan and Harbath attended the May 18, 2016 meetings. Harbath was “the director over dedicated Democratic and Republican teams” that supported elections at the time by selling them ads and providing other services.¹⁹⁰ Facebook had “dedicated” partisan teams at the time. Harbath explains why: “[political clients] want somebody who understands how they do politics on their side, understands the background, and in some ways, is one of them.”¹⁹¹ Thus, Facebook had (colloquially) a “Democrat team” and a “Republican team.” The Republican team—which included Harbath and at least two other, more junior people supporting Harbath (“FB1” and

¹⁸⁸ Alex Johnson & Matthew DeLuca, *Facebook’s Mark Zuckerberg Meets Conservatives Amid ‘Trending’ Furor*, NBC News (Mar. 18, 2016).

¹⁸⁹ *Id.*

¹⁹⁰ Daniel Kreiss & Shannon C. McGregor, *Technology Firms Shape Political Communication: The Work of Microsoft, Facebook, Twitter, and Google With Campaigns During the 2016 U.S. Presidential Cycle*, *Journal of Political Communication* (Oct. 26, 2017) at 162.

¹⁹¹ *Id.*

James Barnes)—regularly met with Cambridge Analytica’s representatives to discuss business opportunities on behalf of Facebook.¹⁹²

192. Shortly after the May 18, 2016 meetings between Facebook’s senior management and prominent conservatives—wherein Zuckerberg, Sandberg and Kaplan offered special training to the meeting attendees—Facebook’s Republican team met with Cambridge Analytica about the Trump campaign.¹⁹³ Facebook would ultimately extend a number of benefits to the Cambridge Analytica data team—led by Cambridge Analytica data scientists Matt Oczkowski and Molly Schweickert—as they got to work on the Trump campaign.

3. Facebook Learns that Cambridge Analytica Lied About Deleting Facebook Data

193. On June 11, 2016, Facebook learned new facts about the Facebook-labelled “certification of deletion”

¹⁹² Kaiser first met Harbath in 2015, and met with Facebook’s Republican team from time to time thereafter. Facebook’s team would meet Cambridge Analytica’s team offsite at that company’s Washington DC (or, previously, Alexandria, VA offices) or via telephone or at conferences. Facebook’s Republican team would also interact regularly with one of Cambridge Analytica’s top data scientists, Molly Schweickert. James Barnes (“Barnes”) was one of three or more Facebook employees whom Facebook embedded inside the Trump campaign’s digital operations in San Antonio, Texas. Barnes has since provided a number of public interviews. It appears as though “FB1” has not provided any public interviews about Cambridge Analytica, so “FB1” is anonymized herein.

¹⁹³ Kaiser shared these facts in remarking about questions that a senator had posed to Mark Zuckerberg; the questions focused on whether Facebook employees were involved in the Trump campaign *with* Cambridge Analytica. Kaiser stated: “Yes we were, *the [Facebook] republican team in D.C. was*, I met them.” *The Great Hack* (The Othrs 2019) at 1:01:56.

that Cambridge Analytica (Nix/Tayler) had completed in January 2016. On June 11, 2016, GSR and Kogan provided new certifications to Facebook showing that Cambridge Analytica’s January 2016 certification was necessarily false.¹⁹⁴

194. These new June 11, 2016 certifications disclosed to Facebook the App ID of the Quiz App and certified that the Quiz App took information sufficient to personally identify those who installed the app,¹⁹⁵ including these data: “[n]ame, gender, location, birthdate, page likes, friends list, each friend’s name, each friend’s gender, each friend’s location, each friend’s birthdate, each friend’s page likes.”¹⁹⁶ But GSR and Kogan transferred more data in addition to these so-called “raw” data.

195. On June 11, 2016, GSR and Kogan also confirmed that they had modelled Facebook users’ data to create

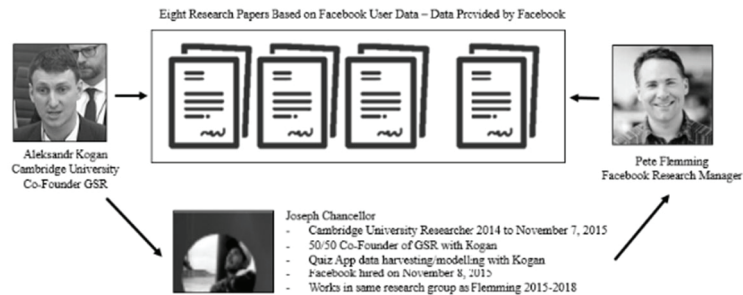
¹⁹⁴ See Facebook, Responses to U.S. Senate Committee on the Judiciary, Questions for the Record addressed Chairman Grassley (June 8, 2018) at 126 (“On June 11, 2016, Kogan executed and provided to Facebook signed certifications of deletion on behalf of himself and GSR. The certifications also purported to identify all of the individuals and entities that had received data from GSR (in addition to Kogan and his lab), listing the following: SCL” and others.); see also Stimson Letter at 29, 33 of 40 (June 11, 2016 Certs. and June 24, 2016 Settlement Agr. attachments) (showing “6/11/2016” execution dates).

¹⁹⁵ Kogan and Facebook apparently overlooked the fact that Kogan also collected Facebook User IDs, but this omission would have been an insignificant oversight at the time because Facebook could just look up all the data that the Quiz App took with the App ID—Facebook knew he took those identification numbers. This omission is curious on the part of Facebook, however, because the Facebook user identification numbers were the data points that a third party, like a government investigator, would need to trace the data set back to Facebook itself.

¹⁹⁶ Stimson Letter at 24 of 40.

psychographic scores (*i.e.*, “predicted survey responses”) from the “likes” of the app installer and their Facebook friends. GSR and Kogan certified that they had also modelled correlations among demographic groups and “likes” for the purpose of giving the modelled results (and the model) to SCL Elections Limited, a U.K. company (Nix was SCL’s CEO).

196. On June 11, 2016, GSR and Kogan further certified that SCL had paid GSR £750,000 for the Facebook app data.



GSR and Kogan also confirmed at the time that Kogan wrote eight research papers in collaboration *with* Facebook’s research group based on user data provided *by* Facebook. Kogan told reporters that he had worked on at least ten papers with Pete Fleming from Facebook’s research group. Fleming and Chancellor worked for Facebook in June 2016:

These disclosures about Chancellor are important because they gave Facebook’s investigation team access to detailed facts about the purpose and nature of the Facebook “likes” data and modeling that they sold to Cam-

bridge Analytica via SCL and Nix. Facebook’s investigation team learned that Cambridge Analytica was still using that model, in violation of Facebook’s stated policies.¹⁹⁷

197. Kogan and GSR’s June 11, 2016 certification also confirmed that Facebook had reviewed and approved a paper about “donations” that rested on the data that he and Chancellor had harvested via the Quiz App. GSR and Kogan told Facebook that it “was *prepared* with a graduate student” in Kogan’s lab “*and members* (current and former) of the Protect and Care team *at Facebook*.” “The paper has previously been reviewed and approved by Facebook’s internal review team,” as GSR disclosed. Kogan’s graduate student, Rui Sun, had previously presented this paper at Cambridge University while on a panel with Kogan and Chancellor.¹⁹⁸ The paper was part of Sun’s dissertation; in the dissertation, she referenced a number of current and former “labmates” that included “Joseph Chancellor,” though she did not credit Chancellor as having substantive input on the research.¹⁹⁹ In sum, Facebook’s own employees had input into a paper that

¹⁹⁷ See, e.g., ¶177 (Facebook investigation teammate admitting that Cambridge Analytica’s receipt of any *derivative* data, such as the modeled “personality score data from Dr. Kogan that *was derived from* Facebook data” violated Facebook’s publicly stated platform policies); see also ¶118 (Kogan and Chancellor’s company (GSR) contract with Cambridge Analytica affiliate (SCL), proving the Facebook data were core inputs to the model and its outputs); see also §IV.I.1.c.-d. (adducing additional evidence of Cambridge Analytica’s continued misuse of the misappropriated “likes” model).

¹⁹⁸ Stimson Letter at 31 of 40 (June 11, 2016 Certs. and June 24, 2016 Settlement Agr. attachments).

¹⁹⁹ Rui Sun, Dissertation: *Be Rich or Be Good: The Interaction Between Prosociality and Socioeconomic Status in Predicting Personal Benefits*, University of Cambridge, Department of Psychology, King’s College (Feb. 2020).

Kogan’s grad student write a paper that rested, in part, on the data that GSR had misappropriated and sold to Cambridge Analytica.

198. On June 11, 2016, Kogan also certified that he transferred to Nix—CEO of Cambridge Analytica and SCL Elections—the “likes” for 30,000,000 Facebook users and facts sufficient to identify those users personally—*i.e.*, unique Facebook profiles:

Name	Contact Information	Number of unique Facebook, and Specific Data Points Shared
SCL	Alexander Ashburner Nix	Approximately 30 million people. Shared forecasted survey responses (derived from page likes) and some limited profile data (such as name, location, birthday, and whether an individual had liked any of a limited list of specific Facebook pages)

199. Faced with the above evidence, Facebook’s investigation team unequivocally knew or willfully blinded themselves to the fact that Cambridge Analytica had made material factual misrepresentations in support of its so-called “certification” of deletion of January 2016.

a. Facebook Knew by June 11, 2016 that Cambridge Analytica Had Misrepresented Its Use of the Data at Issue

200. Facebook learned on June 11, 2016 that Cambridge Analytica had misled Facebook’s investigation team about the kind of Facebook data that it purchased from GSR. On December 15, 2015, Cambridge Analytica

represented to Facebook that it had “subcontracted the research phase of the psychographic data project to GSR, who provided us with an append to our voter file containing the **psychographic scoring**.” A few days later, Facebook spoke with Cambridge Analytica about the sources of the psychographics, and memorialized, again, that the psychographics rested on Kogan’s stolen data: “You have told us that you received **personality score data** from Dr. Kogan that was derived from Facebook data,” in violation of Facebook’s policies.²⁰⁰ These factual certifications to Facebook’s investigation officials were both misleading, as Facebook discovered on June 11, 2016. Per Kogan and GSR’s certifications, GSR provided to Cambridge Analytica (via Nix/SCL) not only the psychographic data (“personality scores”) but also everything else that Facebook sent to GSR, including **30 million users’ “likes,”** as well as names and other personally identifiable information—far more than just psychographic scores. In other words, Cambridge Analytica’s claim that it merely purchased “personality scores” was fraudulent, as Facebook learned on June 11, 2016.

b. Facebook Knew that Cambridge Analytica Had Misrepresented Its Funding Role

201. Facebook’s June 11, 2016 discovery of Cambridge Analytica’s data destruction “certification” fraud extended beyond the data itself. Cambridge Analytica’s representations in support of its January 2016 “certification” of deletion included these additional representations: “Cambridge Analytica **did not fund** the development of Dr. Kogan’s app” and “**did not pay GSR** for their time or technology, but rather paid the third-party (*e.g.*,

²⁰⁰ See Jan. 2020 *TechCrunch* article.

survey vendor) costs for the surveys they ran.”²⁰¹ This was false and Facebook knew it. In fact, GSR’s formal certification of June 11, 2016 provided *to Facebook* showed that Cambridge Analytica (via Nix/SCL) had paid the costs of developing the Quiz App and running it—“£750,000” directly to GSR.²⁰² Facebook had previously discovered that GSR had—in the words of Facebook’s top security official—“enticed several hundred thousand individuals to use Facebook to login to his personality quiz” but that GSR “lied to those users” to get them to login.²⁰³ Cambridge Analytica (via Nix/SCL) funded the data extraction and user “lie[s],” as Facebook discovered on June 11, 2016. That discovery further demonstrated to Facebook that Cambridge Analytica’s January 2016 “certification” of destruction was a fraud.

c. Facebook Knew that Cambridge Analytica Had Misrepresented the Data’s Value

202. On June 11, 2016, Facebook’s Cambridge Analytica investigation team discovered other fraudulent aspects of Cambridge Analytica’s December 2015/January 2016 “certification” of data destruction. Cambridge Analytica stated at the time that “the model we received from Dr. Kogan wasn’t very accurate,” implying that it would never use “the model” that was supposedly the only thing it ever received from Kogan.²⁰⁴ That, too, was false. Facebook’s investigation team knew that GSR (Kogan and

²⁰¹ Jan. 2020 *TechCrunch* article.

²⁰² Stimson Letter at 26 of 40 (June 11, 2016 Certs. and June 24, 2016 Settlement Agr. attachments).

²⁰³ Kurt Wagner, *Here are the New York Times and Observer stories that pushed Facebook to suspend Trump’s data analytics company*, N.Y. Times (Mar. 17, 2018).

²⁰⁴ Jan. 2020 *TechCrunch* article.

Chancellor) had pulled the 30 million users' 17.1 billion "likes" in three waves: May 2014 (the "rejection overruled" wave); June-July 2014 (the "throttled" wave); May 2015 (the "whitelisting" wave). The fact that Cambridge Analytica propagated three harvesting waves demonstrated that everything GSR provided to Cambridge Analytica (via Nix/SCL) was "accurate" enough for commercial purposes, which is why GSR was paid £750,000 to harvest the three waves of data, build the model, model the data, and sell it all to Cambridge Analytica (via Nix/SCL).

The £750,000 payment and three collection waves belie Cambridge Analytica's contrary assertions in the "certification" provided on January 18, 2016. And Facebook's own employee, Chancellor, no doubt informed Facebook's investigation team that he and Kogan had accurately replicated the Facebook "likes" model that was one of the key goals of the data harvest. §§IV.D.6.-7.; §IV.E.3.

4. Facebook Senior Management Learns that Cambridge Analytica's January 18, 2016 "Certification" of Deletion Was False

203. Additional facts demonstrate that Zuckerberg, Sandberg and the 28 other executives who were apprised of Facebook's Cambridge Analytica investigation knew about the June 11, 2016 revelations showing Cambridge Analytica's January 2016 certification of deletion was fraudulent—and that, therefore, Facebook's investigation team could not believe it was true.

204. Facebook learned that the January 18, 2016 "certification" from Cambridge Analytica was not accurate no later than **June 11, 2016**—the day that Facebook received the Kogan/GSR certifications. Those certifications and

others prompted discussions by Facebook senior management, as reflected in Senate testimony:²⁰⁵

Harris: . . . So my question is, did anyone at Facebook have a conversation at the time that you became aware of this breach, and have a conversation where in the decision was made not to contact the users?

Zuckerberg: Senator, I don't know if there were any conversations at Facebook overall because I wasn't in *a lot* of them. But . . .

Zuckerberg's testimony shows that there were discussions at Facebook about the Cambridge Analytica breach and whether to notify the affected user and, indeed that he was involved in at least "some" of those discussions. Senator Harris asked several follow-up questions:²⁰⁶

Harris: And I've heard your testimony in that regard, but I'm talking about notification of the users. And this relates to the issue of transparency and the relationship (ph) of trust, informing the user about what you know in terms of how their personal information has been misused.

And I'm also concerned that when you personally became aware of this, did you or senior leadership do an inquiry to find out who at Facebook had this information, and did they not have a discussion about whether or not the users should be informed ***back in December 2015?***

Zuckerberg: Senator, in retrospect, I think we clearly viewed it as a mistake that we didn't inform people and we did that ***based on false information***

²⁰⁵ Committee Hearing Transcript at 63.

²⁰⁶ *Id.*

that we thought that the case was closed and that the data had been deleted.

Harris: So there was a decision made *on that basis* not to inform the users. Is that correct?

Zuckerberg: That's my understanding. Yes.

Zuckerberg elaborated:²⁰⁷

Zuckerberg: When we learned *in 2015* that Cambridge Analytica had bought data from an app developer on Facebook that people had shared it with, we did take action.

We took down the app, and *we demanded* that both the app developer *and Cambridge Analytica* delete and stop using any data that they had. *They told us that they did this*. In retrospect, it was clearly a mistake to believe them. . . .

Nelson: Yes.

Zuckerberg: . . . and we should have followed up and done a full audit then. And that is not a mistake that we will make.

Nelson: Yes, you did that, and you apologized for it. But you didn't notify them. And do you think that you have an ethical obligation to notify 87 million Facebook users?

Zuckerberg: Senator, *when we heard back from Cambridge Analytica* that they had told us that they weren't using the data and had deleted it, we considered it a closed case. In retrospect, that was clearly a mistake.

²⁰⁷ *Id.* at 10.

We shouldn't have taken their word for it, and we've updated our policies and how we're going to operate the company to make sure that we don't make that mistake again.

205. Facebook and Zuckerberg later responded to follow-up questions from the Senate in writing after Zuckerberg's live testimony. They provided the date of Cambridge Analytica's data destruction certification, which they now described as a written assurance.²⁰⁸

Why did Facebook wait until eight months after *The Guardian's* report about Cambridge Analytica to send a letter asking for certification that the data was deleted?

Facebook did not wait until eight months after *The Guardian's* report about Cambridge Analytica to seek assurance that the data was deleted. Facebook contacted Cambridge Analytica the day the article was released. About one month later, on **January 18, 2016**, ***Cambridge Analytica assured Facebook in writing*** that it had deleted ***the data*** received from Kogan/GSR and that their server contained no backups of the data.

Facebook then wrote to the U.S. Senate about the importance of the January 18, 2016 certification from Cambridge Analytica; here, a confirmation or certification:

Facebook knew about Cambridge Analytica in 2015, when Facebook banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook ***considered the matter***

²⁰⁸ Facebook, Responses to U.S. Senate Committee on the Judiciary, Questions for the Record addressed Chairman Grassley (June 8, 2018) at 6.

closed after obtaining *written* certifications and confirmations from Kogan [June 11, 2016], GSR [June 11, 2016], Cambridge Analytica [January 18, 2016], and SCL [April 3, 2017 (2017, not 2016 or 2015)] declaring that all such data they had obtained was accounted for and destroyed.

206. These answers show the case was first “closed” as to Cambridge Analytica on January 18, 2016 (the date of the only written confirmation (or assurance or certification) that Facebook ever received from “Cambridge Analytica); yet, the case was not closed as to GSR/Kogan until June 11, 2016. The GSR/Kogan June 11, 2016 certifications re-opened the case as to Cambridge Analytica, because those “certifications” demonstrated to Facebook that Cambridge Analytica’s January 18, 2016 written confirmation rested on false statements that GSR only gave Cambridge Analytica “personality scores,” which was a lie that Facebook uncovered on June 11, 2016.

207. Yet Facebook wrote to the Senate:²⁰⁹

We did *not have any reason* to affirmatively question *the veracity* of any of these certifications *until* March 2018, when we learned that *questions had been raised* concerning the accuracy of the certifications. Moreover, while Facebook’s policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan’s app’s access to Facebook (and there was no intention of considering its reinstatement). Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future.

²⁰⁹ *Id.* at 9.

208. That answer was false. The June 11, 2016 GSR/Kogan certifications demonstrated, to Facebook, that Cambridge Analytica made misleading statements in its January 18, 2016 certification—and, as a result, Facebook could not and did not believe that certification was true as of June 11, 2016.

5. One Day After “Brexit,” Facebook Forces GSR and Kogan Not to Disclose the Facts that Revealed Cambridge Analytica’s Certification to Be a Fraud—and Threatens Him with Liquidated Damages Plus “Reasonable” Fees and Costs If He Does Disclose the Truth

209. On June 22, 2016, Sandberg and Kaplan were in Washington DC discussing global politics that included issues relating to the EU.²¹⁰ Facebook’s investigation into Cambridge Analytica had uncovered the fact that Cambridge Analytica was working for an advocacy group that favored the U.K. leaving the EU in the “Brexit” referendum.²¹¹

²¹⁰ *Facebook and Technological Innovation*, AEI Institute, C-SPAN (June 22, 2016) at 17:26-17:44 (Sandberg noted that the team was “talking to policymakers” and members of Congress about policy issues that were important to Facebook and noted that “one of the big open issues right now is the transfer of data from the EU to the US.”).

²¹¹ See, e.g., Robert Booth, *EU referendum: Grassroots Out brings ‘a hint of the Trump’ to middle England*, Guardian (Feb. 15, 2016) ([Brexit advocacy group] GO! is bidding to be designated by the Electoral Commission as the official leave campaign, which would allow it to raise up to £7m in total. US political consultants, originally hired by Leave.EU, have been placed at GO!’s disposal, including some from **Cambridge Analytica**, who work for Ted Cruz, the Republican presidential candidate and Goddard Gunster, Washington-based referenda experts.); Paul Gallagher, *EU referendum: Controversial Leave.EU co-founder Arron Banks on why he’s happy to put noses*

210. On June 23, 2016, U.K. citizens voted to leave the EU—this news headlined major media:

The screenshot shows the front page of The Washington Post. The main headline reads "Britain braces for Brexit as strong 'leave' results pour in". Below the headline, there is a sub-headline: "While voters from much of the country have yet to be counted, the count showed a stunningly large percentage of Britons in favor of leaving the E.U., which would have economic, political and security implications around the globe." The byline is "By Jeff Klauz, Kara Adam and Dan Baz" and it is dated "24 minutes ago". There are two images: one showing a group of people and another showing a man's face. A video player is visible on the right side of the article.

211. The results were clear by the end of the (U.S.) day on June 23, 2016:

The screenshot shows the front page of The Wall Street Journal. The main headline reads "The U.K. Votes to Leave European Union". Below the headline, there is a sub-headline: "Live Results and Market Reaction". A progress bar shows "352 VOTING AREAS REPORTING (100%)". The bar is divided into "Remain" (50%) and "Leave" (50%). To the right, there is a section titled "Markets" with a table of market data.

	U.S.	EUROPE	ASIA	FX	RATES	FUTURES
DIA	1808.27	330.24	1.29%			
S&P 500	2113.32	27.87	1.34%			
Nasdaq	4910.04	76.72	1.59%			
Russel 2000	1772.22	23.25	2.02%			

212. Facebook scrambled to prevent Kogan and GSR from talking to the media about their involvement in the Brexit vote.

213. On June 24, 2016, Facebook required Kogan and GSR to sign a new document, in addition to the two certifications that he signed on June 11, 2016. The June 24,

out of joint, The Independent (Dec. 7, 2015) (“**Cambridge Analytica**, a data-modelling firm that employs ‘psychographic profiling’ and who US Republican presidential hopeful Ted Cruz recently spent \$750,000 on, has helped boost Leave. EU’s social media campaign.”); Sam Burne James, *Leave.EU campaign brings in US voter data and messaging firm Cambridge Analytica*, PR Week (Nov. 18, 2015) (“Late last month [Leave.EU] also took on board Cambridge Analytica, a Washington DC, New York and London-based firm specialising in data and behaviour-driven work on elections. It is currently working with a number of Republican US presidential candidates.”).

2016 document was a settlement agreement that forced Kogan and GSR to hold in “strict confidence” the fact that they had transferred 30,000,000 “likes” and personally identifiable information to Cambridge Analytica (via Nix/SCL).²¹² Facebook included a \$25,000 liquidated damages provision in the agreement, tied to the “strict confidence” provision.²¹³ But the liquidated damages were small compared to another provision that Facebook required Kogan and GSR to sign, requiring them to pay all of Facebook’s “reasonable” legal fees and costs if they ever disclosed the truth to third parties like *The Guardian*.

214. Facebook further required Kogan and GSR to tell Nix and SCL Elections that **they** had to complete the same “CERTIFICATION” that Kogan and GSR completed, and that it “shall be completed within fourteen business (14) business days following receipt.”²¹⁴ But Nix—Cambridge Analytica’s CEO—and SCL Elections Limited (whose CEO was Nix) refused to sign any such

²¹² See Stimson Letter at 03 of 40 (responding to question five, “a formal agreement was signed by Dr. Kogan on 24 June 2016 . . . [a] copy of the agreement is enclosed”); see also *id.* at 21 of 40 (Settlement Agreement at §II.D.1).

²¹³ *Id.* at 21 of 40 (June 11, 2016 Certs. and June 24, 2016 Settlement Agr. attachments) (III.B).

²¹⁴ *Id.* at 20 of 40 (II.A.4); *id.* at 22 of 40 (III.B) (liquidated damages) or by Wednesday July 27, 2016 at the latest. Kogan sent the form of Certification (the Exhibit B’s) out no later than July 7, 2016—one of the data transferees he identified (a University of Toronto researcher) signed it on that date, and Facebook gave it to the U.K. government, showing Kogan did what Facebook required him to do with the notices no later than July 7, 2016, though he more likely sent them out on June 24th. From the later July 7, 2016 “start date,” the Cambridge affiliates were on notice that Facebook required them to Certify, in writing, no later than Wednesday, July 27, 2016, but Cambridge defaulted.

“certifications” while they continued to abuse the purloined data to support the Trump campaign.

6. The “Ugly Truth” Was It Did Not Matter to Facebook that Cambridge Analytica’s Deletion Certification Was Fraudulent—Cambridge Analytica Was a “Marketing Partner” with a Huge Ad Budget from the Trump Campaign

215. Andrew Bosworth (“Bosworth”) was one of the 30 Facebook executives who knew about Facebook’s Cambridge Analytica investigation. He was the VP of Ads during the relevant time, reporting either to Zuckerberg, to Sandberg or to both of them.

216. Bosworth wrote an internal memorandum in 2020 to all employees that was “accidentally” leaked to the press a few days after internal publication. The internal post shows Facebook not only declined to “ban” Cambridge Analytica after discovering its certification fraud on June 11, 2016, but actually chose to let Cambridge Analytica stay within its elite group of “Facebook Marketing Partner[s] . . . , who other companies could hire to run their ads.”²¹⁵

217. Bosworth’s colleague, Rose, ran the FMP program, while reporting to Sandberg.²¹⁶ Facebook had pre-

²¹⁵ *Lord of the Rings, 2020 and Stuffed Oreos: Read the Andrew Bosworth Memo*, N.Y. Times (Jan. 7, 2020)

²¹⁶ Dawn C. Chmielewski, *Dan Rose, Facebook Executive Overseeing Partnerships, Is Leaving The Company*, Deadline (Aug. 22, 2018) (Rose, “[t]he 12-year Facebook veteran reports directly to COO Sheryl Sandberg, and oversees all of the social network’s partnerships—including its high-profile deal with the NFL to live-stream

viously called FMPs the “Preferred Marketing Developers.” That designation “described as the world’s most important social media marketing collective and certification program rolled into one.”²¹⁷ “Facebook grants certain privileges to PMDs, allowing them to collect analytics and serve ads into the social network with the latest and most advanced tools. Facebook often consults PMDs on “product plans”—they “have as close as it gets to an inside view on Facebook marketing.”²¹⁸ Facebook created the program “to help businesses scale their marketing efforts on Facebook,” with participants required to “meet or exceed Facebook partner standards.”²¹⁹ Industry publications reported that there were only 12 companies like Cambridge Analytica that had been “awarded the media buying badge.”²²⁰

games.”); *Lord of the Rings, 2020 and Stuffed Oreos: Read the Andrew Bosworth Memo*, N.Y. Times (Jan. 7, 2020) (Quoting from a largely self-serving internal memo from “Andrew Bosworth, a long-time Facebook executive and confidant of Mark Zuckerberg” that Bosworth published to the entire company on an internal network, after Rose left Facebook: “The company Cambridge Analytica started by running surveys on Facebook to get information about people. It later pivoted to be an advertising company, part of our Facebook Marketing Partner program [during the 2016 campaign season], who other companies could hire to run their ads. Their claim to fame was psychographic targeting.”).

²¹⁷ Cooper Smith, *Facebook Has A Program That Gives Special Access To Elite Marketers—These Are Their Insights*, Business Insider, Australia (Mar. 12, 2014).

²¹⁸ *Id.*

²¹⁹ *Making it Easier to Find the Right Partners: Updates to the Facebook PMD Program*, Facebook for Business (Oct. 22, 2014).

²²⁰ Tim Peterson, *Social Media Marketing: Facebook is eliminating its Marketing Partners program’s media buying specialty, which will remove four agencies from the program*, Marketing Land (Nov. 21, 2016).

218. Bosworth knew about Facebook’s investigation into Cambridge Analytica as he wrote that Cambridge Analytica “certified to us *in writing* that they had” deleted the data in December 2015/January 2016.²²¹

219. In his self-exculpatory “leaked” retrospective company-wide internal communication in 2020, which he wrote as the media continued raising questions about Facebook’s role in the 2016 election, Bosworth suggested that he personally believed, in 2016, that Cambridge Analytica’s “psychographic targeting” was “snake oil.” But Cambridge Analytica had admitted to Facebook that one of the key ingredients to this so-called snake oil was the stolen data; and, as of June 11, 2016, Bosworth and everyone else on Facebook’s investigation team had a compelling reason to believe, and did believe, that Cambridge Analytica had previously submitted a phony “certification” so that it could keep using the data that it spent about a year and £750,000 harvesting from Facebook’s servers.

220. On June 18, 2016, Bosworth wrote a company-wide memorandum that more accurately reflects the context in which Bosworth and the rest of Facebook’s investigation team let Cambridge Analytica stay in its preferred marketing program, despite its privacy violations:²²²

²²¹ *Lord of the Rings, 2020 and Stuffed Oreos: Read the Andrew Bosworth Memo*, N.Y. Times (Jan. 7, 2020)

²²² Ryan Mac, Charlie Warzel & Alex Kantrowitz, *Growth At Any Cost: Top Facebook Executive Defended Data Collection In 2016 Memo—And Warned That Facebook Could Get People Killed*, BuzzFeed (Mar. 28, 2018).

Andrew Bosworth
 June 18, 2016

The Ugly

We talk about the good and the bad of our work often. I want to talk about the ugly.

We connect people.

That can be good if they make it positive. Maybe someone finds love. Maybe it even saves the life of someone on the brink of suicide.

So we connect more people

That can be bad if they make it negative. Maybe it costs a life by exposing someone to bullies. Maybe someone dies in a terrorist attack coordinated on our tools.

And still we connect people.

The ugly truth is that we believe in connecting people so deeply that anything that allows us to connect more people more often is "de facto" good. It is perhaps the only area where the metrics do tell the true story as far as we are concerned.

That isn't something we are doing for ourselves. Or for our stock price (ha!). It is literally just what we do. We connect people. Period.

That's why all the work we do in growth is justified. All the questionable contact importing practices. All the subtle language that helps people stay searchable by friends. All of the work we do to bring more communication in. The work we will likely have to do in China some day. All of it.

221. This real-time account of Facebook's growth mentality is telling. Bosworth wrote this post a few days after being put on notice—as part of Facebook's Cambridge Analytica investigation team who was privy to the certification process—that the certification was a fraud.²²³

²²³ *Id.*

I know a lot of people don't want to hear this. Most of us have the luxury of working in the warm glow of building products consumers love. But make no mistake, growth tactics are how we got here. If you joined the company because it is doing great work, that's why we get to do that great work. We do have great products but we still wouldn't be half our size without pushing the envelope on growth. Nothing makes Facebook as valuable as having your friends on it, and no product decisions have gotten as many friends on as the ones made in growth. Not photo tagging. Not news feed. Not messenger. Nothing.

In almost all of our work, we have to answer hard questions about what we believe. We have to justify the metrics and make sure they aren't losing out on a bigger picture. But connecting people. That's our imperative. Because that's what we do. We connect people.

222. Bosworth's statements here go a long way to explaining why Facebook allowed Cambridge Analytica to continue operating on the platform after June 11, 2016. The psychographic "snake oil" that Cambridge Analytica peddled (per Bosworth) was based entirely on 30,000,000 Facebook users' whitelisted, throttled data that Cambridge Analytica bought for £750,000.

223. This data was big business to Facebook as it supported Cambridge Analytica's efforts to drive user engagement around the Trump campaign. Harbath—one of the Facebook executives who worked on the "Republican team" at Facebook and met with Cambridge Analytica's Business Development director (Kaiser) from time to time—said, in 2016, that "US election was the **number one** most talked about topic **globally** on our platform."²²⁴ Sandberg similarly stated that "we're pretty excited about what's happening with the elections organically on Facebook" and that "the 2016 election is a big deal in

²²⁴ Katie Harbath, *Campaigning on Facebook: Lessons from the US and around the world*, Campaigning Summit Europe 2016, YouTube (Mar. 25, 2016) at 2:30-39.

terms of ad spend,” similar to the World Cup, Super Bowl and Olympics.²²⁵ And Zuckerberg noted, in 2016, that “Donald Trump has more fans on Facebook than any other presidential candidate.”²²⁶ Cambridge Analytica—as the Trump campaign’s ad buyer at Facebook—represented a key source of user engagement and ad revenue, ultimately spending between \$75 million and \$85 million in ads.²²⁷

²²⁵ Q4 2015 Facebook Inc. Earnings Call Tr. at 16 (Jan. 27, 2016); see also Q3 2015 Facebook Inc Earnings Call Tr. at 12 (Nov. 04, 2015) (Sandberg noted, with regards to “elections and political activity and political advertising, we’re excited about the elections . . . over 68 million people on Facebook in the US made over 1 billion interactions about the campaign alone . . . [U.S. presidential candidate] Ben Carson ran 240 different ads targeted at different audiences. And so we’re starting to see candidates use our platform to communicate, to advertise and to share.”).

²²⁶ Alex Johnson & Matthew DeLuca, Facebook’s *Mark Zuckerberg Meets Conservatives Amid ‘Trending’ Furor*, NBC News (Mar. 18, 2016).

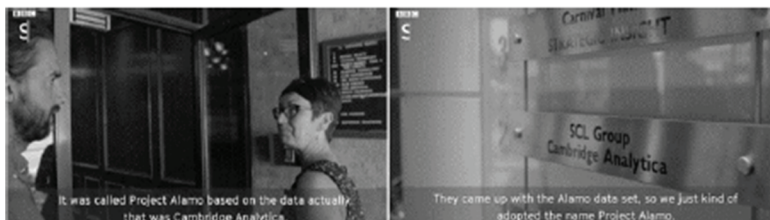
²²⁷ Facebook party admissions state the Trump and Clinton campaigns spent “approximately \$81 million” on Facebook ads, “combined.” Social Media Influence in the 2016 US Elections: Hearing before the S. Rep. Select Comm. on Intelligence, 115th Cong. (Nov. 1, 2017) at 41. A Trump campaign official helps split that figure: the Trump campaign spent approximately \$75 million on Facebook ads (80% of its \$94 million budget). Philip Bump, *‘60 Minutes’ profiles the genius who won Trump’s campaign: Facebook*, Wash Post (Oct. 9, 2017) at 2. Thus, the Clinton campaign spent approximately \$6 million (the \$81 million combined minus the \$75 million Trump share) based on these sources. A U.K. government report states that Project Alamo “spent \$85 million on Facebook adverts.” See House of Commons, Dig., Culture, Media and Sport Comm., *Disinformation and fake news*: Final Report (Feb. 14, 2019) (“U.K. Parliamentary Comm. Final Rep.”) at 40. Both the \$75 million and the \$85 million likely are correct but the \$85 million likely includes Trump super PAC ads that Cambridge Analytica purchased in parallel with Project Alamo.

G. Facebook “Embeds” Its Employees Inside the Center of Cambridge Analytica’s Data Center, Inside the Trump Campaign

1. Facebook’s Political Team “Embeds” Facebook Employees to Work in the Same Room as the Cambridge Analytica Data Team Supporting the Trump Campaign

224. By the end of June 2016, Facebook “embedded” at least three political advertising employees to work alongside Cambridge Analytica, which, in turn, was embedded inside the Trump campaign’s digital operations in San Antonio, Texas. These Facebook employees collaborated with Cambridge Analytica inside of “the center of the data center,” as Trump campaign official Theresa Hong explained to the *BBC*, as she walked a *BBC* reporter and film crew through the office where the data center was set up in June 2016.²²⁸

225. The Facebook employees who were embedded with Cambridge Analytica saw Cambridge Analytica’s name printed on the directory of the location where they would report for work during that time. The operation was named “Project Alamo” by Cambridge Analytica, based upon the Cambridge Analytica dataset:



²²⁸ *The digital guru who helped Donald Trump to the presidency*, BBC News (Aug. 17, 2017) (video shows the room’s size).

226. Hong demonstrated where Facebook’s employees worked when they were embedded with Cambridge Analytica in a small room with “a line of computers” inside of the Cambridge Analytica center that “speciali[zed] in psycho-graphics”:



227. Hong said Facebook sent the embeds to serve as the campaign’s “hands-partners.”

228. Some of the Facebook embeds worked inside of the Cambridge Analytica psychographics data center. Another Trump campaign official (Brad Parscale) told reporters that “we had [Facebook]—their staff embedded inside our offices,” and that “Facebook employees would show up for work every day in our offices”—“sittin[g] right next to us.”²²⁹ Parscale “wanted people who support Donald Trump,” which was feasible because Facebook

²²⁹ Unlike the Facebook embeds, Parscale was not sitting inside of the Cambridge Analytica data center. Brittany Kaiser, *Targeted: The Cambridge Analytica Whistleblower’s Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How it Can Happen Again*, 2019 (Kaiser, “*Targeted*”) (“Parscale had been a longtime website designer for Trump, and Trump had picked him to run his digital operations. The problem was that Parscale had no data science or data-driven communications experience, so Bekah [Mercer] knew that Trump needed Cambridge [Analytica].”).

“already ha[d] divisions set up that way.”²³⁰ Facebook’s executive Harbath agreed with this account, having shared information with researchers that she was “serving as the director over dedicated Democratic and Republican teams” at the time²³¹ and the partisan structure “facilitate[d] working relationships with campaigns.”²³² Harbath shared on social media that the role involved “working in the Facebook DC office leading the team helping elected officials, politicians and governments around the world use Facebook to communicate with constituents/voters.”²³³

229. Cambridge Analytica executive (Kaiser) emailed with one of the senior people from the Cambridge Analytica data team, “which consisted of Matt Oczkowski, Molly Schweickert and a handful of [other] data scientists” at the time, and Kaiser would later provide written confirmation: “*Seated beside* Molly, Matt, and our [other] data scientists were embedded *employees from Facebook*,”²³⁴ consistent with Hong, Parscale and Harbath’s accounts.

²³⁰ Lesley Stahl, *Facebook “embeds,” Russia and the Trump campaign’s secret weapon*, CNBC, 60 Minutes (Oct. 08, 2017).

²³¹ Daniel Kreiss & Shannon C. McGregor, *Technology Firms Shape Political Communication: The Work of Microsoft, Facebook, Twitter, and Google With Campaigns During the 2016 U.S. Presidential Cycle*, *Journal of Political Communication* (Oct. 26, 2017) at 162.

²³² *Id.*

²³³ *Partisan Programming: How Facebook and Google’s Campaign Embeds Benefit Their Bottom Lines*, Campaign for Accountability, Google Transparency Project (Aug. 2018); *Id.*, Appendix A: Google Elections and Politics Employees.

²³⁴ Kaiser, *Targeted*.

2. Facebook Embeds Witnessed Cambridge Analytica Deploying Unique Facebook User Identification Numbers to Target Voters—Showing that Facebook Was the Source of Cambridge Analytica’s Data

230. From June 24, 2016, through the completion of the U.S. presidential election, Facebook’s “embeds” who walked to their work stations inside the Trump-Cambridge Analytica data center were directed to the second floor of the building by this sign in the lobby:



231. The Facebook embeds helped Cambridge Analytica target potential voters by way of an ad tool that Facebook called “Custom Audiences”—this tool enabled advertisers like Cambridge Analytica to target specific segments of a population based upon data that they (the advertisers) already possessed by uploading lists of their targeted customers to Facebook who would send those particular customers the advertisements via the Facebook platform.²³⁵ Cambridge Analytica needed to name

²³⁵ Facebook senior management communicated about the custom audiences tool externally and internally. *See, e.g.*, Q4 2012 Facebook, Inc. Earnings Call Tr. at 5 (Jan. 30, 2013) Sandberg on investor conference call (“As Mark said, one of the products we’re most excited about is **Custom Audiences**, which lets marketers show their ads to exactly the right people . . . [a] large retailer, for example, **can send one set** of ads to customers who typically buy sporting goods, **and a different set of ads** to those who would purchase TV products . . . **some of the best targeting** available . . . [allowing retailers] to **target specific segments** of its customer database.”). Zuckerberg, Sandberg, Rose and others would communicate about the Custom Audi-

the lists and include an “identifier” for each person on the list.²³⁶

232. Cambridge Analytica named its custom audiences—sometimes called universes—by “personality type” thereby alerting Facebook to the fact that it was still using psychographics.²³⁷ Cambridge Analytica also

ences tool internally from time to time. *See, e.g.*, Six4Three Documents, Ex. 184 at FB-101366934 (Facebook internal email among Zuckerberg, Sandberg, Rose and others noting “Custom Audiences or link page posts” drive approximately “(~320B annually)” through a “Consideration” marketing funnel that “is about getting people who know about what you do to want to buy (or buy it sooner)”; *see also* Six4Three Documents, Ex. 40 at FB-00943407 (Facebook internal email among Sandberg and others about, among other things, “news fee and custom audiences” in relation to various market opportunities); *see also* Six4Three Documents, Ex. 27 at FB-01381973 (Facebook internal daily media summary noting: “Earlier this week, Facebook’s new advertising policies raised some privacy concerns. The new Custom Audiences advertising feature allows marketers to target their ad or sponsored story to a specific set of users using phone numbers or email addresses posted on the site. Facebook COO Sheryl Sandberg defended the new feature and stated that ‘we never sell user information, we don’t make money when you share more, and we do not give your information to marketers.’”).

²³⁶ *See, e.g., Use a Customer List to make a Custom Audience*, Facebook for Business (Facebook: “To make a Custom Audience from a customer list, you provide us with information about your existing customers and we match this information with Facebook profiles. The information on a customer list is known as an ‘identifier’ (such as email, phone number, address) and we use it to help you find the audiences you want your ads to reach. . . . Prepare your customer list: Select the identifiers to include, then add the customer list you want to use for your new Custom Audience and give it a name.”).

²³⁷ *See, e.g., SEC Complaint at ¶35* (“As an additional indication to Facebook that Cambridge might have been misusing Facebook user data, some employees on **Facebook’s political advertising team knew** from August 2016 through November 2016 that Cambridge

used Facebook user identification numbers (called “Facebook User IDs” or “UIDs”) that were unique to each psychographic target.²³⁸ This fact is significant because it revealed that the company’s database rested on data that Cambridge Analytica had previously harvested from Facebook itself.

233. The Facebook employees embedded at Cambridge Analytica knew that Cambridge Analytica was still using the improperly accessed Facebook user data. Indeed, the Facebook employees embeds showed campaign personnel and Cambridge staff how to aggregate look-alikes [and] create custom audiences,²³⁹ and because the personality names of the lists and the UIDs were part of

named Facebook and Instagram advertising *audiences by personality trait* for certain clients that included advocacy groups, a commercial enterprise, and a political action committee.”); *see also* Canada Report at ¶26 (“Lists of individuals *based on certain traits* were then used [by Cambridge Analytica] to target political messaging to very specific groups based on those psychological profiles (including by creating ‘custom audiences’ for targeting advertisements on Facebook.”).

²³⁸ One of the Cambridge Analytica data scientists who worked on Project Alamo with the embeds and others at Facebook, Molly Schweitker, admitted this fact at a conference after the election in describing “an integration with the campaign’s database such that we would be able to flag someone that had returned their ballot, we were then connecting attribution *particularly through Facebook*, because since that’s *a person-based ID*, we could then see if someone saw an ad, and, ultimately, the individual associated with *the ad id*—that saw that ad—turned in their ballot.” *See d3Con2017—Molly Schweickert Cambridge Analytica*, Digital Life Design Conference, YouTube (Feb. 26, 2018); *see also* FTC Cambridge Complaint at ¶24 (“the GSRApp collected the Facebook User ID of those users who authorized it . . . [a] Facebook User ID is a persistent, unique identifier that connects individuals to their Facebook profiles”).

²³⁹ Kaiser, *Targeted* at 193-94.

that process, the embeds saw these facts.²⁴⁰ The Facebook User IDs and the custom audiences (named by “personality type”) further tied the Project Alamo data to the data that Cambridge Analytica misappropriated and then misrepresented in its January 2016 “certification” of deletion to Facebook, as Facebook discovered on June 11, 2016.

234. Cambridge Analytica’s “personality” universes and unique Facebook User IDs became increasingly important as Project Alamo entered into its “persuasion” phase starting in July 2016 followed by the “[g]et out the vote” phase closer to election day.²⁴¹

235. A Trump campaign official shed light on what the embeds would have been seeing and hearing (seated next

²⁴⁰ The personality score names and Facebook User ID fields would have been obvious red flags to Facebook that Cambridge Analytica continued using the data that it paid Kogan 750,000 GBP to misappropriate. *See, e.g.*, Facebook, Responses to U.S. Senate Committee on the Judiciary, Questions for the Record addressed Chairman Grassley (June 8, 2018) at 128 (“Cambridge Analytica **used hundreds** of Contact List Custom Audiences during the 2016 election cycle created from contact lists that Cambridge Analytica uploaded to our system, and Cambridge Analytica used those and other custom audiences in the majority of its ads targeting in combination with demographic targeting tools,” like gender and ethnicity). Importantly, Cambridge Analytica only took Facebook User IDs—not emails, phone number or app ids from Facebook—and those were the only fields that Facebook’s embeds and Cambridge Analytica could have used to create the Custom Audiences. *See, e.g.*, (Facebook January 2016 Customer List instructions to use in creating Custom Audiences, showing advertisers can use one of four identifiers: “emails, phone numbers, Facebook user IDs or mobile advertiser IDs”); (Facebook January 2016 Customer List; *see also* (Facebook November 2016 Customer List instructions to use in creating Custom Audiences showing same) (Facebook November 2016 Customer Lists).

²⁴¹ Kaiser, *Targeted* at 193.

to Cambridge Analytica) during this time inside Project Alamo:²⁴²

[BBC Reporter]: Were they [Cambridge Analytica] able to kind of understand people’s personalities?

[Trump Campaign Official Hong]: Yeah, I mean, you know, they do specialize in psychographics, right? But based on personal interests, and based on what they, you know, a person cares for, and what, you know, means something to them, they were able to extract, and then we were able to target.

[BBC Reporter]: So the *psychographic stuff*, were they using that here, was that part of the model that you were working off of?

[Hong]: Well, I mean, toward the end with the persuasion, you know, *absolutely*. I mean, *we really* [were] targeting *on these universes* that they had collected.

236. Cambridge Analytica had previously disclosed the origins of their psychographic scores to Facebook on December 15, 2015, in its written confirmation that Cambridge Analytica “subcontracted the research phase of the *psychographic data* project to GSR, who provided us with an append to our voter file containing the psychographic scoring.” That same email ruled out public data sources (and RNC data) as inputs to the psychographics;

²⁴² Transcription, *Secrets of Silicon Valley—The Persuasion Machine—Alexander Nix*, BBC (2017) (“Persuasion Machine Tr.”) at 6:12-23.

those off-the-shelf and RNC data were *not* used for psychographics but only for political predictions.²⁴³

<https://statere.com/2018/12/11/leaked-email-facebook-data/>
 This article suggests that we model from Facebook likes. In actuality, the data we use for [personality prediction](#) is based on the voter file (public record) enriched with [voter name and location](#) that we have licensed from Acquis, Integrity, Kinetics, LI and the RNC, CEI/Trust. The article also suggests that we have collected information from Facebook without users' permission. This is incorrect; we haven't taken data from Facebook, and Cambridge Analytica has never collected primary data without individual consent.
<https://statere.com/2018/02/08/might-have-used-facebook-data-doesnt-sound-so-1747023880>
 This article states that Cambridge Analytica paid people \$1 to allow us to access their Facebook profile. This is untrue; we have not directly engaged with people over Facebook except through paid advertising efforts; we subcontracted the research phase of [the psychographic data project](#) to GSR, who provided us with an appeal to our voter list containing [the psychographic scores](#).

A few days later, Facebook spoke with Cambridge Analytica about the sources of the psychographics, and memorialized, again, that the psychographics rested on Kogan's stolen data: "You have told us that you received *personality score data* from Dr. Kogan that was derived from Facebook data, and those scores were assigned to individuals included in lists that you maintained," which was "in violation of our terms." ¶177. Facebook understood how GSR had harvested and modeled the personality scores based upon the 30 million Facebook users' data. §IV.E.4.

237. Facebook's political team—"embedded" inside Cambridge Analytica's Trump operations—was aware of all these findings because they commenced the investigation into Cambridge Analytica and stayed involved in it. Thus, when they saw and heard discussions about "psychographics," they would have known Cambridge Analytica was still using the misappropriated data that violated Facebook's policies.

²⁴³ Allan Smith, *Leaked email shows how Cambridge Analytica and Facebook first responded to what became a huge data scandal*, Business Insider (Mar. 22, 2018) (Cambridge Analytica's emailed responses to Facebook, responding to questions that Facebook investigation teammate Hendrix sent to Cambridge Analytica via email on December 12, 2015).

3. The Facebook Employees Embedded with Cambridge Analytica Saw that Cambridge Analytica Relied upon the Same Misappropriated Data It Used in the Cruz Campaign Because Trump Had Little Data/Models and Not Enough Time to Build Them Before the Election

238. Indeed, the Facebook embeds knew Cambridge Analytica did not have time to re-create that data set, which had taken over a year to build and model. Further, when these Facebook employees arrived at Cambridge Analytica in June 2016, the “Trump campaign’s digital operations [were] in an alarming state of disarray” and the Cambridge Analytica team was “horrified to find [the campaign] had no existing voter models of its own, nor any marketing apparatus.”²⁴⁴

239. Cambridge Analytica’s CEO verified that they kept using the Facebook data they had harvested in 2014-

²⁴⁴ Paul Lewis & Paul Hilder, *Leaked: Cambridge Analytica’s blueprint for Trump victory*, Guardian (Mar. 23, 2018); *see also* Kaiser, *Targeted* at 192 (In June 2016, the “Trump campaign’s digital operations [were] in an alarming state of disarray” and the Cambridge Analytica team was “horrified to find [the campaign] had no existing voter models of its own, nor any marketing apparatus.”); *see also* Transcription, *It’s Personal! Your Real Relationship with Data*, Digital Life Design Conference, YouTube (Jan. 22, 2017) at 4:25-5:6 (“And then after Donald Trump’s team won the primary election, I think they realized suddenly that now they had to run a presidential election. When we started working for Trump for America in June, there was probably less than 30 people working for his campaign. They made very little investment into data or science or modern advertising technology.”); ¶239 (Nix stating Cambridge Analytica “simply didn’t have the time” to make new models and collect new data for Trump, so used “legacy models” based on “Facebook” data.).

2015; Facebook's internal investigation proved these harvests violated its stated policies:²⁴⁵

[BBC REPORTER]: I want to start with the Trump Campaign. Did Cambridge Analytica ever use psychometric or psychographic methods in this campaign?

ALEXANDER NIX: We left the Cruz Campaign in *April [2016]* after the nomination was over. We pivoted *right across* onto the Trump Campaign. It was about five and a half months before polling. And whilst on the Cruz campaign we were able to do invest a lot more time into building psychographic models, into profiling, using behavioral profiling to understand different personality groups, and different personality drivers in order *to inform our messaging, and our creative*. We simply *didn't have the time* to employ this level of rigorous methodology for Trump.

* * *

ALEXANDER NIX: Now, there is clearly some legacy psychographics in the data, because the data is model data, all of it, *is model data that we've used* across the last 14, 15 months of campaigning *through the [2014] midterms and through the [2015-2016] primaries*. But specifically, did we build specific psychographic models for the Trump Campaign, no, we didn't.

[BBC REPORTER]: So you didn't build specific models for this campaign, but it sounds like you did

²⁴⁵ Persuasion Machine Tr. at 12:11-13:2; 13:9-14:16. Facebook provided statements on the record to the *BBC* for the *BBC* to read.

use some element of *psychographic modeling* as an approach in the Trump Campaign.

ALEXANDER NIX: *Only, only as a result of legacy data models.* So the answer is—the answer you’re looking for is no.

[BBC REPORTER]: The answer I’m looking for is to the extent to which it was used. I mean, *I don’t know what that means, legacy data modeling, what does that mean for the Trump Campaign?*

ALEXANDER NIX: Well, so we were able to take models that we’ve made previously *over the last two or three years*, and *integrate those into some of the work we were doing.*

[BBC REPORTER] (Voice Over): Where did all the information to predict voters’ personalities come from?

ALEXANDER NIX: Very originally, we used a combination of telephone surveys, and then we used a number of *online platforms for gathering questions.* As we started to gather *more data*, we started to look at other platforms *such as Facebook*, for instance.

240. Facebook’s employee embeds also helped Cambridge Analytica design ads for the Trump campaign.²⁴⁶ This part of the ad campaign process also relied upon the Facebook-based psychographics. Above, Nix stated that

²⁴⁶ Emily Glazer & Jeff Horwitz, *Facebook Curbs Incentives to Sell Political Ads Ahead of 2020 Election*, Wall St. J. (May 23, 2019) (“And in at least one instance, Facebook employees wrote potential Trump campaign ads, according to a person familiar with the matter and records reviewed by The Wall Street Journal.”). Facebook paid the embeds commissions to sell ads to the Trump campaign, though Harbath says Facebook no longer follows that compensation model.

his Cruz team used “behavioral profiling to understand different personality groups, and different personality drivers in order to inform our messaging, and our creative.” “Messaging” and “creative” refers to the ads themselves.

241. Trump campaign official Hong said that Cambridge Analytica’s data and modelling drove the creative ads process—the images, message, and tone of the Trump ad campaigns.²⁴⁷ Prior to October 27, 2016, a “senior official” in the Trump campaign told *Bloomberg* that the campaign had “three major voter suppression operations under way”—focused on “idealistic white liberals, young women, and African Americans.”²⁴⁸ One ad—titled: “Hillary Thinks African Americans are Super Predators”—was “delivered to certain African American voters through Facebook ‘dark posts’—nonpublic posts whose viewership the campaign controls so that, as [Project Alamo/Trump campaign official] Parscale puts it, ‘only the people we want to see it, see it.’” In a “confidential document seen by Channel 4 News, Cambridge Analytica admitted the Trump campaign did target ‘AA’ (African Americans) with what it called the ‘Predators video’—spending \$55,000 USD in the state of Georgia alone.”²⁴⁹

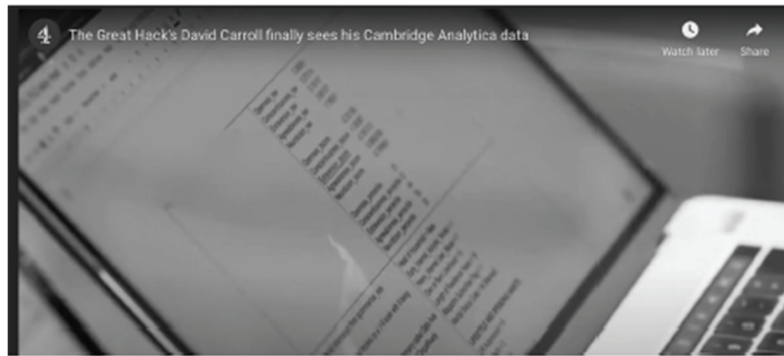
²⁴⁷ See, e.g., Persuasion Machine Tr. at 7:21-8:10 (“Now we’re going to go into the big kind of bullpen where a lot of the creatives were, and this is where I was as well . . . [t]his universe right here, that Cambridge Analytica, they’ve collected data, and they have identified as working mothers that are concerned about childcare.”).

²⁴⁸ Joshua Green & Sasha Issenberg, *Inside the Trump Bunker, with Days to Go*, *Bloomberg* (Oct. 27, 2016).

²⁴⁹ *Id.*

That video advertisement “received millions of views on Facebook.”²⁵⁰

242. Channel 4 News also obtained copies of the database that Cambridge Analytica deployed while Facebook was embedded. That database “reveals that 3.5 million Black Americans were categorised by Trump’s campaign as ‘Deter-



rence’—voters they wanted to stay home on election day.” The database “[had] a score for personality type” in it.²⁵¹ There were scores for “openness, conscientiousness, extraversion, agreeableness and neuroticism.”²⁵² The database was easy to use—a reporter quickly retrieved Professor David Carroll’s scores.²⁵³

“Just a click is all it took,” as Professor David Carroll explained. It would be absurd to suggest that the Face-

²⁵⁰ *Revealed: Trump campaign strategy to deter millions of Black Americans from voting in 2016*, Channel 4 News (Sept. 28, 2020).

²⁵¹ *Id.*

²⁵² *It works as a suppression system, it works to subvert the will of the people’—Professor David Carroll*, Channel 4 News (Sept. 29, 2020).

²⁵³ *Id.*

book embeds were unaware of the facts that “a click” revealed, given the degree to which they support Cambridge Analytica’s activities.

243. The “Facebook embeds showed campaign personnel and Cambridge [Analytica] staff how to aggregate look-alikes”—audiences similar to custom audiences—**“create custom audiences**, and implement so-called **dark ads**, content that only certain people could see on their feeds.”²⁵⁴ Facebook helped Cambridge Analytica target—via custom audiences (targeting) and dark ads (messaging)—African Americans by race at levels that were disproportionate to their share of the overall population, showing that race was an important factor in the targeting.

244. The team at Channel 4 that obtained a copy of the Project Alamo database reported these examples:²⁵⁵

In Michigan, a state that Trump won by 10,000 votes, 15% of voters are black. But they represented 33% of the special deterrence category in the secret database, meaning black voters were apparently disproportionately targeted by anti-Clinton ads.

In Wisconsin, where the Republicans won by 30,000, 5.4% of voters are black, but 17% of the deterrence group. According to Channel 4, that amounted to more than a third of black voters in the state overall,

²⁵⁴ Kaiser, *Targeted* at 193-94.

²⁵⁵ *Revealed: Trump campaign strategy to deter millions of Black Americans from voting in 2016*, Channel 4 News (Sept. 28, 2020) (“Trump 2016 campaign ‘targeted 3.5m black Americans to deter them from voting’ Secret effort allegedly focused on 16 swing states, several narrowly won by Trump after the black Democrat vote collapsed.”).

all placed in the group to be sent anti-Clinton material on their Facebook feeds.

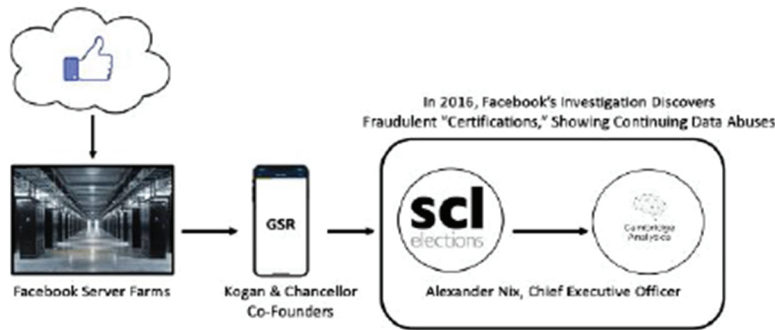
These facts are consistent with Barnes' characterization of the Trump campaign's core message, as *The Wall Street Journal* reported: "Trump's slogan, Make America Great Again, was about 'activating the deepest, darkest, soul of white nationalism.'" Unfortunately, Zuckerberg, Sandberg, Kaplan and Harbath's May 2016 assurances to the Trump campaign's leadership that Facebook would give it special training, coupled with the \$75-85 million dollar ad "Super Bowl"—as Sandberg saw it—meant that the embeds had to keep supporting the Trump campaign.

H. The Facebook Cambridge Analytica Investigation Team Learns that a Cambridge Analytica Affiliate, Which Participated in the Data Scam, Refuses to Sign Facebook's "Full Legal Contract" that Facebook "Required" Others to Sign by August 2016

245. On September 6, 2016, Facebook's investigation team learned new facts showing Cambridge Analytica was still abusing the subject data. The new facts came from one of the entities in the data transfer chain, SCL Elections Limited, a U.K. entity and affiliate of Cambridge Analytica, LLC, the U.S. entity involved in U.S. elections.

246. SCL Elections and Cambridge Analytica were both involved in the data heist and shared a common CEO—Nix. All of their roles in the data harvest were clear to Facebook well before September 6, 2016: Facebook's users trusted Facebook to safeguard their estimated 17.1 billion "likes" and other personal data; Facebook transferred all of that data to GSR via "whitelisting"

and other illicit means; GSR sold the data (including derivatives) to SCL Elections Limited; and SCL (via its CEO, Nix), in turn, gave the data to Cambridge Analytica. §IV.D.-E. A simplified illustration of this data flow follows:²⁵⁶



247. On September 6, 2016, “SCL Elections” told Facebook’s investigation team (in an apparent oral communication) “*that SCL* had permanently deleted all Facebook data and derivative data received from GSR *and that* this data had *not been transferred or sold to any other entity.*”²⁵⁷ That statement was false, as Facebook knew at the time.

248. Cambridge Analytica—another “entity”—admitted to Facebook that it had received the stolen data. In responding to the Facebook investigation team’s questions on December 12, 2015, for example, Cambridge Analytica’s Chief Data Officer (Tayler) wrote that he was “cc’ing in our CEO, Alexander Nix,” in “commenting on

²⁵⁶ In this demonstrative, the image of a Facebook server farm is from a September 29, 2016 article by The Verge, entitled: “*Mark Zuckerberg shares pictures from Facebook’s cold, cold data center.*”

²⁵⁷ Facebook, Responses to U.S. Senate Committee on Commerce, Science, and Transportation, Questions for the Record addressed to Chairman John Thune (June 8, 2018) at 126.

those sections [in news articles] relevant to *Cambridge Analytica*.”²⁵⁸ In that same email, Tayler and Nix commented on an article by *Gizmodo* and wrote that “Cambridge Analytica” did not pay people to take personality quizzes but that “we subcontracted the research phase of the *psychographic data* project to *GSR*, who provided us with an append to our voter file containing the *psychographic scoring*.”²⁵⁹ These facts illustrate that “Cambridge Analytica” *had* received the stolen data, contrary to SCL’s September 6, 2016 (oral) representation that the data “had *not* been transferred or sold to any other entity.”²⁶⁰

249. SCL’s September 6, 2016 oral representation was not just false; it constituted a refusal to provide a written certification, which also alerted Facebook’s investigation team to the fact that Cambridge Analytica was still abusing the stolen data. One of the terms of Facebook’s June 24, 2016 “settlement” contract with Kogan and Chancellor’s GSR company was that GSR had to recover written “certifications” of deletion from SCL—the foreign affiliate of Cambridge Analytica—no later than mid-July 2016.²⁶¹ Zuckerberg would later give testimony

²⁵⁸ Allan Smith, *Leaked email shows how Cambridge Analytica and Facebook first responded to what became a huge data scandal*, Business Insider (Mar. 22, 2018).

²⁵⁹ *Id.*

²⁶⁰ Facebook, Responses to U.S. Senate Committee on Commerce, Science, and Transportation, Questions for the Record addressed to Chairman John Thune (June 8, 2018) at 126.

²⁶¹ Facebook, Responses to House of Commons, Dig., Culture, Media and Sport Comm. to Damian Collins (May 14, 2018) at 20 of 40 (Confidential Settlement Agreement and Mutual Release at §II.A.4.) (“GSR will notify all persons that accessed or received App Data from GSR or Dr. Kogan or with whom either GSR or Dr. Kogan shared or disclosed App Data that all App Data is to be permanently deleted.

admitting the “certification” was a “full legal contract.”²⁶² Facebook has stated that it had “**demanded** certifications” after learning of the data transfer “in 2015.”²⁶³ These facts raise a compelling inference that Facebook, in substance, called SCL on September 6, 2016 to “demand” that it sign a “full legal contract” (or at least *something*) in writing that SCL had deleted the data—and that SCL said, in substance, “no.” Cambridge Analytica never signed a “full legal contract” or gave any written certification other than the one Facebook discovered to be a fraud on June 11, 2016; as to SCL, it refused to put anything in writing about deleting data until April 3, 2017—

GSR will also provide all persons receiving notice with a Certification in the form attached as Exhibit B. GSR will inform all such persons [who received the 30 million users’ Facebook “likes” and other personal data] that this notification ***shall be completed within fourteen (14) business days*** following receipt by such persons.”). July 14, 2016 was 14 business days after June 24, 2016.

²⁶² Comm. Hearing Tr., Senate Commerce, Sci. and Transp. Comm. and Senate Judiciary Comm. Joint Hearing on Facebook (Apr. 10, 2018) at 35-36 (“Senator Whitehouse: OK. And with ***respect to Cambridge Analytica***, your testimony is that first ***you required them to formally certify*** that they had deleted all improperly acquired data. Where did that formal certification take place? . . .” Zuckerberg: “Senator, first ***they sent us an e-mail notice*** from their chief data officer telling us that they didn’t have any of the data any more, that they deleted it and weren’t using it. And then later we followed up with, I believe, ***a full legal contract*** where they certified that they had deleted the data.”).

²⁶³ Jonathan Shieber & Taylor Hatmaker, *Facebook suspends Cambridge Analytica, the data analysis firm that worked on the Trump campaign* (Mar. 16, 2018).

16 months after Facebook “demanded” it, and **six months** after the Trump campaign was finished.²⁶⁴

250. Cambridge Analytica’s affiliate, SCL, would **not** sign Facebook’s “demanded certification” deletion at any point before the Trump election was over because its affiliate (and source of the £750,000 funding the data harvest) was **still using** the data, as Facebook knew. Facebook’s investigation into Cambridge Analytica continued to discover more facts that Cambridge Analytica was misusing the purloined data in the Trump campaign.

I. Facebook’s Investigation Team Witnesses a Cambridge Analytica Presentation and Interview that, in Combination with Private Emails from Cambridge, Show Cambridge Analytica Is Using the Misappropriated Data in the Trump Campaign

²⁶⁴ That date, April 3, 2017, also was well after Facebook collected its \$75-\$85 million in advertising revenue from Cambridge Analytica’s Trump work **while** its “embeds” were working inside the Cambridge Analytica data. Facebook removed the “Date” line from that April 3, 2017 SCL “certification,” despite required “Date” lines on other certifications of deletion. On the face of SCL’s April 3, 2017 “certification,” SCL wrote that “this certificate is provided without liability or prejudice to me [Nix] personally or to SCL and **cannot be relied upon** to found any action against SCL or any related person or entity.” Facebook, Responses to House of Commons, Dig., Culture, Media and Sport Comm. to Damian Collins (May 14, 2018) (Confidential Settlement Agreement and Mutual Release at 38 of 40). Facebook could not “believe” in this April 3, 2017 date before it even existed—*i.e.*, during the 2015-April 2016 period, and did not “believe” it was true in April 3, 2017 given SCL’s refusal to sign while its affiliate, Cambridge Analytica, and Facebook were both making millions of dollars from the Trump campaign in the run up to the 2016 election.

1. Facebook’s Investigation Team Watches Nix’s September 2016 Concordia Presentation

a. Cambridge Analytica “Is Using” Personality Scores

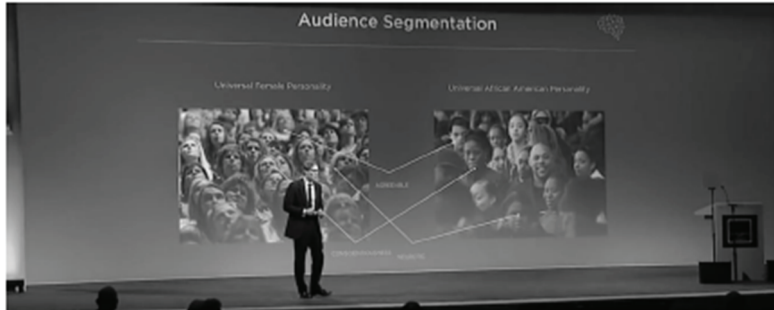
251. Cambridge Analytica—with Facebook’s support—sent selected African Americans listed in Cambridge Analytica’s psychographic database the exact same disengagement ads during Project Alamo. Nix made this point in a video of a presentation that he made on September 27, 2016.²⁶⁵

The idea that all women should receive the same message because of their gender or all African-Americans because of their race or all old people or rich people or young people to get the same message because of their demographics just doesn’t make any sense.

Clearly demographics and geographics and economics will influence your world view, but ***equally important or probably more important are psychographics***. That is an understanding of your personality, because it’s ***personality that drives behavior and behavior that obviously influences how you vote***.

Nix illustrated that Cambridge Analytica would sub-segment its audiences, by personality trait, based upon the OCEAN model:

²⁶⁵ ECF No. 130-6, Transcription of *Cambridge Analytica—The Power of Big Data & Psychographics*, Concordia Summit (Sept. 27, 2017) (“The Power of Big Data & Psychographics”) at 3:16-4:1.

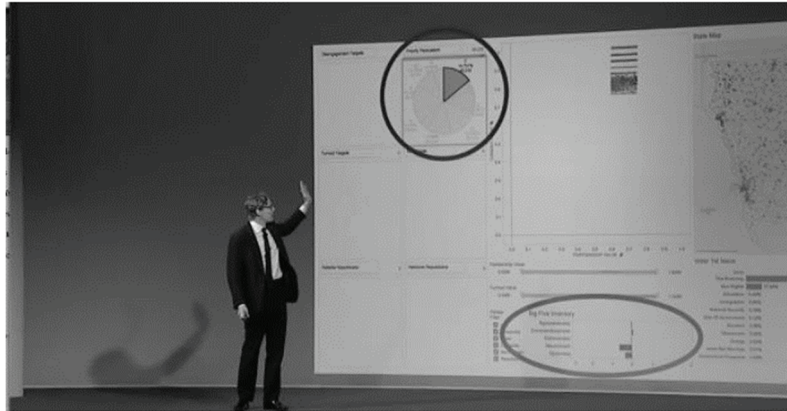


On that day, Tuesday, September 27, 2016, Facebook’s “embeds” continued working inside of the Cambridge Analytica data center deploying these technologies, as Nix admitted: “I can tell you is that of the two candidates left in this election, one of them *is using* these technologies, and it’s going to be very interesting to see how they impact the next seven weeks.”²⁶⁶

b. Cambridge Analytica “Is Using” Personality Score Dashboards

252. On September 27, 2016, Nix even provided images of the computer dashboards that the Facebook embeds would have seen over the course of the months that they supported Project Alamo:

²⁶⁶ The Power of Big Data & Psychographics at 9:14-18.



253. Nix’s September 27, 2016 presentation highlighted (with the circular and oval-shaped emphases in the original presentation, above) that Cambridge Analytica’s “Priority Persuasion” targeting methodology was related to its “Big Five Inventory”—the OCEAN scores. These facts are significant because they corroborate evidence that Cambridge Analytica named its Facebook custom audiences, while working on the Trump campaign in San Antonio, by personality type for targeting purposes. The “embeds” witnessed those facts, as did the rest of Facebook’s investigation team because they saw Nix’s video presentation.

c. Cambridge Analytica “Is Using” the Stolen “Likes” Model

254. Facebook’s investigation team also saw—in Nix’s September 27, 2016 presentation—a clear picture of Nix admitting that Cambridge Analytica continued to use the OCEAN model, as Nix explained at the presentation: “at Cambridge, we’ve rolled out a long-form quantitative instrument to probe the underlying traits that inform per-

sonality. This is the cutting-edge in experimental psychology known as the OCEAN *model*.²⁶⁷ Nix presented a large slide to illustrate the importance of the model:

255. Facebook’s investigation team would have appreciated the importance of this “cutting edge” OCEAN model,



as Nix put it. The “five-factor personality model” was fruit of the poisonous tree—a derivative of the stolen data that Facebook’s investigation team had ruled a policy violation.²⁶⁸

256. Facebook’s investigation team understood that Cambridge Analytica’s cutting edge OCEAN model was inspired by the Kosinski’s “likes” paper because Facebook’s in-house research team surfaced that fact and Kosinski contacted Facebook personally to convey that fact and other warnings. ¶164. Facebook’s investigation team closed a settlement agreement with Kogan on June 24, 2016, wherein Kogan told Facebook that he had been

²⁶⁷ The Power of Big Data & Psychographics at 4:1-6.

²⁶⁸ See ¶177 (“You have told us that you received personality score data from Dr. Kogan that was *derived from* Facebook data, and that those scores were assigned to individuals included in lists that you maintained. Because that data was improperly *derived from* data obtained from the Facebook Platform, and then transferred to Cambridge Analytica in violation of our terms”).

working with “current and former” members of Facebook’s research team on the stolen data. ¶¶196-197. Those “current” members included Kogan’s co-founder of GSR, full-time Facebook employee Chancellor. *Id.*; see also §IV.E.3. Kogan presented his and Chancellor’s findings from the stolen Cambridge Analytica dataset to Facebook’s research team. §IV.E.3. And Chancellor presented more general findings at an academic conference on September 24, 2015—a presentation that enticed Facebook to hire Chancellor on November 9, 2015. *Id.*

257. Chancellor’s September 24, 2015 academic presentation, which Kogan or Chancellor presented to Facebook, clearly demonstrated to Facebook that Kogan and Chancellor used the purloined “likes” data to replicate Kosinski’s “likes” model for sale to Cambridge Analytica—the *same* model that the CEO of Cambridge Analytica was presenting on September 27, 2016, which Facebook’s investigation reviewed on or about that date.

258. Both Chancellor’s “likes” presentation and Kosinski’s “likes” paper rely upon the same performance metrics—area under the curve (AUC) and r-value coefficients.²⁶⁹ Both models use a set of dichotomous and con-

²⁶⁹ The AUC (“Area Under Curve”) metric addresses dichotomous variables that only have two outcomes (like a coin toss). In the case of a model, if it is presented with Facebook “likes” associated with one random male and one random female, the model will correctly classify these two individuals 93% of the time. A value of AUC that equals 0.5 means the model is no better than a random guess, and a value of AUC that equals 1.0 means the model makes perfect predictions. By contrast, r-values test variables where outcomes can fall on a range. The figure is also a measurement of model accuracy for continuous variables: r-values can measure the strength of the relationship between the model’s estimate and the test result. A value of r that equals 0 indicates that the model has no predictive value of the test

tinuous attributes with many of the same attributes showing up in each document. Both Kosinski’s “likes” model and Chancellor’s “likes” model rely upon one single data source—Facebook “likes.” Chancellor’s presentation illustrates that Facebook “likes” were the exclusive input to the process of training, validating, and using the model. These steps require a large volume of “ground truth” data, which Kogan told Facebook they had secured from the Quiz App. §IV.E.3.; §IV.F.3.-4. Responses to the Quiz App reveal actual 5-factor OCEAN scores based upon survey responses, and the Facebook “likes” from those survey respondents were used to train and validated the models. Quantitatively, the model that Chancellor presented bore striking similarities with the model in Kosinski’s paper.²⁷⁰ The Facebook “likes” model that Kogan and Chancellor built for Aleksandr Nix *was* the Kosinski model, as Facebook knew by talking to Kogan and Chancellor about the model, before hiring Chancellor to help Facebook apply the model internally, in November 2015.

259. Critically, Facebook had previously attempted to pressure Kosinski into teaching Facebook how to repli-

results. A value where r equals 1 indicates that there is a perfect linear relationship between the model’s result and the test result.

²⁷⁰ For example, the AUC metric for the “gender” dichotomous variable in the Chancellor presentation was approximately 0.92; in the Kosinski paper, it was 0.93. Both also tested whether a person was African American or Caucasian; Kosinski’s AUC was 0.95, and Chancellor’s presentation (*i.e.*, of the model he and Kogan sold to Cambridge Analytica via SCL) was 0.84. As another example, r -value for the “conscientiousness” continuous variable in the Chancellor presentation was approximately 0.32; in the Kosinski paper, it was 0.29. These and other modeling results show that Kogan and Chancellor closely replicated Kosinski’s Facebook “likes” model, which, as Facebook knew, was one of the key reasons Cambridge Analytica hired them.

cate his published “likes” model: “On the day that Kosinski published these findings [in his “likes” paper], he received two phone calls. The threat of a lawsuit *and* a job offer. Both from Facebook.”²⁷¹

260. The fact that Facebook threatened Kosinski with a lawsuit and job offer with regard to his “likes” model further reveals Facebook’s knowledge as to Cambridge Analytica’s “likes” model. The lawsuit demonstrates that creating derivative products from lawfully-obtained “likes” data violated Facebook’s stated policies. The job offer shows Facebook believed the “likes” model was so commercially valuable that it wanted to hire Kosinski full-time to teach Facebook how to replicate it—and that’s exactly what they got from Chancellor, as Facebook’s investigation discovered. Facebook’s investigation team knew all these facts because of their access to Chancellor (as employee); Kosinski (as a volunteer); Kogan (as a cooperating witness); and Facebook’s in-house research staff who were part of the investigation team, and connected the Kosinski-likes-OCEAN model dots for the rest of the team.

²⁷¹ Hannes Grassegger and Mikael Krogerus, *The Data That Turned the World Upside Down*, Stanford University (Jan. 28, 2017) at 5 (“The strength of their modeling was illustrated by how well it could predict a subject’s answers. Kosinski continued to work on the models incessantly: before long, he was able to evaluate a person better than the average work colleague, merely on the basis of ten Facebook ‘likes.’ Seventy ‘likes’ were enough to outdo what a person’s friends knew, 150 what their parents knew, and 300 “likes” what their partner knew. More ‘likes’ could even surpass what a person thought they knew about themselves. On the day that Kosinski published these findings, he received two phone calls. The threat of a lawsuit and a job offer. Both from Facebook.”)

d. Cambridge Analytica “Is Using” the Stolen “Likes” Data

261. Facebook and Cambridge Analytica also collaborated on the \$85 million worth of ads—the images, sounds, colors—that Facebook sold to Cambridge Analytica in Project Alamo. “And in at least one instance, Facebook employees wrote potential Trump campaign ads, according to a person familiar with the matter and records reviewed by *The Wall Street Journal*.”²⁷² This creation of advertisements inside Project Alamo depended upon the OCEAN data, as Nix admitted that their ads “need[ed] to be nuanced according to the certain personality that we’re interested in.”²⁷³ “Pretty much every message that Trump put out was data-driven,” Nix explained.²⁷⁴ Nix said that “[w]e did all the research, all the data, all the analytics, all the targeting, we ran all the digital campaign, the television campaign, and our data informed all the strategy.”²⁷⁵ A Nix colleague said about their Trump ads: “We just put information into the bloodstream [of] the internet and then . . . watch[ed] it grow.”²⁷⁶

262. Facebook was still investigating Cambridge Analytica at the time that he made his presentation on September 27, 2016.

²⁷² Emily Glazer & Jeff Howitz, *Facebook Curbs Incentives to Sell Political Ads Ahead of 2020 Election*, Wall St. J. (May 23, 2019).

²⁷³ The Power of Big Data & Psychographics at 7:13-15.

²⁷⁴ Hannes Grassegger & Mickael Krogerus, *The Data That Turned the World Upside Down*, Motherboard (Jan. 28, 2017).

²⁷⁵ Exposed: Undercover secrets of Trump’s data firm, Channel 4 News (Mar. 20, 2018).

²⁷⁶ *Cambridge Analytica executives: We invented ‘Crooked Hillary’ campaign*, The New Daily Australia (Mar. 21, 2018).

263. Facebook’s Cambridge Analytica team watched the video and circulated it internally. “Employees responsible for coordinating Facebook’s response to the Guardian article also circulated a link to a video of a marketing presentation by Cambridge’s chief executive officer about the firm’s ability to target voters based on personality.”²⁷⁷ That team watched Nix refer to the way that Cambridge Analytica built the OCEAN model: “By having hundreds and *hundreds of thousands* Americans undertake this *survey*, we were able to perform a model to predict the personality of every single adult in the United States of America.”²⁷⁸ Facebook investigation team knew that the Quiz App *was* a survey that 250-270 hundred thousand Americans installed, as Facebook knew because that app was a Facebook app, with an App ID number and download history that the investigation team reviewed. ¶¶170-173.

264. Facebook’s investigation team also necessarily would have viewed Nix’s September 27, 2016 presentation in

<https://fortune.com/2016/12/15/leaked-cra-fb-facebook-data/>
This article suggests that we model from Facebook likes. In actuality, the data we use for making political predictions is based on the voter file (public record) enriched with consumer and lifestyle data that we have licensed from Axion, Infogroup, Aristotle, L2 and the RNC Data Trust. The article also suggests that we have collected information from Facebook without users permission. This is incorrect; we haven't taken data from Facebook, and Cambridge Analytica has never collected primary data without individual consent.
<http://iarmodo.com/leaked-cra-might-have-your-facebook-data-depending-on-ho-174752380/>
This article states that Cambridge Analytica paid people \$1 to allow us to access their Facebook profile. This is untrue; we have not directly engaged with people over Facebook except through paid advertising. Further, we subcontracted the research phase of the psychographic data project to GSR, who provided us with an append to our voter file containing the psychographic scores.

light of his prior admissions to Facebook that Cambridge Analytica derived political predications from a host of publicly available information but derived its “*psychographic scoring*” from *one* source—GSR.²⁷⁹

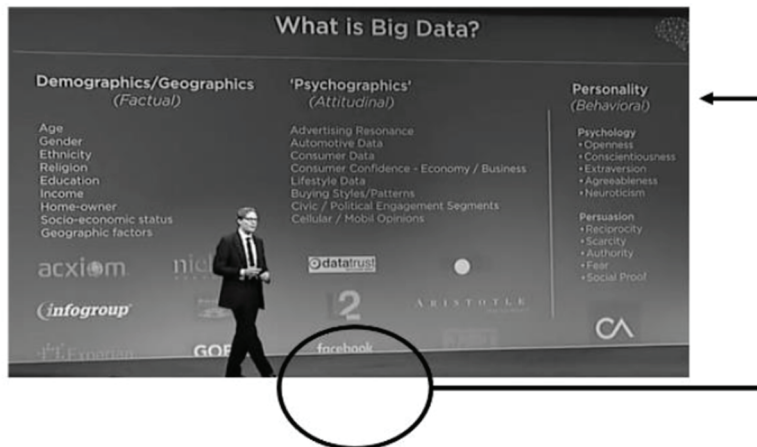
²⁷⁷ SEC Complaint at ¶35.

²⁷⁸ The Power of Big Data & Psychographics at 4:14-18.

²⁷⁹ Allan Smith, *Leaked email shows how Cambridge Analytica and Facebook first responded to what became a huge data scandal*, Business Insider (Mar. 22, 2018) (Cambridge Analytica’s emailed re-

The investigators immediately understood this written confirmation and provided its own written confirmation to Cambridge Analytica that the psychographic scores were inappropriate. See ¶177. (“You have told us that you received personality score data from Dr. Kogan that was derived from Facebook data, and that those scores were assigned to individuals included in lists that you maintained . . . in violation of our terms.”).

265. Facebook’s investigation team did review Nix’s September 27, 2016 presentation with those facts in mind and therefore understood that Facebook data alone—and none of the other data for sale on the market—were the key input to Cambridge Analytica’s personality scores. Facebook still was using this £750,000’s worth of Facebook “Big Data”:



266. Yet again, Facebook’s investigation team caught Nix continuing to violate Facebook’s publicly stated po-

sponses to Facebook, responding to questions that Facebook investigation teammate Hendrix sent to Cambridge Analytica via email on December 12, 2015).

lices as, Nix admitted that one of the presidential candidates “*is using* [Cambridge Analytica’s] technologies,” referring to then-candidate Trump.²⁸⁰ Facebook’s investigation amassed even more evidence that Cambridge Analytica continue to violate Facebook’s stated policies on October 27, 2016.

2. Facebook’s Investigation Team Reviews Nix’s Statements to *The Washington Post* that Cambridge Analytica’s Psychographics Rely on Facebook “Likes,” Knowing Nix Spent One Year and £750,000 Harvesting Approximately 17.1 Billion “Likes” with GSR and Then Lied About It

267. On October 27, 2016, while Cambridge Analytica was still under investigation by Facebook, Cambridge Analytica shared the following information on social media:



²⁸⁰ The Power of Big Data & Psychographics at 9:14-18.

268. Facebook’s investigation team picked up on *The Washington Post* article that Nix shared and endorsed on social media. “Facebook lawyers and employees in the company’s political advertising group saw and discussed an October 27, 2016, article in *The Washington Post* reporting that Cambridge combined psychological tests with ‘likes’ on ‘social-media sites.’”²⁸¹ The political advertising employees were among the many Facebook employees involved in Facebook’s investigation into Cambridge Analytica.²⁸² Ample facts show Kaplan (a lawyer,

²⁸¹ SEC Complaint at ¶35.

²⁸² Facebook’s political advertising activities were among Harbath’s responsibilities in the policy group—*i.e.*, the political team was part of “policy.” See, *e.g.*, Somini Sengupta, *Facebook Builds Network of Friends in Washington*, *The New York Times* (May 19, 2012) at 1 (“Patrick Bell, an aide to Representative Cathy McMorris Rodgers, Republican from Washington, recalled a meeting last fall where a onetime Republican aide, **Katie Harbath, counseled** a room full of Republican lawmakers on how to use the site to communicate with voters. ‘We had a Republican from Facebook talking to Republicans. They love that,’ he said.”); Kyle Trygstad, *Online Political Advertising Gets Personal*, *Roll Call* (Sept. 20, 2012) at 2 (“That’s led companies including [Facebook] to hire strategists from the political world **to help with outreach to potential advertisers . . .** Facebook brought on Katie Harbath, the former chief digital strategist at the National Republican Senatorial Committee”); Anna Brand, *The women bridging tech and politics in the 2016 election*, *MSNBC.com* (June 23, 2015) at 2 (“Katie Harbath: My team helps candidates, political parties, elected officials and governments around the globe use Facebook effectively to engage with people in those countries. The Politics and Government Outreach team has grown from three **to seven in the last two years**. We are globally focused and **have worked extensively**, for example, on elections in **the UK** this year, as well as the [mid-term] 2014 elections in . . . **the U.S.**”). A detailed study of Facebook political employees’ social media found just four Facebook employees working on political advertising for the Republican team were Harbath, Barnes, “FB1” and another Facebook em-

political advisor and lobbyist overseeing Harbath in the political advertising group) and Harbath (a businessperson running the small political ads group, including the Trump-Cambridge Analytica “embeds”) were among the “lawyers and employees” who saw and discussed *The Washington Post’s* October 27, 2016 article. The same is true of Sandberg (who had a dotted-line reporting relationship with Kaplan on political matters) and Schrage (who was Kaplan’s direct manager); each of Sandberg and Schrage also received media “flags” as a matter of standard operating procedure at Facebook (§162 n.159); political news involving Facebook, however, was particularly important to Sandberg.²⁸³ Moreover, Zuckerberg and Sandberg instructed Kaplan and Harbath to help the Trump campaign in May 2016 (Kaplan and Harbath, in turn, helped convince Zuckerberg and Sandberg to personally court the Trump campaign); thus, it would be absurd to suggest that Kaplan and Harbath failed to apprise Zuckerberg and Sandberg of the facts reported by *The*

employee. *Partisan Programming: How Facebook and Google’s Campaign Embeds Benefit Their Bottom Lines*, Campaign for Accountability, Google Transparency Project (Aug. 2018). Harbath shared on social media: “[I] [a]m working in the Facebook DC office **leading the team** helping elected officials, politicians and governments around the world use Facebook to communicate with constituents/voters.” Appendix A: Google Elections and Politics Employees.

²⁸³ For example, on July 27, 2016, Sandberg participated in a conference call with investors. Q2 2016 Facebook, Inc Earnings Call Tr. at 12 (July 27, 2016). On that call, one participant asked Sandberg about political spending and Sandberg responded in relevant part: “**While the political campaign, obviously a lot of money is spent in ads. That’s also true of an Olympics. It’s also true of a World Cup. It’s also true of a Superbowl.** With all of these events taking place around the world, there’s no one event that we think drives a huge portion of revenue. **That said, we are pleased by what’s happened on Facebook for the election cycle.** Not just on the paid side **but actually on the organic side as well.**”).

Washington Post on October 27, 2016, particularly in light of the other facts uncovered by Facebook’s ongoing investigation into Cambridge Analytica, such as its affiliate’s continuing refusal to sign a written certification of data destruction and Cambridge Analytica’s fraudulent certification, which Facebook uncovered on June 11, 2016. Zuckerberg, Sandberg, Kaplan and Harbath all knew about Facebook’s own investigation into Cambridge Analytica.

269. *The Washington Post’s* October 27, 2016 article, titled: “Trump’s plan for a comeback,” includes building a ‘psychographic’ profile of every voter,” informed Facebook’s investigation of a number of important facts. The article was based on an interview of Nix, and reported these facts about Cambridge Analytica’s psychographics: “The psychological tests are combined with a collection of data, such as a person’s taste in movies, music, books, restaurants, **and the ‘likes’** or ‘hearts’ on **social media sites**.”²⁸⁴ *The Washington Post’s* article quoted from (and provided a hyperlink to) Nix’s September 27, 2016 presentation at the Concordia Annual Summit discussed above.

270. All of this information had special significance to Facebook’s Cambridge Analytica investigation team, on account of the below facts that GSR and Kogan had formally certified to Facebook:²⁸⁵

²⁸⁴ Michael Kranish, *Trump’s plan for a comeback includes building a ‘psychographic’ profile of every voter*, Wash. Post (Oct. 27, 2016).

²⁸⁵ Stimson Letter at 28 of 40 (June 11, 2016 Certs. and June 24, 2016 Settlement Agr. attachments) (showing “6/11/2016” execution dates).

Name	Contact Information	Number of unique Facebook, and Specific Data Points Shared
SCL	Alexander Ashburner Nix	Approximately 30 million people. Shared forecasted survey responses (derived from page likes) and some limited profile data (such as name, location, birthday, and whether an individual had liked any of a limited list of specific Facebook pages)

3. Facebook Learns About Cambridge Analytica's Voter Suppression Campaign Based on the Misappropriated Psychographics

271. On the same day that Facebook's investigation team saw and discussed the October 27, 2016 article from *The Washington Post*, *Bloomberg* published an article about how the Trump campaign was following a voter suppression strategy.²⁸⁶ *Bloomberg's* report, "Inside the Trump Bunker, With Days to Go," reported that "Trump's data scientists, including some from the London firm Cambridge Analytica who worked on the 'Leave' side of the Brexit initiative, think they've identified a small, fluctuating group of people who are reluctant to admit their support for Trump and may be throwing off public polls." Yet, as *Bloomberg* reported, "Trump's reality is plain: He needs a miracle." Thus, as *Bloomberg* reported, a Trump campaign official said: "***We have three major***

²⁸⁶ Joshua Green & Sasha Issenberg, *Inside the Trump Bunker, with Days to Go*, *Bloomberg* (Oct. 27, 2016).

voter suppression operations under way,” and then *Bloomberg* noted that suppression operations are “aimed at three groups Clinton needs to win overwhelmingly: idealistic white liberals, young women, and African Americans.” This was the campaign that Facebook was monetizing and supporting with the Facebook embeds in San Antonio.

272. The actual advertisements (so-called “dark ads” or “dark posts”) that Facebook delivered to Cambridge Analytica’s suppression targets on behalf of the Trump campaign—with one exception about Hillary Clinton allegedly believing African American youths are “super predators”—have not been disclosed by Facebook. But the Trump campaign’s dark posts enjoyed special treatment inside of Facebook, as *The Wall Street Journal* reported on October 21, 2016: VP “Kaplan defended an internal whitelist maintained by Facebook to protect certain high-profile accounts, including President Trump’s”²⁸⁷ account along with other major media outlets’ accounts. The internal whitelists flagged controversial content for additional review, so that Facebook did not prevent the content’s publication without further review.

273. Sensitive content subjects like Trump’s reported voter suppression campaign—and related custom audiences and “dark posts”—rose quickly to the appropriate personnel at Facebook on October 27, 2017. *Reuters* reported on that day: “an elite group of at least five senior executives regularly directs content policy and makes editorial judgment calls, particularly in high-profile controversies, eight current and former Facebook executives

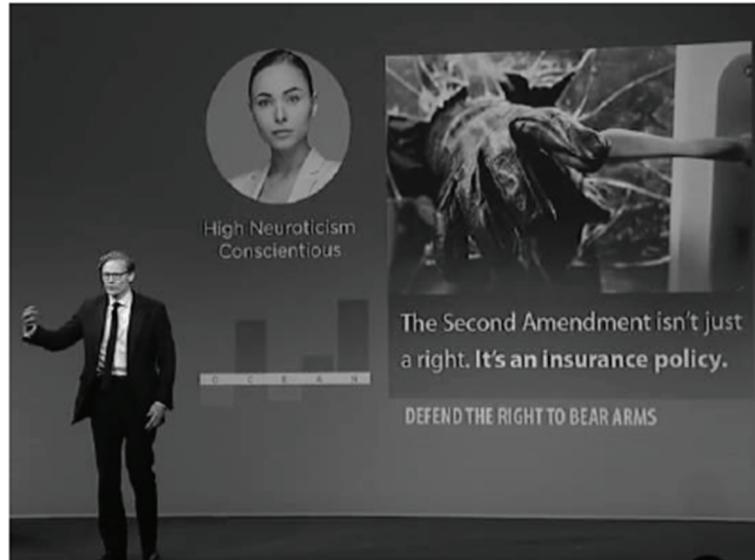
²⁸⁷ Deepa Seetharaman, *Facebook’s Lonely Conservative Takes on a Power Position*, Wall St. J. (Dec. 23, 2018).

told Reuters.”²⁸⁸ The voter suppression campaign reported by *Bloomberg* meets that description. “The current and former Facebook executives, most of them speaking on condition of anonymity, told *Reuters* in detail how complaints move through the company’s content-policing apparatus. The toughest calls, they said, rise to an elite group of executives.” “In addition to **Sandberg** [and two others], executives involved in sensitive content issues include Joel **Kaplan**, Facebook’s Washington-based government relations chief; and Elliot **Schrage**, the vice president for public policy and communications.”²⁸⁹ These facts relating to Facebook’s internal procedures show that Sandberg, Kaplan and Schrage would have been aware of the *Bloomberg* voter suppression report and would have been briefed on the fact that Facebook had its own personnel “embedded” inside the Trump campaign while that conduct was ongoing and, in fact, supported the conduct as set forth above with precision as to the exact manner of support.

274. Reports about Cambridge Analytica’s voter suppression campaign followed just a month after Nix’s Concordia presentation. There, he displayed how the company’s advertisements were informed by the policy-violating “psychographics”:

²⁸⁸ Kristina Cooke, Dan Levine, & Dustin Volz, *Facebook executives feel the heat of content controversies*, Reuters (Oct. 27, 2016).

²⁸⁹ *Id.*



275. Here, Nix states in a video—which Facebook’s investigation team reviewed several times (*e.g.*, ¶¶294, 298)—that his “psychographics” inform both the content of all of Cambridge Analytica’s ads, and its targets, as in the case of the person that the stolen data and models identified by name, by psychographic trait (high neuroticism) and targeted with an ad designed to shock someone who possessed that personality trait. Nix said in the above video that one the presidential campaigns was “using” the methodologies that he just discussed. ¶251. Based on these facts, it follows that Cambridge Analytica continued to run Facebook ads that violated Facebook’s *stated* policies because they were derived from the stolen data. This inference strengthens when viewed in light of the fact that Facebook’s political team “whitelisted” content from the Trump campaign and the fact that Facebook helped Cambridge Analytica suppress voter turnout from protected classes in the 2016 election, as demonstrated above.

276. Unfortunately, because Facebook largely sold “dark posts” to Cambridge Analytica to support its voter suppression campaign, it is not possible to provide examples of those ads. Many have asked Facebook to disclose examples, but it refuses to do so, for obvious reasons.²⁹⁰

J. Zuckerberg, Sandberg and Rose Discuss Voter Suppression and Cambridge Analytica with Roger McNamee over the October 2016-2017 Period

1. McNamee Approaches Zuckerberg and Sandberg Before the 2016 Election

277. On October 30, 2016, McNamee—an early Facebook investor and business mentor to Zuckerberg and Sandberg—called them to express concerns about Facebook’s role in political contests and other areas. Brexit was one of the issues that concerned McNamee, as he explained in an interview:²⁹¹

²⁹⁰ See, e.g., McKenzie Funk, *Cambridge Analytica and the Secret Agenda of a Facebook Quiz*, N.Y. Times (Nov. 19, 2016) (Reporting: “In this election, [Facebook’s] dark posts were used to try to suppress the African-American vote.”).

²⁹¹ McNamee is a highly regarded venture capitalist in Silicon Valley who had extensive ties to Zuckerberg and Sandberg: McNamee encouraged Zuckerberg not to sell the company in its early days, and mentored Zuckerberg about developing Facebook in those early days; McNamee understood that Zuckerberg would benefit from additional business support and personally introduced him to Sandberg; McNamee invested in Facebook; McNamee was friends with other Facebook senior executives; in short, McNamee considered Facebook one of the most important investments that he had made in a successful career, explaining at an interview that “I felt like this truly was my baby.” Transcription, *From Mentor to Activist: Facebook Through the Eyes of Roger McNamee*, Real Vision Finance, YouTube (Apr. 13, 2019) at 15:24-15, 17:10-18:6, 18:14-18.

Fast forward to June [2016], Brexit, the British voting on whether or not to leave the European union. The final polls say that they're going to remain, and remain's going to win by 4 points. That night out comes the election returns, and leave has won by 4 points. So 8 points. And in the postmortems there was a lot of talk about the role Facebook had played. And what was interesting was nobody was blaming Facebook.

But if you were in my position looking at this thing, you're going, whoa, leave had a really inflammatory campaign, right? They're basically saying those evil immigrants are going to destroy your culture, take away your jobs, and they're ruining the country and all the crime is blamed on them. And then they were offering this pie-in-the-sky thing of, hey, we're going to save billions of dollars—or billions of pounds on exiting the EU, we're going to take all that money and pour it into the national health system. So effectively they were saying to everybody, you can vote because of some racially motivated animus, but you can feel good about it because you're going to save the national health system.

* * *

Meanwhile, the remain side has no emotion in it at all. They're basically going, we have the sweetest deal on earth. We get all the benefits of EU membership and we get to keep our own currency; that's a great deal, don't screw it up. Should have won in a walk. I mean, the British are—I mean stay the course is the British way. And yet the thing swings 8 points.

And I'm thinking to myself, is Facebook giving an advantage to inflammatory political campaigns over

neutral ones? ***That was the hypothesis that Brexit brought me to.***

278. These and other Facebook-related issues prompted McNamee to consider writing an op-ed that was critical of Facebook; but, rather than going the press, he first sought to work with his mentees, Zuckerberg and Sandberg, privately. He contacted them on October 30, 2016. “And they get right back to me, ***I mean within hours,***” McNamee explained.²⁹²

And they said, but, you know, ***we take you seriously,*** you know, you’ve been a friend of ours for a long time, so we’re going to have one of our senior people work really closely with you to figure out if there’s something we should be investigating. And they turned me over to ***Dan Rose.***

Now, Dan I think is the second-longest serving executive at Facebook and he’s somebody I knew really well, respected a lot, and liked very much. And Dan gives me the same basic shtick the next day, but with one important added note. He goes, Roger, you know, we’re a platform, we’re not a media company, so as such we’re not responsible for what third parties do on the platform. ***And we go back and forth roughly once a day up until right before the election.***

Then the election happens, and I’m apoplectic. At this point I go, okay, guys, I’m sorry, you have played a role here. We don’t know exactly what the role is, but the platform has been used. It’s been used in Brexit, it’s been used in the U.S. election.

²⁹² *Id.* at 24:1-23.

And Dan’s going, no, no, no, you don’t understand, we’re a platform, we’re not a media company, we’re not responsible.

279. McNamee’s discussions with Rose, Zuckerberg and Sandberg continued from October 30, 2016 through February 2017—approximately four months. “And so, I’m sitting there thinking to myself, I mean, Trump won because of really *spectacularly well-executed voter suppression*, and Facebook played a role”—McNamee recalled—“So I wouldn’t let go. And I think I got up to maybe 15 or 16 different examples of situations where they had contributed to bad actors, you know, harming innocent people.”

2. McNamee’s Discussions with Zuckerberg, Sandberg and Rose Reveal that “Senior Management Knew” Facebook Had Embedded Three Employees Inside the Cambridge Analytica War Room

280. Cambridge Analytica was one such “bad actor” that McNamee discussed with Rose, Zuckerberg and Sandberg; in fact, Cambridge Analytica repeatedly surfaced in the news over the October 27, 2016—February 2017 period. The *Bloomberg* and *Washington Post* October 27, 2016 articles (¶¶248, 267-680) and numerous other articles related directly to McNamee’s “voter suppression” concerns.²⁹³ On November 8, 2016, Cambridge Analytica’s top data scientist, who was in the same war room as the Facebook embeds, shared a number of social media posts corroborating McNamee’s concerns and further

²⁹³ See, e.g., McKenzie Funk, Cambridge Analytica and the Secret Agenda of a Facebook Quiz, *N.Y. Times* (Nov. 19, 2016) (Reporting: “In this election, [Facebook] dark posts were used to try to suppress the African-American vote.”).

supporting the conclusion that the voter suppression campaign was no secret inside of Project Alamo.²⁹⁴ Matt Oczkowski and the rest of the team were able to figure out voter statistics by race in real time because, as his data partner at Project Alamo (Molly Schweikert) would later admit, they used Facebook user identification data to pull reports on voters as they turned in ballots. ¶233 n.238.

281. During the October 2016-February 2017 period, McNamee learned that Facebook’s “senior management knew” they had employees embedded in the Trump campaign working on the dataset that Cambridge Analytica had misappropriated:

McNamee: In roughly June 2016, “they embed three employees in the Trump campaign working in a war room in the San Antonio data office of Trump working side by side with Cambridge Analytica people on this gigantic dataset that was obviously *the same one that had been misappropriated by Cambridge Analytica* two years earlier.”

“And here’s the thing: *The top management of Facebook knew* they had employees embedded in the campaign, *everybody knew* that Cambridge Analytica was working for Trump, and there *wasn’t enough*

²⁹⁴ On November 8, 2016, Cambridge Analytica’s lead data scientist inside Project Alamo posted to his Twitter account: (1) “Lower African American turnout, coupled with not enough Hispanic turnout to make up the difference, and an increase in rural voters = win”; (2) “In states like Florida and North Carolina Hispanics did not break enough towards Clinton (not anti-trump enough) to make up the difference”; and (3) “States like Iowa, Wisconsin, Michigan, and Indiana all benefited from this boost. Some will call like ‘brexit-like.’”

time between December [2015] and June [2016] to recreate that dataset.”²⁹⁵

282. McNamee did, in fact, have personal knowledge of what “top management of Facebook knew” regarding Cambridge Analytica’s misuse of stolen data because McNamee personally spoke with Zuckerberg, Sandberg and Rose about that subject and others from October 30, 2016 through February 2017.

3. Unbeknownst to McNamee, Cambridge Analytica Benefited from Zuckerberg’s and Sandberg’s Selective Policy Enforcement Model that Rose Helped Set Up

283. Zuckerberg’s and Sandberg’s decision to appoint Rose as their representative in their dealings with McNamee bears upon scienter. **First**, Rose ran the team that rejected and overrode the rejection of the GSR Quiz App; and the team that subsequently “whitelisted” the Quiz App. §IV.D.4.-8. Rose also helped put Zuckerberg and Sandberg’s “whitelisting” (selective policy enforcement) business model into action.²⁹⁶ **Second**, there is evi-

²⁹⁵ Transcription, *From Mentor to Activist: Facebook Through the Eyes of Roger McNamee*, Real Vision Finance, YouTube (Apr. 13, 2019) at 30:4-15.

²⁹⁶ See, e.g., Six4Three Documents, Ex. 159 at FB-01368452 (August 15, 2012 Facebook email from Rose about a presentation point “Develop partnerships with value-added 3rd-party services to supply data in exchange for revenue-share and/or equity” in response to an email string noting “Dan, I left Sheryl off this on the assumption that you will share with her tomorrow at your 1:1”); Six4Three Documents, Ex. 41 at FB-01369065 (November 8, 2012 Facebook email among Rose, Justin Osofsky and others (attaching powerpoint) (noting “friend” data in top category of information downloaded by developers); Six4Three Documents, Ex. 41 at FB-01369070 (ranking the

dence that, in carrying out Zuckerberg’s selective enforcement vision, Rose worked with other senior executives at Facebook to move the policy enforcement reporting line away from General Counsel Colin Stretch (“Stretch”) and into the business teams.²⁹⁷ **Third**, Rose

“PR risk” associated with various data monetization approaches); Six4Three Documents, Ex. 41 at FB-01369072 (“siz[ing] the FB revenue opportunity” associated with charging five developers “access to our friends API”); Six4Three Documents, Ex. 41 at FB-01369086 (quantifying the number of times that 30 app developers pull “friend” data at 1,328,800,000 per week); Six4Three Documents, Ex. 46 at FB-00948764-8765 (November 16, 2012 Facebook email/message among Zuckerberg, Vernal, Rose and others) (regarding the “PBM” (Platform Business Model) that “comes down” to three choices including “paid friends [data], categorical [data] reciprocity for all, total [data] reciprocity for big guys/competitors” and noting, to Zuckerberg, “the ball is in your court on this one”); Six4Three Documents, Ex. 64 at FB-00948264 (November 12, 2012 Facebook email amongst Zuckerberg, Sandberg, Rose, Justin Osofsky and others discussing “premium read/engagement” and discussing all the changes as “Platform 3.0” as they “really represent[] a substantial relaunch of platform”).

²⁹⁷ For example, one of Rose’s business colleagues (Justin Osofsky) (*Facebook VP of Global Operations and Media Partnerships Kurt Wagner & Rani Molla, Mark Zuckerberg’s birthday photo shows the 20 Facebookers you should know not named Mark Zuckerberg*, Vox (May 16, 2017)) wrote to Rose: “I’m also working with Colin [Stretch] to develop a more proactive and strategic approach to enforcement in competitive **and other key contexts**.” Six4Three Documents, Ex. 50 at FB-01368116. Rose then reported to his team that “Monika Bickert” was “moving **from** Colin Stretch’s [legal] team over **to** Justin’s [Osofsky’s business] org **to lead** global policy enforcement.” Six4Three Documents, Ex. 51 at FB-01370736; *see also* Six4Three Documents, Ex. 73 at FB-00061223 (Facebook internal email among Hendrix and others regarding “Proactive and Reactive removal of permissions” to access data via Facebook’s API, and stating: “We **enforce** L10 **sparingly**, often only after extensive consultation with Justin [Osofsky] on a case-by-case basis”). Monika Bickert ran “Developer Policy Enforcement” from 2013-20 (Monika Bickert,

understood the purpose of Zuckerberg and Sandberg’s selective policy enforcement was to make money or extract value from third parties who were violating Facebook’s stated policies, provided those third parties drove “sharing” or user engagement on Facebook.²⁹⁸ Zuckerberg long tied enforcement of all policies to business factors; he wrote: “in any model, I’m assuming we enforce our policies against competitors much more strongly.”

284. Zuckerberg and Sandberg’s selective policy enforcement business model had a \$250,000 threshold. Third parties who violated policies but drove value back to Facebook in excess of that threshold enjoyed two policy enforcement options—no enforcement, or slow enforcement.²⁹⁹ Facebook’s political (“policy”) team was keen to

LinkedIn)—the business unit involved directly in the recidivist misconduct leading to the FTC’s \$5 billion punishment of Facebook. “Developer Policy Enforcement” is listed as one of the teams involved in the Cambridge Analytica investigation.

²⁹⁸ See, e.g., Six4Three Documents, Ex. 51 at FB-01370735 (“Mark’s [Zuckerberg’s] insight about the purpose of our platform is important for people to internalize: [quoting Zuckerberg]: ‘There’s a clear tension between platform ubiquity and charging, so it’s important to first fully explore what we’re trying to get out of platform. The answer I came to is that we’re trying to enable people to share everything they want, and to do it on Facebook. Sometimes the best way to enable people to share something is to have a developer build a special purpose app or network for that type of content and to make that app social by having Facebook plug into it. However, that *may be good for the world but it’s not good for us* unless people also share back to Facebook and that content increases the value of our network. So ultimately, I think *the purpose of platform—even the read side—is to increase sharing back into Facebook.*’ This insight leads to the reciprocity requirement where developers who pull data from FB must allow those people to push data from the app back to FB.”).

²⁹⁹ As the FTC found after an investigation based upon a review of internal Facebook documents and interviews of Facebook witnesses: “Facebook relied on administering consequences for policy violations

make money by “relaxing” policies.³⁰⁰ Cambridge Analytica’s \$75-\$85 million in Facebook ad purchases was over **300 times** larger than the amount necessary to persuade Facebook’s business team to slow-enforce or not enforce any of its policies against Cambridge Analytica. Facebook’s political team in Washington DC was responsible for driving this revenue, revenue that Sandberg had referenced several times in 2016 on investor calls as a “big deal.” ¶180.³⁰¹

that came to its attention after third-party developers had already received the data,” but that “the severity of consequences that Facebook administered to third-party developers for violating the company’s Platform Policies, **and the speed** with which such measures were effectuated, took into account the financial benefit that Facebook considered the developer to offer to Facebook.” FTC Complaint at ¶123. “As internal Facebook documents explained, Facebook would contact apps spending more than \$250,000 on advertising and ask them to confirm the need for the data they were accessing, while Facebook would terminate access for apps spending less than \$250,000.” *Id.* at ¶90.

³⁰⁰ See, e.g., Six4Three Documents, Ex. 179 at FB-00109951 (Facebook internal email to Public Policy team, including Elliot Schrage, concerning “Policy Management” and noting “This targeting capability is only currently available for dating, but the ads product team is working to expand it to other verticals (**like political**) and make it available via self-serve. This is a big win for the dating vertical specifically, but also **supports our efforts to examine ‘good’ revenue opportunities resulting from policy relaxation/changes.**”).

³⁰¹ Facebook’s Republican political team in Washington, DC—including Harbath, FB1, and Barnes—helped develop a business relationship with Cambridge Analytica, in particular, from at least summer 2015 through the November 2016 election. Harbath personally met with Kaiser to discuss business opportunities with Cambridge Analytica from time to time, and members of Facebook’s political team in DC regularly visited Cambridge Analytica’s offices with a view to selling ads to Cambridge Analytica’s political clients and sharing, with Cambridge Analytica, the Facebook tools that Cambridge Analytica could use to that end.

4. During the Period When He Was Discussing “Bad Actors” Like Cambridge Analytica with McNamee, Rose Presents at the DLD Conference in Germany—One Day After Cambridge Analytica’s Presentation at DLD

285. In November 2016—while McNamee continued to plead with Zuckerberg, Sandberg and Rose to take responsibility for their role in Cambridge Analytica’s data misuse—reporters asked Sandberg and Schrage’s communications team about the investigation that they had told *The Guardian* they were conducting into Cambridge Analytica starting a year earlier.³⁰²

286. The media continued to press the communications team for answers into early 2017. In January 2017, Facebook and Cambridge Analytica sent representatives to a popular tech conference in Munich, Germany, known as “DLD” (Digital Life Design).³⁰³ Cambridge Analytica’s Chief Data Officer, Tayler, represented his company on

³⁰² SEC Complaint at ¶47 (“Beginning in November 2016, reporters asked Facebook about the investigation that the company said it was conducting in the December 2015 *Guardian* article. These inquiries were referred to Facebook’s communications group, which was aware that the company had confirmed that the researcher had improperly transferred personality profiles based on U.S. user data to Cambridge in violation of Facebook’s policy, and had told both parties to delete the data.”).

³⁰³ Digital Life Design (<https://www.dld-conference.com/about>) (“While DLD has evolved from a single event into series of conferences and events throughout the years, we make sure to always preserve the atmosphere of an intimate gathering of friends through a highly curated, “by invitation only” application process for attendees. Our annual conference in Munich each January, shortly before the World Economic in Davos, is internationally renowned for attracting the best and the brightest in the world of digital.”).

January 15, 2017; Rose represented Facebook on January 16, 2017. The presentations were in Q&A format.

287. Tayler’s presentation focused on Cambridge Analytica’s work on the Trump campaign, which was particularly relevant to the audience in Munich at the time. A popular German-language magazine, *Das Magazin* had published an article in its December 2016 edition, titled (in its English translation) “The data that turned the world upside down.”³⁰⁴ The article relied on accounts from Michal Kosinski expressing his concerns about the way that Cambridge Analytica had commercialized his “likes” data modelling—the modelling that Facebook’s internal investigation had called “solid science” about a year earlier. By December 2016, Kosinski was teaching at Stanford University; that is where he was working in December 2015, when he warned Facebook’s investigation team about how Kogan’s activities brought his field “disrepute.”

288. In this context, the first question that Tayler’s moderator posed was: “Now, can I see by a show of hands, how many people in this room have read about Cambridge Analytica in the last, probably, 30 days?” Many responded in the affirmative:



289. When questions arose about *Das Magazin* article, Tayler responded that Kosinski was “an opportunist

³⁰⁴ Hannes Grassegger & Mikael Krogerus, *The Data That Turned the World Upside Down*, Motherboard (Jan. 28, 2017).

who’s using this [situation as] an excuse to raise his own profile.”³⁰⁵ Cambridge Analytica’s responded on the record, as *Das Magazin* published:³⁰⁶

In a statement after the German publication of this article, a Cambridge Analytica spokesperson said, “Cambridge Analytica does not use data from Facebook. It has had no dealings with Dr. Michal Kosinski. It does not subcontract research. It does not use the same methodology. ***Psychographics was hardly used at all.*** Cambridge Analytica did not engage in efforts to discourage any Americans from casting their vote in the presidential election. Its efforts were solely directed towards increasing the number of voters in the election.”

Facebook’s embeds and investigation team, including Rose, knew all of Cambridge Analytica’s statements to *Das Magazin* were false or misleading. In fact, Cambridge Analytica used misappropriated “likes” data and models that generated psychographics based upon Kosinski’s paper, which, as Facebook’s internal documents show, was “solid science”—according to Facebook’s investigation team. ¶164.

290. Rose presented at the DLD conference the next day. On January 16, 2017, Rose made his remarks at DLD—in a Q&A format, with the moderator and audience members asking a number of questions relating to the 2016 U.S. presidential election.

³⁰⁵ Transcription, *It’s Personal! Your Real Relationship with Data*, Digital Life Design Conference, YouTube (Jan. 22, 2017) at 10:16-17.

³⁰⁶ Hannes Grassegger & Mikael Krogerus, *The Data That Turned the World Upside Down*, Motherboard (Jan. 28, 2017).



291. The moderator raised questions about how Facebook dealt with “bad actors” who disseminated misleading or absurd information such as “Hillary Clinton is a lizard.” The moderator asked, “how much of that is being manipulated by others and how aware are you of that and how aware can you make us aware of that?”³⁰⁷

We want to give as much voice to as many people in the world. That’s really important. That’s part of our mission. We also want to have a safe environment so that people feel comfortable being on Facebook and communicating on Facebook. And so we’ve always had community standards and we have values that we have articulated around our newsfeed—the things that we think are important to keep Facebook safe and make people feel comfortable there.

I think that there’s always a tension, clearly, but the way that we have navigated that tension is by stating our values clearly and, at the same time, understanding that our role is to give voice to people.

Now, I will say that, within that, we’ve always teams of people at Facebook that deal with bad actors, right. We’re a huge target for spam, we don’t want people on

³⁰⁷ *Highlights—Friending The News (Dan Rose, Facebook & Jeff Jarvis, CUNY/Buzzmachine)—DLD17, DLD Conference, YouTube (Jan. 16, 2017); Friending The News (Dan Rose, Jeff Jarvis)—DLD17, DLD Conference, YouTube (Jan. 23, 2017).*

Facebook being fished, and we have experience dealing with bad actors whose sole intention is to manipulate the system, and one of the lessons you learn in dealing with bad actors is you don't tell them how you're dealing with them because it just informs them and helps them manipulate the system better. ***So to some extent some of that we do that without being as open about it because we know that's just going to teach the bad actors how to get around it.***

Facebook's internal documents referred to Cambridge Analytica's data misuse as a kind of "bad actor" conduct—it suspected the "bad actor" conduct in September 2015 and learned more facts about Cambridge Analytica's fraudulent certification and continuing data misuse thereafter. It was a "bad actor," as Facebook defined it.³⁰⁸

292. Rose's statement (highlighted above) was false or misleading because the most prominent, alleged "bad actor" in Germany at the time—as evidenced by the popular *Das Magazin* article—was Cambridge Analytica. In truth, Facebook was not "open" about Cambridge Analytica's actions because Facebook was complicit in the bad actions—by overruling its own App Review rejection; by throttling and then un-throttling data that the Quiz App never needed; by allowing Cambridge Analytica to run ads that violated Facebook's ads policies; by "whitelisting" the Quiz App so that it could take one last bite from "friends data"; by actively concealing the fact of Cam-

³⁰⁸ Sept. 2015-May 2016 Facebook email thread at 9 (discussing "plenty of bad actor behavior" in the political space, where political vendors were moving Facebook users' data off the platform, figuring out who the users were in real life, and then appending those users' "data" (personal information) to the voting records of those users for political purposes).

bridge Analytica’s policy-violating harvest even after Facebook learned its December 2015/January 2016 “certification” was a fraud; by helping Cambridge Analytica execute a voter suppression campaign that rested on the misappropriated data; by giving Cambridge Analytica special marketing “partner” privileges; by giving Cambridge Analytica “embeds” who saw the continuing violations (or readily inferred them) but did not stop Cambridge Analytica; and by overlooking all of Cambridge Analytica’s policy violations in the context of a selective enforcement model that Zuckerberg and Sandberg created. Under the circumstances, Rose’s statement was false and misleading at the time, as he knew or should have known.

5. Journalist Carole Cadwalladr Recalls, “Facebook’s Press Team Lied to Me in February 2017”—the Last Month of Zuckerberg’s, Sandberg’s and Rose’s Discussions with McNamee

293. In February 2017, reporters continued to press Facebook for updates on its investigation into Cambridge Analytica. Facebook’s “communications group initially responded to the press inquiries indirectly. For example, beginning in February 2017, the communications group pointed reporters to Cambridge’s public statement that it ‘does not use data from Facebook’ and ‘does not obtain data from Facebook profiles or Facebook likes.’”³⁰⁹ Specifically, in February 2017, Facebook’s communications group directed reporters to this statement from the *Das Magazin* article that was published in English in two sources at the end of January.³¹⁰

³⁰⁹ SEC Complaint at ¶48.

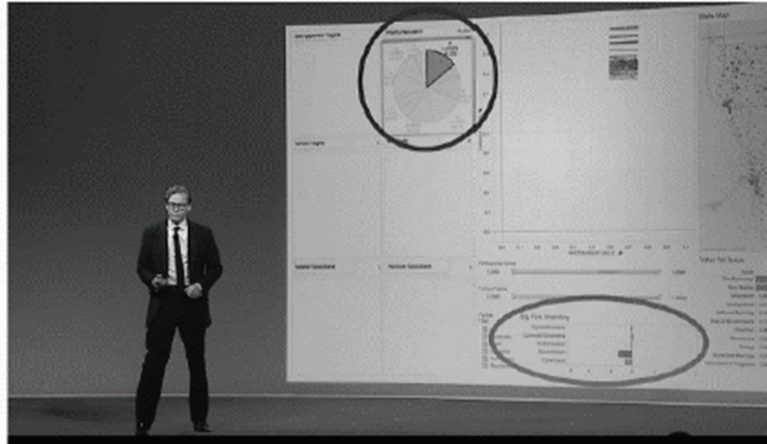
³¹⁰ Hannes Grassegger & Mikael Krogerus, *The Data That Turned the World Upside Down*, Motherboard (Jan. 28, 2017).

“Cambridge Analytica does not use data from Facebook. It has had no dealings with Dr. Michal Kosinski. It does not subcontract research. It does not use the same methodology. Psychographics was hardly used at all. Cambridge Analytica did not engage in efforts to discourage any Americans from casting their vote in the presidential election. Its efforts were solely directed towards increasing the number of voters in the election.”

The “communications group”—including Schrage and Sandberg—read that article because Schrage and Sandberg were responsible for addressing Facebook’s relationship with Cambridge Analytica in public communications. ¶¶161-162.

294. It follows that Facebook’s Cambridge Analytica investigation team—likely for the second time—saw Nix’s September 2016 presentation at the Concordia Summit. The *Das Magazin* article discussed that presentation over the course of eight paragraphs, linked to a video of the presentation on line, and included an image from Nix’s Concordia presentation focusing on its psychographic scoring dashboard:³¹¹

³¹¹ *Id.*



ALEXANDER NIX AT THE 2016 CONCORDIA SUMMIT IN NEW YORK. IMAGE: CONCORDIA SUMMIT

Nix shows how psychographically categorized voters can be differently addressed, based on the example of gun rights, the 2nd Amendment: "For a highly neurotic and conscientious audience the threat of a burglary—and the insurance policy of a gun." An image on the left shows the hand of an intruder smashing a window. The right side shows a man and a child standing in a field at sunset, both holding guns, clearly shooting ducks: "Conversely, for a closed and agreeable audience. People who care about tradition, and habits, and family."

295. The *Das Magazin* article included extensive reporting about an interview with Kosinski (previously at Cambridge University in 2014, but teaching at Stanford University by late 2015). Kosinski suspected that Cambridge Analytica had used its Facebook “likes” model. The *Das Magazin* article referred to Facebook “likes” approximately 18 times and discussed his “likes” modelling, and reported that Facebook made a “threat of a lawsuit and a job offer” to Kosinski on the date that he published his “likes” research, which rested “on an average of 68 Facebook ‘likes’” from a group of volunteers.³¹² The article brought up Kogan’s work again—Kogan had changed his name to “Spectre” and was living in Singapore at the time. But the *Das Magazin* article did not refute Kogan’s prior assertions that he only obtained “a couple thousand” survey responses from Facebook users in some “anonymous”

³¹² *Id.*

form. ¶154. Kogan’s prior representations painted a picture of a miniscule data set in comparison to the one that Kosinski had relied upon—from “58,000 volunteers who provided their Facebook Likes.”³¹³

296. On or around February 28, 2016, Schrage and Sandberg’s Cambridge Analytica communications team pointed Carole Cadwalladr (“Cadwalladr”), in particular, to Cambridge Analytica’s false statements in the *Das Magazin* article in February 2017. Cadwalladr was investigating Cambridge Analytica’s role in the Brexit and Trump elections at the time.³¹⁴ Regarding the Brexit campaign, Cadwalladr interviewed an official from one of the groups advocating in favor of Brexit, Andy Wigmore, who told Cadwalladr that “Cambridge Analytica had worked for them” and that “Facebook was the key to the entire campaign”—a “Facebook ‘like’, he said, was their most ‘potent weapon.’” This was the context in which Facebook’s communications team directed Cadwalladr and others to Cambridge Analytica’s statements in *Das Magazin*.

297. Cadwalladr—a Pulitzer Finalist for her Cambridge reporting—would later reflect: “**Facebook’s press team lied to me in February 2017.**”³¹⁵ Cadwalladr kept investigating.

³¹³ Michael Kosinski, David Stillwell & Thore Graepel, *Private traits and attributes are predictable from digital records of human behavior*, *Procs. of the Nat. Acad. of Sci. of the U.S.A.* 110, 5802 (2013).

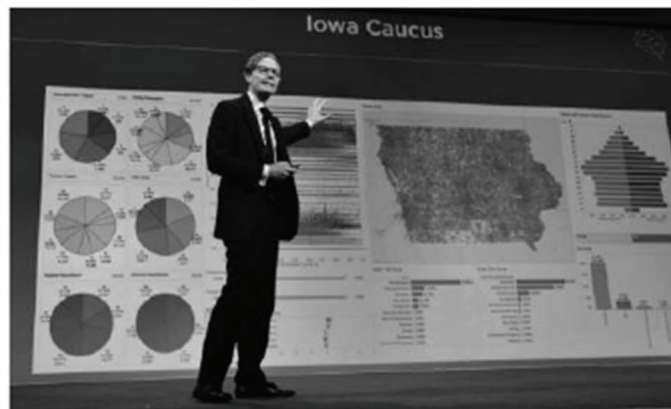
³¹⁴ See, e.g., Carole Cadwalladr, *Robert Mercer: the big data billionaire waging war on mainstream media*, *Guardian* (Feb. 26, 2017).

³¹⁵ David Uberti, *Facebook Misled Journalists About How Bad the Cambridge Analytica Scandal Was*, *Vice News* (July 25, 2019); Carole Cadwalladr (@carolecadwalla), *Twitter* (July 25, 2019 9:41 AM); Carole Cadwalladr, *What happened when Alexandria Ocasio-*

K. Facebook’s Materially False and Misleading Statements About Its Investigation into Cambridge Analytica

1. The March 4 and 5, 2017 Statements Were Materially False and Misleading, as Facebook’s “Spokesperson” Knew in the Most Direct Way

298. On March, 4, 2017, Cadwalladr published yet another report concerning Cambridge Analytica’s political activities in *The Guardian*. The article, titled: “Watchdog to launch inquiry into misuse of data in politics,” included a photograph of Nix making its presentation at the 2016 Concordia Summit:³¹⁶



Alexander Nix speaks at the 2016 Concordia Summit at the Grand Hyatt in New York on 19 September 2016. Photograph: Bryan Bedder/(Credit too long, see caption)

299. Facebook’s investigation team saw this image—just as they had seen a video of that presentation in September 2016—and were reminded of that presentation in

Cortez came face to face with Facebook’s Mark Zuckerberg, Guardian (Oct. 26, 2019); Finalist: Staff of the New York Times with contributions from Carole Cadwalladr of The Guardian/The Observer of London, Pulitzer.org.

February 2017 when they “pointed” reporters to Cambridge Analytica’s misleading statements in that report. Nonetheless, as *The Guardian* reported: “A Facebook spokesperson said: ‘Our investigation to date has **not uncovered anything that suggests** wrongdoing with respect to Cambridge Analytica’s work³¹⁶ on the Leave and Trump campaigns.’”³¹⁷ Cadwalladr later wrote, with respect to Facebook’s (above) statement: “**Because we know Facebook lied.** The SEC investigation says that. To us at the Observer, in fact ‘. . . when asked by reporters in 2017 about its investigation into the Cambridge Analytica matter, Facebook falsely claimed the company found no evidence of wrongdoing.’”³¹⁸

300. Facebook’s March 4, 2017 statement—“Our investigation to date has not uncovered anything that suggests wrongdoing with respect to Cambridge Analytica’s work on the Leave and Trump campaigns”—was materially false and misleading, as Facebook’s “investigation” demonstrated, and as Facebook’s “spokesperson” knew given the fact that the “spokesperson” referenced the investigation in its statement. The statement was false and misleading when made for numerous reasons because Facebook’s investigation into Cambridge Analytica discovered serious policy violations and wrongdoing, which Facebook knew by January 2016:

³¹⁶ Jamie Doward, Carole Cadwalladr & Alice Gibbs, *Watchdog to launch inquiry into misuse of data in politics*, *Guardian* (Mar. 4, 2017).

³¹⁷ Jamie Doward, Carole Cadwalladr & Alice Gibbs, *Watchdog to launch inquiry into misuse of data in politics*, *Guardian* (Mar. 4, 2017).

³¹⁸ Carole Cadwalladr, *What happened when Alexandria Ocasio-Cortez came face to face with Facebook’s Mark Zuckerberg*, *Guardian* (Oct. 26, 2019).

(a) the fact that the Quiz App failed Facebook’s App Review because it was designed to take data that it did not need, implying that the data would be used for some purpose no one knew about at the time;

(b) the fact that Facebook overruled its own rejection of the Quiz App;

(c) the fact that the Quiz App took so much data that it did not need that Facebook’s engineers’ “throttled” the data transfer rate, again implying the data was going to serve some purpose other than supporting some “quiz”;

(d) the fact that Facebook “whitelisted” the Quiz App in May 2015, giving it access to “friends data,” when it was supposedly impossible for that data to leave Facebook’s server before that time; and

(e) the fact that Cambridge Analytica bought “personality scores” in violation of stated policies. All of those policy violations related directly to subsequent policy violations because they all underpin Cambridge Analytica’s desire to make money from the ill-gotten data.

301. After January 2016, Facebook learned more facts showing serious, continuing policy violations and wrongdoing, while Cambridge Analytica was working on the Trump campaign and in connection with that work, including:

(a) on June 11, 2016, the fact that Cambridge Analytica had previously submitted a fraudulent “certification” or confirmation of data deletion—the *only* “certification” that Cambridge Analytica ever submitted;

(b) over summer 2016, the fact that Cambridge Analytica continued using the ill-gotten “psychographic scores,” models and underlying data (including the Facebook User IDs);

(c) over summer and into fall 2016, the fact that Cambridge Analytica was executing a massive voter suppression campaign aimed at protected classes based upon the ill-gotten “psychographic scores” and issuing ads that violated Facebook’s ads policies;

(d) in or about September 2016—and numerous times thereafter—the fact that Cambridge Analytica admitted the Trump campaign “is using” the OCEAN score model and data, which, only Facebook knew were based on the ill-gotten data; and

(e) on or about October 27, 2016, the fact that Cambridge Analytica admitted that its methodologies relied upon Facebook “likes”—and, as Facebook learned privately, Cambridge Analytica’s modelling methodology depended on “likes” that it bought for £750,000.

302. All of these facts amount to far more than *mere* “suggestions” of wrongdoing by Cambridge Analytica in connection with its work on the Trump campaign, as Facebook told *The Guardian*, and show the statements of the Facebook “spokesperson” were materially false and misleading at the time, as the “spokesperson” knew or should have known, given the spokesperson’s specific reference to Facebook’s “investigation” into Cambridge Analytica. And Facebook’s “spokesperson” repeated that same misrepresentation at least two more times.

303. On March 5, 2017, *The Daily Mail* published a similar article and a substantially identical statement from a Facebook spokesman that “Our investigation to

date has not uncovered anything that suggests wrongdoing with respect to Cambridge Analytica’s work on the Leave and Trump campaigns.’”³¹⁹ This statement, like the March 4, 2017 statement, was false and misleading because Facebook had by then uncovered wrongdoing, as Facebook’s Cambridge Analytica “investigation” team knew. Reporters in the United States also looked into Facebook’s investigation.

2. Facebook’s March 30, 2017 Statements About Its Cambridge Analytica Investigation Were Materially False and Misleading as Facebook Knew or Should Have Known

304. On March 30, 2017, *The Intercept* published an article titled: “Facebook Failed to Protect 30 Million Users From Having Their Data Harvested by Trump Campaign Affiliate,” wherein *The Intercept* resurfaced prior reporting from December 2015.

305. *The Intercept*, in its March 30, 2017 article, wrote: “*The Guardian*, which was was [sic] the **first to report** on Cambridge Analytica’s work on U.S. elections, in late 2015, noted that the company drew on research ‘spanning tens of millions of Facebook users, harvested largely without their permission’”; but, as *The Intercept* reported: “Kogan disputed this at the time, telling *The Guardian* that his turker surveys had collected no more than ‘a couple thousand’ responses.”³²⁰

³¹⁹ Tim Sculthorpe, *Privacy watchdog launches a probe into how the Leave campaigns used voters’ personal data to win Brexit*, *The Daily Mail* (Mar. 5, 2017).

³²⁰ Mattathias Schwartz, *Facebook Failed to Protect 30 Million Users From Having Their Data Harvested by Trump Campaign Affiliate*, *The Intercept* (Mar. 30, 2017).

306. When *The Intercept* wrote its March 30, 2017, article about *The Guardian* being the “first to report” the subject, those three words hyperlinked to *The Guardian*’s December 11, 2015 article, which reported:³²¹

After this article was published, Facebook said the company was “carefully investigating this situation” regarding the Cruz campaign.

“[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,” a Facebook spokesman said in a statement to the Guardian.

The Intercept, in its March 30, 2017 article, also reported:³²²

Shortly after *The Guardian* published its 2015 article, Facebook contacted Global Science Research and requested that it delete the data it had taken from Facebook users. Facebook’s policies give Facebook the right to delete data gathered by any app deemed to be “negatively impacting the Platform.” The company believes that Kogan and SCL complied with the request, ***which was made during the Republican primary, before Cambridge Analytica switched over from Ted Cruz’s campaign to Donald Trump’s.*** It remains unclear what was ultimately done with the Facebook data, or whether any models or algorithms

³²¹ Dec. 2015 *Guardian* article.

³²² Mattathias Schwartz, *Facebook Failed to Protect 30 Million Users From Having Their Data Harvested by Trump Campaign Affiliate*, *The Intercept* (Mar. 30, 2017).

derived from it wound up being used by the Trump campaign.

In public, *Facebook continues to maintain that whatever happened during the run-up to the election was business as usual. “Our investigation to date has not uncovered anything that suggests wrongdoing,”* a Facebook spokesperson told *The Intercept*.

Facebook appears not to have considered Global Science Research’s data collection to have been a serious ethical lapse. Joseph Chancellor, Kogan’s main collaborator on the SCL project and a former co-owner of Global Science Research, is now employed by Facebook Research. “The work that he did previously has no bearing on the work that he does at Facebook,” a Facebook spokesperson told *The Intercept*.

307. Facebook’s statement—“Our investigation to date has not uncovered anything that **suggests** wrongdoing”—was materially false and misleading at the time, as the “spokesperson” knew or should have known for the substantially the same reasons that Facebook’s substantially similar “investigation” statements of March 4 and 5 statements were materially false and misleading.

308. In addition, the Facebook spokesperson’s March 30, 2017 statements breathed new life into Facebook’s December 11, 2015 prior statements about swiftly “banning” companies that mislead people or misuse user data because *The Intercept* did discuss the Trump campaign extensively, but it also discussed the root of the potential data misconduct—the 2014/2015 harvesting and sale of the data to Cambridge Analytica. Facebook privately concluded that Cambridge Analytica **had** violated its policies; yet, Facebook did **not** “ban” Cambridge Analytica,

which would lead a reasonable investor to conclude that the data never reached Cambridge Analytica's hands. Far from "banning" Cambridge Analytica, it received a promotion to preferred marketing partner status. Facebook sent "embeds" to help Cambridge Analytica conduct the Trump campaign's data operations. Facebook even let Cambridge Analytica violate its policy of "requiring deletion" by giving Facebook the fraudulent December 2015 / January 2016 "certification" or "confirmation" of deletion—a fraud that Facebook discovered no later than June 11, 2016.

309. On April 3, 2017—six months after Facebook was finished billing the Trump campaign \$75-\$85 million for ads—Facebook *still* had not obtained a written "certification" of destruction from Cambridge Analytica, other than one that was a fraud, as Facebook knew on June 11, 2016. Instead, it asked "SCL Elections Limited" to sign a throwaway piece of paper saying it had destroyed the purloined data and had not transferred the data to any other party, which was yet another fraudulent statement, as Facebook knew on April 3, 2017, because SCL *had* transferred the data to Cambridge Analytica, as Facebook had known since December 2015.

L. During the Class Period, Defendants Made False Statements Regarding User Data Control, Risks to Facebook and Compliance with the 2012 FTC Consent Decree

310. Defendants knew throughout the Class Period that third parties possessed and were misusing sensitive user information. Indeed, defendants knew that Kogan had sold user data to Cambridge Analytica in violation of Facebook's policies. Defendants were also aware of Facebook's own practice of secretly "whitelisting" third parties, including multiple major corporations, for continued

access to users' friends' data after that access was supposedly shut down. They further knew that Facebook was overriding users' privacy settings. Nonetheless, defendants assured the public that Facebook users could "control" their data, that the Company faced only hypothetical risks of data misuse, that defendants had found no wrongdoing in their investigation of Cambridge Analytica and that defendants had not violated the FTC Consent Decree. These statements were false.

1. Defendants Falsely Stated that Users Controlled Their Data

311. Facebook and the Executive Defendants repeatedly stated during the Class Period that Facebook users controlled their data on Facebook. These statements were designed to inspire trust in Facebook by assuring the public (including investors) that Facebook respected user privacy and only shared its users' data with users' knowledge and consent. On multiple occasions during the Class Period, Zuckerberg, Sandberg and Facebook expressly assured the public that Facebook users had control of their own data, that Facebook was not sharing sensitive user data with third parties, and that Facebook was not overriding user privacy settings.

312. On October 12, 2017, for example, Sandberg gave an interview to *Axios* in which she stated: "[W]hen you share on Facebook, you need to know" that "no one is going to get your data that shouldn't have it" because "***you are controlling who you share with.***"³²³ On April 4, 2018,

³²³ Mike Allen, *Exclusive interview with Facebook's Sheryl Sandberg*, *Axios* (Oct. 12, 2017).

Zuckerberg likewise stated: “[Y]ou have control over everything you put on the service.”³²⁴ This statement was reiterated on Facebook’s website in an April 24, 2018 post stating: “[It’s] important to know that ***you are in control*** of your Facebook, what you see, what you share, and what people see about you.”³²⁵

313. On April 10, 2018, Zuckerberg testified to the Joint Senate Commerce and Judiciary Committees. And he gave very precise and detailed answers assuring Congress that users controlled what information they shared, stating that “every piece of content that you share on Facebook, you own and ***you have complete control*** over who sees it and how you share it,” “that control is something that’s important,” and when “you sign up for the Facebook, you get the ability to share the information that you want” because “every person gets to control who gets to see their content.”³²⁶

314. These and similar statements detailed below (*see* §VI.A.) were materially false and misleading. In reality, throughout the Class Period, defendants knew that users did not have control over their personal data because Facebook was engaged in a massive—and secret—information sharing campaign with whitelisted app developers and business partners who were given users’ friends’ data in exchange for providing benefits to Facebook. Facebook deliberately provided this information to third parties despite the fact that: (i) Facebook users did not know

³²⁴ *Hard Questions: Q&A With Mark Zuckerberg on Protecting People’s Information*, Facebook Newsroom (Apr. 4, 2018).

³²⁵ *How to Take Control of Your Facebook*, Facebook Newsroom (Apr. 24, 2018).

³²⁶ *Transcript of Mark Zuckerberg’s Senate hearing*, Wash. Post (Apr. 10, 2018).

about and had *not* consented to the information sharing; (ii) doing so was an obvious breach of the FTC Consent Decree; and (iii) defendants themselves had stated publicly in April 2014 that such information was *not* being shared.

315. As extensively detailed in the FTC Complaint filed in connection with Facebook’s record-breaking \$5 billion settlement with the FTC, Facebook’s own admissions to the United States Senate, news reports, and other disclosures the Company was illicitly sharing reams of sensitive user data with third parties without user knowledge or consent while making contrary representations to the public.

316. The FTC Complaint explains that that from “April 30, 2015, to *at least June 2018*,” Facebook falsely stated that users could “control” the privacy of their data “by using Facebook’s desktop and mobile privacy settings to limit to their Facebook Friends the information that Facebook could share.” In reality, “regardless of the privacy settings a user checked, Facebook continued to provide access to [user friend data] to Whitelisted Developers.”³²⁷

317. These Whitelisted Developers included dozens of “gaming, retail, and technology companies, as well as third-party developers of dating apps and other social media services.”³²⁸ As the FTC charged: “Facebook did not tell its users that it was still granting these Whitelisted Developers access to their data,” and users “had no way

³²⁷ See FTC Complaint at ¶¶173-174; *see also generally id.* at ¶¶106-113, 166-175.

³²⁸ *Id.* at ¶108.

of knowing that Facebook would still share it with these Whitelisted Developers.”³²⁹

318. This special access allowed specifically approved third parties, including app developers and mobile device makers, to “access user data without permission” including by allowing them to “circumvent users’ privacy [or] platform settings and access Friends’ information, even when the user disabled the Platform.”³³⁰

319. Relatedly, an investigation by *The New York Times* revealed that, during the Class Period, Facebook had “struck agreements allowing phone and other device makers access to vast amounts of its users’ personal information.” As set forth in the article, Facebook allowed **at least 60** phone and other device makers continued access “to the data of users’ friends without their explicit consent” throughout 2017 and 2018—“even after [Facebook] declar[ed] that it would no longer share such information with outsiders.”³³¹ *The New York Times* reported that Facebook entered into these whitelisting agreements with dozens of third parties such as **Apple, Amazon, BlackBerry, Microsoft and Samsung**—which “allowed Facebook to expand its reach.” Further, “most” of these relationships “remain[ed] in effect” in June 2018 (with Facebook starting to wind down some in April 2018). According to the article:³³²

[T]he partnerships, whose scope has not previously been reported, raise concerns about the company’s

³²⁹ FTC Complaint at ¶¶112-113.

³³⁰ U.K. Parliamentary Comm. Final Rep. at 28.

³³¹ Nicholas Confessore, Gabriel J.X. Dance and Michael LaForgia, *Facebook Gave Device Makers Deep Access to Data on Users and Friends*, N.Y. Times (June 3, 2018).

³³² *Id.*

privacy protections and compliance with a 2011 consent decree with the Federal Trade Commission. Facebook allowed the device companies access to the data of users' friends without their explicit consent, even after declaring that it would no longer share such information with outsiders. Some device makers could retrieve personal information even from users' friends who believed they had barred any sharing, The New York Times found.

320. Even Facebook itself has admitted, in response to written questions from Congress, that certain of these "whitelisting" relationships, including with Tobii, Apple and Amazon, continued through at least October 2018.

321. The fact that Facebook was overriding users' privacy settings in order to provide these third parties with data contradicted defendants' Class Period statements and violated the 2012 FTC Consent Decree, which required the Company to obtain express consent before enacting changes that overrode users' privacy preferences. This practice also violated Parts I.B and I.C of the FTC Consent Decree, which, as discussed above, prohibited Facebook from misrepresenting the extent to which users could control their data and the extent to which Facebook makes user data available to third parties.

322. One of the sources for *The New York Times*' reporting, Ashkan Soltani ("Soltani"), a former Chief Technology Officer of the FTC (who also worked on the FTC's 2011 investigation into Facebook), reported that: "Whitelisted 'partners' could access friend's non-public profile information including religion, birthday, political affiliation, location even with 'platform settings' (Apps, Websites, and Games) was turned off . . . @Facebook 'whitelisted' platform partner's apps by automatically registering them as 'installed' for a given user's friends (is_app_user

= true) in the platform API, **overriding users' privacy settings**.”³³³ Soltani further explained that “a tell-tale sign of an @FTC-like problem is when the legal department updates the data use policy to ‘clarify’ that these arrangements existed after a press inquiry.” He pointed to Facebook’s “clarification between” May 20, 2018, and June 3, 2018.

323. In testimony to the U.K. Parliamentary Committee (the “Soltani Test”), Mr. Soltani also confirmed that: “As recently as June 2018, using the Blackberry token that *The New York Times* was testing with, which was provided to me, I was able to access user data **in lieu of a user's platform settings**.”³³⁴

324. He further testified: “. . . based on *The New York Times* reporting and my testing, [user friend data] was still accessible to certain apps—at least the whitelisted apps that we tested” after Facebook and Zuckerberg had announced in 2014 that it would no longer be available.³³⁵ Indeed, Mr. Soltani confirmed that Facebook “**allowed whitelisted apps to completely override [platform] setting[s] altogether**”³³⁶ and did so for nearly a decade through 2018:

Jo Stevens: So we are effectively talking about, in the case of whitelisted apps, potentially nine years—nearly a decade—when they have been able to access—

Ashkan Soltani: Friends' information.

³³³ Ashkan Soltani (@ashk4n) TWITTER (June 4, 2018).

³³⁴ Soltani Test at Q4333.

³³⁵ *Id.* at Q4335.

³³⁶ *Id.* at Q4342.

Jo Stevens:—friends’ information, overriding privacy settings?

Ashkan Soltani: That’s right; I believe so, yes.³³⁷

325. In connection with his testimony to the U.K. Parliamentary Committee about Facebook’s improper whitelisting practices, Soltani identified Sandberg as the Facebook executive responsible for making the decision to engage in this practice. Soltani testified:³³⁸

My understanding is that a lot of these decisions [including whitelisting and overriding privacy settings] are [Ms. Sandberg’s]. She is the one who makes the monetization calls and makes the priorities, and that is who I would want to see up here testifying on these business decisions, and specifically on the monetization and decisions of what to prioritize.

326. The Six4Three Documents discussed above also show that whitelisting was widespread. For example, an internal Facebook email exchange dating from November 2013 reveals that Facebook had at least “5,200 existing whitelisted apps.”³³⁹

327. This unauthorized information sharing program included foreign companies with close ties to foreign governments. On June 5, 2018, *NBC News* reported that Facebook had improperly shared user data with “Chinese companies believed to be national security risks.”³⁴⁰ Under pressure from members of Congress, Facebook later

³³⁷ *Id.* at Q4343.

³³⁸ *Id.* at Q4348.

³³⁹ Six4Three Documents, Ex. 100 at FB-00521473.

³⁴⁰ Alyssa Newbomb, *Sen. Bill Nelson asked: “What in the world is next? And what in the world is going to protect American’ personally identifiable private information?”, NBC News* (June 6, 2018); *see also*

revealed that it had “integrations” under which it shared users’ data with Chinese companies Lenovo, OPPO, and TCL.³⁴¹

328. On June 5, 2018, *The Washington Post* reported that:³⁴²

Facebook admitted Tuesday that it allowed Huawei, a Chinese telecom company with alleged ties to the country’s government, to have special access to data about the social site’s users, an arrangement that could stoke fears that consumers’ personal information is at risk.

The relationship between Facebook and Huawei was one of the special agreements brokered between the social giant and device makers over the past decade that sought to make it easier for Facebook users to access site services on a wide array of technologies.

For years, lawmakers in Congress and top U.S. national security officials have raised red flags about the security of Huawei products, fearing that the Chinese government could demand access to communications stored on their devices or servers. The company has denied the charges, but the Pentagon took the rare step this year of banning sales of Huawei smartphones on U.S. military bases.

Ben Brody & Steven Dennis, *Senators Aim to Call Facebook, Google, Twitter to Hearings*, Bloomberg (June 7, 2018) (quoting Sen. Cornyn: “Huawei is a ‘Chinese national-security threat to the United States and any collaboration there is a problem’”).

³⁴¹ See Ben Brody & Sarah Frier, *Facebook Discloses It Shared Data With Chinese Device Makers*, Bloomberg (June 6, 2018).

³⁴² Tony Romm, *Facebook granted devices from Huawei, a Chinese telecom firm, special access to social data*, Wash. Post (June 5, 2018).

The Washington Post further reported that “the social media giant quietly ***began unwinding*** the program in April”—that is, ***April 2018***.

329. On June 8, 2018, *The Wall Street Journal* reported that even more companies than previously reported had been whitelisted well after the point when Facebook claimed to have stopped sharing user data in this manner. As detailed in the article, which described the previously undisclosed agreements:³⁴³

Facebook Inc. [FB 0.49%] struck customized data-sharing deals that gave select companies special access to user records well after the point in 2015 that the social network has said it walled off that information, according to court documents, company officials and people familiar with the matter.

Some of those and other agreements, collectively known internally as “whitelists,” also allowed certain companies to access additional information about a user’s Facebook friends, the people familiar with the matter said. That included information like phone numbers and a metric called “friend link” that measured the degree of closeness between users and others in their network, the people said.

The whitelist deals were struck with companies including Royal Bank of Canada and Nissan Motor Co., who advertised on Facebook or were valuable for other reasons, according to some of the people familiar with the matter. They show that Facebook gave special data access to a broader universe of companies than was previously disclosed. They also raise further

³⁴³ Deepa Seetharaman & Kirsten Grind, *Facebook Gave Some Companies Special Access to Additional Data About Users’ Friends*, Wall St. J. (June 8, 2018).

questions about who has access to the data of billions of Facebook users and why they had access, at a time when Congress is demanding the company be held accountable for the flow of that data.

Many of these customized deals were separate from Facebook’s data-sharing partnerships with at least 60 device makers, which it disclosed this week. Several lawmakers and regulators have said those device-maker arrangements merit further investigation.

* * *

Privacy experts said Facebook users likely didn’t know how their data was being shared.

* * *

Eventually, Facebook set up internal teams dedicated to brokering and developing customized data deals.

330. On July 11, 2018, CNN revealed that Facebook had given a “Russian internet company with links to the Kremlin” the right:³⁴⁴

to collect data on unknowing users of the social network after a policy change supposedly stopped such collection. Facebook told CNN on Tuesday that apps developed by the Russian technology conglomerate Mail.Ru Group, were being looked at as part of the

³⁴⁴ Donie O’Sullivan, Drew Griffin & Curt Devine, *Russian company had access to Facebook user data through apps*, CNN Business (July 11, 2018).

company's wider investigation into the misuse of Facebook user data in light of the Cambridge Analytica scandal.³⁴⁵

331. A July 12, 2018 article in *The New York Times* confirmed that the same type of "rich behavioral data" provided to Cambridge Analytica was also provided to Mail.Ru Group. *The New York Times* article stated that Facebook "gave a Kremlin-linked company access to years of user data. You are right to be scared."³⁴⁶

332. Until at least early April 2018, Facebook was exposing private friends lists to third-party app developers through "taggable friends" interface on the Facebook Platform. As reported by *The Telegraph* on April 17, 2018: "Facebook exposed private friend lists to app developers without their knowledge until two weeks ago, despite claiming to have blocked the service three years ago."

333. This practice allowed apps to collect the friend lists of anybody who had installed the app, exposing their names and profile photos. Facebook quietly switched the "taggable friends" interface off on April 4, 2018, burying the announcement among a series of other privacy measures.³⁴⁷

334. In sum, contrary to defendants' Class Period representations, Facebook users did not have control over their most sensitive data. To the contrary, Facebook was

³⁴⁵ *Id.* (Donie O'Sullivan, Drew Griffin & Curt Devine, *Russian company had access to Facebook user data through apps*, CNN Business (July 11, 2018)).

³⁴⁶ Siva Vaidhyanathan, *This Russian Company Knows What You Like on Facebook*, N.Y. Times (July 12, 2018).

³⁴⁷ Margi Murphy, *Facebook quietly stopped apps from harvesting users' private data just two weeks ago*, Telegraph (Apr. 17, 2018).

deliberately shared by Facebook with dozens—and perhaps thousands—of non-parties pursuant to contractual arrangements that they had with Facebook.

2. As the SEC Found, Facebook Made Materially False Statements About the Risks Facing the Company Due to the Cambridge Analytica Scandal

335. During the Class Period, Facebook filed two Form 10-K annual reports and four Form 10-Q quarterly reports with the SEC. In each of those periodic reports Facebook included generic language stating that a risk it faced was that third parties might obtain or misuse sensitive user information. These boilerplate warnings were written as hypothetical investment risks, *i.e.*, that there **could** be injury to investors “**if**” a third party were to fail to adhere to Facebook’s guidelines because it might result in sensitive user data being “improperly accessed.”

336. For example, in its Form 10-K filed on February 3, 2017, the first day of the Class Period, Facebook stated that “**if** developers fail to adopt or adhere to adequate data security practices . . . our data or our users’ data **may be** improperly accessed, used or disclosed.”³⁴⁸ The Form 10-K also stated that “any failure to prevent or mitigate security breaches and improper access to or disclosure of our data or user data **could** result in the loss or misuse of such data, which could harm our business and reputation[.]”³⁴⁹

337. Nearly identical risk warnings were made in each subsequent Form 10-K and Form 10-Q filed by Facebook

³⁴⁸ FY 2017 Facebook, Inc. Form 10-K (Jan. 31, 2018) at 13.

³⁴⁹ *Id.*

during the Class Period. These include Facebook’s quarterly reports on Forms 10-Q for the: (1) period ended March 31, 2017 (“*if* these third parties or developers fail to adopt or adhere to adequate data security practices . . . our data or our users’ data *may be* improperly accessed, used or disclosed”); (2) period ended June 30, 2017 (same); (3) period ended September 30, 2017 (same); period ended March 31, 2018 (same); and (4) period ended September 30, 2018 (same). In addition, Facebook’s annual report on Form 10k for the fiscal year ended December 31, 2017, filed on February 1, 2018, made the same statement as well as stating “any failure to prevent or mitigate security breaches and improper access to or disclosure of our data or user data *could* result in the loss or misuse of such data, which could harm our business and reputation.”³⁵⁰

338. As confirmed by facts set forth in the recent SEC Complaint, which Facebook settled for \$100 million, Facebook knew or deliberately disregarded throughout the Class Period that each of these statements was materially false and misleading. As the SEC concluded, they acted “as a *fraud or deceit upon purchasers*” of Facebook’s securities.

339. The SEC relied upon detailed and specific evidence showing that, from at least December 2015 through March 16, 2018 Facebook knew that Cambridge Analytica had sensitive user information and was using it for improper purposes that created risks for the Company. But despite this knowledge, Facebook misled investors by repeatedly telling the market that the risks were only hypothetical.

³⁵⁰ FY 2018 Facebook, Inc. Form 10-K (Jan. 31, 2019) at 13.

340. These facts set forth in the SEC Complaint are consistent with those detailed by other sources above. *See* §IV.C.-L., *supra*.

3. Defendants Made False Statements Regarding Their Response to Cambridge Analytica’s Misconduct

341. In addition to the false and misleading statements about Facebook’s investigation into Cambridge Analytica in March 2017 (§IV.K.), Defendants also made false and misleading statements about their response to Cambridge Analytica’s misconduct.

342. When *The Guardian* first reported on the Cambridge Analytica scandal in December 2015, a Facebook spokesman was quoted in the story stating, “[W]e will take swift action against companies that [violate Facebook’s privacy policies], including banning those companies from Facebook and requiring them to destroy all improperly collected data.”³⁵¹ Moreover, Facebook’s data use policy in effect for most of the Class Period stated that Facebook would “notify our users” if Facebook “confirmed their accounts have been compromised.”³⁵²

343. As set forth above, recently-revealed facts demonstrate that these (and other statements set forth below in §VI.D.) were materially false and misleading. Contrary to their public statements during and prior to the Class Period, defendants’ response to learning December 2015 about Cambridge Analytica’s violations of Facebook policy was inadequate and primarily focused on minimizing bad publicity for Facebook rather than protecting Facebook’s users from further misuse of their

³⁵¹ Dec. 2015 *Guardian* article.

³⁵² Facebook Terms of Service (Jan. 30, 2016).

data. Facebook did not take any sort of “swift action” against Cambridge Analytica, it did not “require” Cambridge Analytica to “destroy” user data that Facebook knew it had, and it did not notify either the FTC or the 87 million users whose data was compromised.

344. **Facebook Did Not Notify Users.** The fact that Facebook should have notified these users that their data had been compromised has been acknowledged by defendants themselves. In March 2018, Zuckerberg acknowledged that Facebook should have informed users of the data breach, claiming that he “regret[s] that we didn’t [issue a notification] at the time. And I think that we got that wrong.”³⁵³ Sandberg has also recognized that “*we have the responsibility to disclose to people when problems occur*[],” admitting that the Company failed to meet its disclosure responsibility.³⁵⁴ When asked directly whether Facebook should have timely disclosed that Facebook users’ data had been stolen, Sandberg admitted, “Yes, you are right and we should have done that. Of course you are right, and we should have done it.”³⁵⁵

345. Indeed, the plain language of Facebook’s data use policy in effect for most of the Class Period stated that Facebook would notify users when they learned that the user account had been compromised.³⁵⁶ There was no exception to this policy if Facebook believed—however im-

³⁵³ Interview by Laurie Segall, with Mark Zuckerberg, Chief Operating Officer of Facebook, CNN (Mar. 22, 2018).

³⁵⁴ *CNBC Exclusive: CNBC Transcript: Sheryl Sandberg Sits Down with CNBC’s Julia Boorstin Today*, CNBC (Mar. 22, 2018).

³⁵⁵ Eun Kyung Kim, *Sheryl Sandberg on TODAY: Other Facebook data breaches ‘possible’*, Today (Apr. 6, 2018).

³⁵⁶ Facebook Terms of Service (Jan. 30, 2016).

plausibly—that the data had later been deleted years after it was compromised. Facebook itself admits that it determined in December 2015 that a massive amount of user data had been shared improperly with Cambridge Analytica (affecting nearly 87 million users) and this sharing violated Facebook’s terms of use. At this point Facebook knew that the user’s accounts were “compromised” and they should have been notified immediately under the terms of Facebook’s own data use policy.

346. ***Facebook Did Not “Require” Deletion of Data.*** Facebook did not actually “require” that GSR and Cambridge Analytica delete the user data. Instead, Facebook pretended to rely on oral promises and unverified and utterly implausible certifications (from known bad actors) that data had been deleted. Facebook did so even though defendants knew that GSR and Cambridge Analytica had repeatedly lied to Facebook regarding the scope and type of user data Cambridge Analytica had obtained.

347. Zuckerberg has conceded that Facebook’s failure to follow up on and investigate the extent of the Cambridge Analytica data breach and assure that compromised data was deleted was the “biggest mistake[]”³⁵⁷ Facebook ever made. As he ultimately admitted, Facebook “should have been doing more all along” to protect their users’ privacy.

348. Sandberg has also admitted that it was a “mistake that [Facebook] did not verify” whether Cambridge Analytica had deleted the user data³⁵⁸ and acknowledged

³⁵⁷ Nicholas Thompson, *Mark Zuckerberg Talks to Wired About Facebook’s Privacy Problem*, *Wired* (Mar. 21, 2018).

³⁵⁸ *CNBC Exclusive: CNBC Transcript: Sheryl Sandberg Sits Down with CNBC’s Julia Boorstin Today*, *CNBC* (Mar. 22, 2018).

that the Company should have “checked”³⁵⁹ and “follow[ed]-up”³⁶⁰ to ensure Facebook user’s personal data was, in fact, protected. She stated that Facebook was “not focused enough on the possible misuses of data” and “protecting people’s data” at the time.³⁶¹ Sandberg has also admitted that Facebook “could have done . . . two and a half years ago” what it is doing today.³⁶² Facebook’s Chief Privacy Officer, Erin Egan has similarly admitted that “we should have done more to investigate claims about Cambridge Analytica and take action in 2015.”³⁶³

349. During his Senate testimony, Zuckerberg admitted that, nearly three years after the breach had been detected, Facebook *still* had not verified that the affected data had been deleted. Zuckerberg’s testimony leaves no doubt that Facebook had failed to conduct an investigation or audit or make any other effort to require deletion of the data compromised by Cambridge Analytica in a manner consistent with the Company’s public assurances of what would be done in response to the abuses of user data.³⁶⁴

³⁵⁹ Eun Kyung Kim, *Sheryl Sandberg on TODAY: Other Facebook data breaches ‘possible’*, Today (Apr. 6, 2018).

³⁶⁰ Steve Inskeep, *Full Transcript: Facebook COO Sheryl Sandberg On Protecting User Data*, NPR (Apr. 5, 2018).

³⁶¹ Judy Woodruff, *Sheryl Sandberg: Facebook ‘made big mistakes’ on protecting user data*, PBS (Apr. 5, 2018).

³⁶² Mike Allen, *Exclusive interview with Facebook’s Sheryl Sandberg*, Axios (Oct. 12, 2017).

³⁶³ Sheera Frenkel & Adam Satariano, *Facebook Fined in U.K. Over Cambridge Analytica Leak*, N.Y. Times (July 10, 2018).

³⁶⁴ *Transcript of Mark Zuckerberg’s Senate hearing*, Wash. Post (Apr. 10, 2018) (“we need to . . . go do a full audit of all of Cambridge Analytica’s systems to understand what they’re doing, whether they still have any data, to make sure that they remove all the data. If they

350. Given the size and nature of the breach, and the public representations about the seriousness with which such violations were taken and the swift repercussions that would follow, it was reckless for defendants to fail to undertake audits and other measures at the time of a data breach. The same is true for their reliance on unverified and self-serving certifications of the type described by Wylie to assume that the risks had been eliminated. It was especially reckless for Facebook to do so given its position at the forefront of technological innovation and monetization of personal information.

351. Defendants were well aware of the risks of relying on Cambridge Analytica's bald assertions that data had been deleted. Zuckerberg, Sandberg and numerous other high-ranking executives of Facebook knew all too well how easy it was to obtain private data, and how difficult it was to retrieve it once it had been leaked into the public domain.

352. Wylie's 2018 testimony to the U.K. Parliament lays bare how easy it was for the user data to be accessed indefinitely. In his testimony, Wylie explained that the user data possessed by Cambridge Analytica was "completely fungible in the sense that you can copy it a million times, it can go anywhere and . . . [i]t is often impossible to ascertain where did the data go or where is it or how much of it [there] is."³⁶⁵

don't, we're going to take legal action against them to do so."); Committee Hearing Transcript at 77 ("For Cambridge Analytica, first of all, we need to finish resolving this by doing a full audit of their systems to make sure that they delete all the data that they have and so we can fully understand what happened.").

³⁶⁵ Wylie U.K. Test. at Q1337-Q1338 (intervening comment omitted).

353. In his written testimony to the United States Senate, Wylie explained that Cambridge Analytica “often stored or transmitted data in insecure formats, including files of hundreds of thousands of Americans’ data being passed around via unencrypted emails. [Cambridge Analytica] also allowed access to its American datasets to external contractors, including senior staff from the company Palantir.”³⁶⁶ Wylie’s testimony also noted how Cambridge Analytica’s parent, SCL, “has a documented history of poor handling of sensitive data” and had been criticized in the U.K. “for its inability to properly handle sensitive Ministry of Defense information.”³⁶⁷

354. Facebook’s purported reliance on oral assurances and unverified (and long delayed) “certifications” from GSR and Cambridge Analytica is all the more implausible given the facts detailed above showing how Facebook knew that Cambridge Analytica was “sketchy (to say the least)” and that Cambridge Analytica and GSR had repeatedly lied to Facebook about the scope and type of data that had been taken, as well as repeatedly lying that it had been deleted. *See* §IV.L.2.

355. When asked why he thought Facebook never “made any efforts to retrieve or delete data,” Wylie testified that he thought Facebook did not push the issue because “if you want to investigate a large data breach, that is going to get out and that might cause problems,” and that his “*impression [was] they have sort of wanted to push it under the rug.*”³⁶⁸

³⁶⁶ Wylie Stmt. at ¶128. *See* Wylie Test. at Q1324; *see also* at Q1341 (Wylie: “Staff at Palantir had access to the data; all kinds of people had access to the data.”).

³⁶⁷ *Id.* at 29.

³⁶⁸ Wylie U.K. Test at Q1339

4. Defendants Made Materially False and Misleading Statements Regarding Their Compliance with the FTC Consent Decree

356. The 2012 FTC Consent Decree was in effect throughout the Class Period. As Zuckerberg explained in testimony to the Senate Commerce Committee on June 8, 2012, the FTC Consent Decree obligated Facebook “not to misrepresent the extent to which it maintains the privacy or security” of user data.

357. At various times during the Class Period, defendants made public assurances that they were complying with the FTC Consent Decree. In particular, after the March 2018 disclosures regarding Cambridge Analytica, defendants engaged in an aggressive public relations campaign to reassure the market that Facebook had not violated the FTC Consent Decree. These public statements included:

- On March 18, 2018, in a *Washington Post* article, Facebook stated: “We reject any suggestion of violation of the consent decree. **We respected the privacy settings** that people had in place.”³⁶⁹
- On April 4, 2018, Zuckerberg stated: “You asked about the FTC consent order. We’ve worked hard to make sure that we comply with it.”³⁷⁰

³⁶⁹ Craig Timberg & Tony Romm, *Facebook May Have Violated FTC Privacy Deal, Say Former Federal Officials, Triggering Risk Of Massive Fines*, Wash. Post (Mar. 18, 2018)

³⁷⁰ Q&A *With Mark Zuckerberg on Protecting People’s Information*, Facebook Newsroom (Apr. 4, 2018).

- On April 5, 2018, in an interview with NPR, Sandberg stated: “The FTC consent decree was important. ***And we’ve taken every step we know how to make sure we’re in accordance with it.***”³⁷¹
- On April 10, 2018, in response to questions about the FVTC Consent Decree from the Joint Senate Commerce and Judiciary Committees, Zuckerberg stated that they had changed Facebook in 2014 “so that that way it just massively restricts the amount of—of data access that a developer could get.”³⁷²

358. On June 8, 2018, in response to written questions submitted by the Senate Commerce Committee whether the FTC Consent Decree was implicated by Facebook’s recent disclosures around Cambridge Analytica, Zuckerberg stated that it was not because “Facebook accurately represented the operation of its developer Platform and the circumstances under which people could share data (including friends data) with developers [and] ***honored the restrictions of all privacy settings that covered developer access to data.***”

359. As described above, these statements were materially false and misleading. Far from respecting the restrictions on privacy settings, Facebook was secretly sharing massive amounts of user data with third parties and actively overriding users’ privacy settings as described above. Facebook was secretly overriding users’ privacy settings in order to share information about users’ friends with a wide array of “whitelisted” third-party app developers and major corporations. Thus, defendants’

³⁷¹ Steve Inskeep, *Full Transcript: Facebook COO Sheryl Sandberg on Protecting User Data*, National Public Radio (Apr. 5, 2018).

³⁷² *Transcript of Mark Zuckerberg’s Senate hearing*, Wash. Post (Apr. 10, 2018).

statements regarding user control, including in the context of the FTC Consent Decree were materially false and misleading.

M. Facebook’s Failure to Respond to the Cambridge Analytica Breach in a Manner Consistent with Its Prior Public Statements Is Revealed, Causing Massive Economic Losses to the Class

360. On March 12, 2018 *The New York Times* and *The Guardian* contacted Facebook for comment on articles they were planning to jointly publish regarding Cambridge Analytica’s use of Facebook user data. These articles were going to address the fact that the user data had been deleted. After initially threatening to sue the publications to delay or prevent publication,³⁷³ Facebook sought to pre-empt their articles by issuing a press release of its own.

361. Thus, on Friday, March 16, 2018, Facebook announced in an article published on the Company’s investor relations website that it was suspending Cambridge Analytica, its parent company, and whistleblower Wylie for sharing Facebook’s users’ data without the users’ consent. In the article, Facebook stated: “In 2015, we learned that [Kogan] lied to us and violated our Platform Policies by passing data . . . to SCL/Cambridge Analytica [and] Christopher Wylie of Eunoia Technologies Inc.” Facebook explained that “[a]pproximately 270,000 people downloaded the app” and “[i]n so doing, they gave their

³⁷³ See, e.g., Carole Cadwalladr (@carolecadwalla) TWITTER (Mar. 17, 2018, 6:07 AM) (“Yesterday @facebook threatened to sue us.”) (March 17, 2018).

consent for Kogan to access [their data].”³⁷⁴ The article asserted that “[w]hen [Facebook] learned of the violation in 2015” it had “demanded certification from Kogan and all parties he had given data to that the information had been destroyed.” Alluding to the prior media contacts, the article asserted that “Several days ago, we received reports that, contrary to the certifications we were given, not all data was deleted.” The Company said it was “moving aggressively to determine the accuracy of the claims” and asserted it was “committed to vigorously enforcing our policies to protect people’s information” and “will take whatever steps are required to see that this happens,” including taking legal action “to hold [violators] responsible and accountable for” their actions. Referring to Zuckerberg’s April 2014 announcement that access to user friend data would be shut-off, Facebook further stated: “In 2014 . . . we made an update to ensure that each person decides what information they want to share about themselves, including their friend list.”³⁷⁵

362. The March 16, 2018 article did not disclose that—despite knowing that Cambridge Analytica had “lied”—Facebook had waited many months after first learning about the improper data access to request certifications from Cambridge Analytica, Kogan and Wylie. Nor did the article disclose that other than collecting the worthless certifications, Facebook had made no effort to determine how much user data had been compromised, what that data contained, what users were affected, who else had access to their data, or how that data was being used. Nor did Facebook disclose that it had failed to notify the victims of the data breach and the user data accessed by

³⁷⁴ Paul Grewal, *Suspending Cambridge Analytica and SCL Group From Facebook*, Facebook Newsroom (Mar. 16, 2018).

³⁷⁵ *Id.*

Kogan had been transmitted to other entities and persons who had not certified that the data had been destroyed.

363. To the contrary, the following day, Facebook published an addendum to the article asserting that: “The claim that this is a data breach is completely false.” Facebook stated that the affected users had “chose to sign up to [Kogan’s] app,” “everyone involved gave their consent,” and “[p]eople knowingly provided their information” to Kogan.³⁷⁶ In reality, only around 270,000 users had provided consent—but over 87 million users had their data harvested and misused. The addendum, published at 9:50 a.m. PDT, was plainly intended as a response to articles by the *The New York Times* and *The Guardian* about the data breach, which had been published earlier the same day.

364. On March 17, 2018, *The New York Times* reported that the data breach was “one of the largest data leaks in the social network’s history. The breach allowed the company to exploit the private social media activity of a huge swath of the American electorate, developing techniques that underpinned its work on President Trump’s campaign in 2016.” As described by *The Times*:

Interviews with a half-dozen former employees and contractors, and a review of the firm’s emails and documents, have revealed that Cambridge not only relied on the private Facebook data but still possesses most or all of the trove.

* * *

The data Cambridge collected from profiles, a portion of which was viewed by The Times, included details on users’ identities, friend networks and “likes.” Only a

³⁷⁶ *Id.*

tiny fraction of the users had agreed to release their information to a third party.

* * *

Mr. Grewal, the Facebook deputy general counsel, said in a statement that both Dr. Kogan and “SCL Group³⁷⁷ and Cambridge Analytica certified to us that they destroyed the data in question.”

But copies of the data still remain beyond Facebook’s control. The Times viewed a set of raw data from the profiles Cambridge Analytica obtained.

While Mr. Nix has told lawmakers that the company does not have Facebook data, a former employee said that he had recently seen hundreds of gigabytes on Cambridge servers, and that the files were not encrypted.

365. As noted by *The Times*: “[T]he full scale of the data leak involving Americans has not been previously disclosed—and Facebook, until now, has not acknowledged it.” The newspaper went on to report that Facebook at first “downplayed” the issue, it subsequently “posted a statement expressing alarm and promising to take action.”

366. Reaction to the disclosures was swift and severe. On March 18, 2018, numerous elected officials in the United States and Europe called for investigations into

³⁷⁷ “SCL Group” never gave Facebook any certification; and the only certification that Facebook ever received from “Cambridge Analytica” was from January 2016, which Facebook discovered was fraudulent, on June 11, 2016.

Facebook, demanding that Zuckerberg testify to Congress and Parliament to explain how the breach had occurred and why affected users were not informed.³⁷⁸

367. On March 19, 2018, CNN reported that:³⁷⁹

The Cambridge Analytica scandal has done immense damage to the brand, sources across the company believe. It will now take a Herculean effort to restore public trust in Facebook’s commitment to privacy and data protection, they said.

No one has provided an adequate explanation for why Facebook did not disclose Kogan’s violation to the more than 50 million users who were affected when the company first learned about it in 2015.

368. Others agreed. On March 17, 2018 a prominent tech reporter wrote: “[T]he story here isn’t how this data was used. ***The problem here is how Facebook, the biggest social network, chose to stay silent and not inform the affected users.*** [T]he problem is Facebook’s silence on the matter until it was pushed by the whistleblower who made the details public. In its press release, Facebook blamed everything on how it was lied to by a researcher and takes no charge of its policies that allowed such behavior or says anything about why the affected users weren’t informed.”³⁸⁰

³⁷⁸ David Z. Morris, *U.S. and U.K. Lawmakers Demand Investigations of Facebook’s Data Handling*, Fortune (Mar. 18, 2018).

³⁷⁹ Dylan Byers, *Facebook is facing an existential crisis*, CNN Business (Mar. 19, 2018).

³⁸⁰ Rafia Shaikh, *50 Million Facebook Profiles Harvested Without User Consent—Data Monster Chose NOT to Alert Victims & Is Trying to Threaten Reporters*, Wccfttech (Mar. 17, 2018).

369. Similarly, on March 20, 2018, another tech reporter wrote: “This time around, Facebook might not clamber out of the hot water so easily. . . . The revelation that Facebook data on as many as 50 million users appears to have made its way into a political data operation with no consent from users is Facebook’s burden to bear alone.”³⁸¹

370. Investors and stock analysts recognized that the disclosures and the firestorm of criticism they engendered had fundamentally altered the value proposition for the Company. For example, in explaining the removal of its Buy recommendation on the Company on March 20, 2018, William O’Neill & Co. wrote:³⁸²

Facebook was aware of the privacy breach two years ago. This lack of disclosure could be viewed as a violation of privacy laws in the U.K. and many U.S. states, raising further questions

Furthermore, the increased scrutiny adds to the criticism of Russian social media influence in the 2016 election and will likely bring further backing for social media regulation, which could add uncertainty to share performance.

A *Seeking Alpha* article similarly wrote on March 19, 2018:³⁸³

³⁸¹ Tony Hatmaker, *Zuck and Sandberg go M.I.A. as Congress summons Facebook leadership by name*, TechCrunch (Mar. 20, 2018).

³⁸² Derek Higa, *Facebook, Inc CI A (FB)*, William O’Neill & Co. (Mar. 20, 2018).

³⁸³ Erich Reimner, *The Cambridge Analytica Mishap Is Serious For Facebook*, Seeking Alpha (Mar. 19, 2018)

The importance of this incident cannot be overstated for Facebook on both the user privacy front but also more importantly on Facebook's business model front. If Cambridge Analytica was able to acquire information on tens of millions of Facebook users so quickly and easily, and then keep the information for years without Facebook suspecting otherwise, then that shows a serious flaw in Facebook's ability to keep exclusive control over its information.

Even analysts who remained bullish on the Company and believed Facebook would weather the storm recognized the negative impact of the disclosures. As Piper Jaffray noted on March 21, 2018: "there's a lot of negative sentiment baked into Facebook after the revelation of the data extraction by Cambridge Analytica and Facebook's botched PR responses." The report went on to warn: "This situation could get worse if further data extractions are disclosed or if the FTC pursues a fine with Facebook."

371. Over the next several days, additional details emerged regarding the scope of the data breach and defendants' knowledge of the severity of the breach at the time it occurred, their failure to act to constrain the harm to users privacy interests or to respond to the breach in the manner described in their contemporaneous public statements, and their continuing efforts thereafter to downplay or conceal the extent of the problems and the magnitude of the risks the Cambridge Analytica data misuse continued to present to the Company's business and reputation.

372. Amid these disclosures, several social media campaigns began to urge users to disconnect from Facebook and delete the information they had posted there. On March 20, 2018, Brian Acton, co-founder of WhatsApp, a \$19 billion Facebook acquisition, tweeted: "It is time.

#deletefacebook.”³⁸⁴ A *Business Insider* article similarly reported: “The hashtag #deletefacebook is trending on Twitter. **People are furious, and they have good reason to be.** As a result, **people** are deleting their Facebook accounts en masse.”³⁸⁵

373. The foregoing disclosures caused the price of Facebook stock to decline precipitously. Facebook shares fell nearly 7% on Monday, March 19, 2018—the first trading day after the news broke—and fell an additional 2.5% the next trading day amid additional disclosures of the nature and extent of the risks that had been concealed from investors. As additional details of Facebook’s concealment were disclosed, and the negative news continued to mount, Facebook’s shares continued to decline. Within a week, Facebook’s stock was trading around \$150/share, a stunning drop of nearly 18% in value from its price (~\$185) just before news of the Cambridge Analytica scandal broke, reflecting an extraordinary loss of more than \$100 billion in market capitalization in just one week.

1. Facebook’s Privacy Misconduct Sparked Numerous Government Investigations

374. Given the volume of leaked data and its detailed, personal nature, the number of people affected, and the politically contentious nature of the leaks, multiple government agencies launched investigations into Facebook’s actions.

375. On March 26, 2018, the FTC confirmed that it had launched an investigation into Facebook’s compliance with the 2012 Consent Decree, stating: “the FTC takes

³⁸⁴ Brian Acton @brianacton, TWITTER (Mar. 20, 2018).

³⁸⁵ Ben Gilbert, *#DeleteFacebook is trending: Here’s how to delete your Facebook account*, *Business Insider* (Mar. 20, 2018).

very seriously recent press reports raising substantial concerns about the privacy practices of Facebook.”³⁸⁶

376. On July 12, 2018, *The Wall Street Journal* reported that the SEC was investigating “whether Facebook Inc. adequately warned investors that developers and other third parties may have obtained users’ data without their permission or in violation of Facebook policies.”³⁸⁷ The Justice Department and the FBI also reportedly joined the government investigations into Facebook’s privacy lapses in the wake of the Cambridge Analytica data breach.

377. In addition, and as discussed in greater detail below, numerous governments of other countries began investigating defendants’ misuse of Facebook user information.

2. The U.K. Information Commissioner’s Office

378. On July 11, 2018, a United Kingdom government agency called the Information Commissioner’s Office or “ICO” issued a report following its investigation into the way that Facebook, Cambridge Analytica and others used individuals’ personal information in political processes.³⁸⁸ The report states that in 2017,³⁸⁹ the ICO launched a formal investigation into the misuse of personal information leading up to the “Brexit” vote in summer 2016. Over 40

³⁸⁶ Press Release, *Statement by the Acting Director of FTC’s Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices*, Federal Trade Commission (Mar. 26, 2018).

³⁸⁷ David Michaels and Georgia Wells, *SEC Probes Why Facebook Didn’t Warn Sooner on Privacy Lapse*, Wall St. J. (July 12, 2018).

³⁸⁸ ICO Report.

³⁸⁹ *Id.* at 6.

investigators worked on the investigation along with experts. One key focus of the investigation is the misuse of the same data that Cambridge Analytica applied in the U.S. presidential election.

379. According to the ICO’s report, its investigation in “the second half of 2017 was both complex and wide ranging.”³⁹⁰ The report states that the investigation “involved meetings, interviews and correspondence with over 30 organisations” that included “Facebook, Cambridge Analytica and AggregateIQ (AIQ).”³⁹¹ The ICO report attaches a Notice of Intent to take regulatory action Facebook for data breaches, and the notice states that the **ICO sent an investigation letter “to the Facebook companies on 23 August 2017.”**³⁹² The ICO made iterative requests after that time. The ICO confirms that a “key strand” of its investigation focused on the Cambridge Analytica data leak because the leaked data also included “1 million” users in the U.K..³⁹³

380. The ICO explained that it intended to impose a penalty on Facebook. The penalty arose out of the “very serious” data incident involving Facebook’s failure to take appropriate technical and organizational measures against “unauthorized or unlawful processing of personal data” in violation of its statutory obligations, as the ICO wrote.³⁹⁴ These violations stemmed from Facebook’s fail-

³⁹⁰ *Id.* at 9.

³⁹¹ *Id.*

³⁹² *Data Protection Act 1998, Supervisory Powers of the Information Commissioner, Notice of Intent*, Information Commissioner’s Office (June 19, 2018) at 7 (“ICO Notice”).

³⁹³ ICO Report at 8.

³⁹⁴ ICO Notice at 2-3.

ure to protect the privacy of its users' data that Cambridge Analytica and related companies exploited in both the U.K. "Brexit" election and the U.S. presidential election. The ICO Notice of Intent states that the Facebook's violations were serious because they affected a "very large number of individuals" and a "very substantial volume of personal data" and involved uses that were beyond reasonable expectations thereby causing the victims distress.³⁹⁵

381. The ICO's investigation also demonstrated that Facebook knew or should have known about the Cambridge Analytica data leak and misuse. The ICO wrote that "the Facebook Companies ***knew or ought reasonably to have known*** that there was a risk that the contravention would (a) occur, ***and*** (b) be of a kind likely to cause substantial distress."³⁹⁶ The ICO further wrote that Facebook "failed to take reasonable steps to prevent such contravention" in that Facebook is a large and experienced data collector and "***should have been aware of the risks***."³⁹⁷ And the ICO that Facebook "had ample opportunity over a long period of time to implement appropriate technical . . . measures" to prevent the data violations "but failed to do so."³⁹⁸ The ICO did act on its intent to penalize Facebook and, as *CNBC* reported on July 11, 2018, the ICO was "hitting Facebook with the maximum possible fine it can impose."³⁹⁹ On October 24, 2018, the ICO imposed its maximum penalty of £500,000.

³⁹⁵ *Id.* at 17.

³⁹⁶ *Id.* at 18.

³⁹⁷ *Id.*

³⁹⁸ *Id.*

³⁹⁹ Ryan Brown, *Facebook faces UK fine of around \$660,000 after data scandal found to be illegal*, *CNBC* (July 11, 2018).

3. Defendants Admit Fault for the Cambridge Analytica Privacy Failure

382. On March 21, 2018, defendants broke their silence as Zuckerberg and Sandberg made a number of statements in which they conceded that they had known that the data of millions of its users had been harvested and used without consent but had done nothing. In a post to his personal Facebook page, Zuckerberg took “responsibil[ity] for what happens on our platform” and admitted that the Company had “made mistakes,” and that the Cambridge Analytica issue reflected “a breach of trust between Facebook and the people who share their data with us and expect us to protect it. We need to fix that.”⁴⁰⁰ Sandberg re-posted Zuckerberg’s post on her own Facebook page, adding: “We know that this was a major violation of people’s trust, and I deeply regret that we didn’t do enough to deal with it. We have a responsibility to protect your data.”⁴⁰¹

383. Defendants’ statements were not mere expressions of regret, they were outright admissions of “responsibility” for “breach[es]” and “violations” of user “trust” and acknowledgments that defendants “didn’t do enough” to respect user privacy or provide users with the promised control over their data.

384. In an interview with *Wired* the same day, Zuckerberg similarly admitted that the *Guardian* and *Times* reports were credible and admitted that Cambridge Analytica was not the only third party with which Kogan had shared “a lot” of users’ data, that Facebook had not audited Cambridge Analytica to verify that user data had been deleted, that the Company might have to do a “full

⁴⁰⁰ Mark Zuckerberg, Facebook (Mar. 21, 2018).

⁴⁰¹ Sheryl Sandberg, Facebook (Mar. 21, 2018).

forensic audit” of every one of its developers operating before it could determine the extent of the data breach.⁴⁰²

385. The transcript of the interview published by *Wired* stated in relevant part:⁴⁰³

Thompson: You learned about the Cambridge Analytica breach in late 2015, and you got them to sign a legal document saying the Facebook data they had misappropriated had been deleted. But in the two years since, there were all kinds of stories in the press that could have made one doubt and mistrust them. Why didn’t you dig deeper to see if they had misused Facebook data?

Zuckerberg: So in 2015, when we heard from journalists at The Guardian that Aleksandr Kogan seemed to have shared data with Cambridge Analytica and a few other parties, the immediate actions that we took were to ban Kogan’s app and to demand a legal certification from Kogan and all the other folks who he shared it with. We got those certifications, and Cambridge Analytica had actually told us that they actually hadn’t received raw Facebook data at all. It was some kind of derivative data, but they had deleted it and weren’t [making] any use of it.

In retrospect, though, I think that what you’re pointing out here is one of the biggest mistakes that we made. And that’s why the first action that we now need to go take is to not just rely on certifications that we’ve gotten from developers, but [we] actually need

⁴⁰² Nicholas Thompson, *Mark Zuckerberg Talks to Wired About Facebook’s Privacy Problem*, *Wired* (Mar. 21, 2018).

⁴⁰³ Nicholas Thompson, *Mark Zuckerberg Talks to Wired About Facebook’s Privacy Problem*, *Wired* (Mar. 21, 2018).

to go and do a full investigation of every single app that was operating before we had the more restrictive platform policies—that had access to a lot of data—and for any app that has any suspicious activity, we’re going to go in and do a full forensic audit.

* * *

Thompson: How confident are you that Facebook data didn’t get into the hands of Russian operatives—into the Internet Research Agency, or even into other groups that we may not have found yet?

Zuckerberg: I can’t really say that. I hope that we will know that more certainly after we do an audit. You know, for what it’s worth on this, the report in 2015 was that Kogan had shared data with Cambridge Analytica and others.

386. In an interview with *Recode* on March 21, 2018, Zuckerberg revealed that Facebook needed to investigate tens of thousands, of apps that may have improperly shared data, while conceding that the Company might never be able to determine what or how much user data had been sold to or shared with third parties.⁴⁰⁴ Ime Archibong, Facebook’s Vice President of Product Partnerships, warned that this number may increase as the investigation continues to “find all the apps that may have misused people’s Facebook data.”⁴⁰⁵

387. In the *Recode* interview, Zuckerberg repeated the claim that Cambridge Analytica had said it “never had

⁴⁰⁴ Kara Swisher & Kurt Wagner, *Mark Zuckerberg says he’s ‘open’ to testifying to Congress, fixes will cost ‘many millions’ and he ‘feels really bad’*, *Recode* (Mar. 21, 2018).

⁴⁰⁵ Ime Archibong, *An Update on Our App Investigation and Audit*, Facebook Newsroom (May 14, 2018).

the data and deleted what derivative data” it had,⁴⁰⁶ while admitting that Facebook had done nothing to verify those assertions. While attempting to justify the Company’s actions as reasonable at the time Zuckerberg admitted “in retrospect it was clearly a mistake. I’m explaining to you the situation at the time, and the actions that we took, but ***I’m not trying to say it was the right thing to do.*** I think given what we know now, we clearly should have followed up.”⁴⁰⁷ *Recode* itself was unimpressed by Zuckerberg’s attempts to explain away Facebook’s response to the data breach, noting in a companion article about the interview:⁴⁰⁸

But Zuckerberg did not give any details about why the company did not do those checks, or about why broader monitoring of third-party developers—who in some cases were given vast troves of user information—was so shoddy.

He said Facebook is now trying to go back and check who has user data, although it’s essentially an effort to put the genie back into the bottle. When asked if he could recover some of the data now, Zuckerberg admitted, “not always.”

388. On March 25, 2018, Facebook also took out full-page advertisements in several U.S. and U.K. newspapers, including *The New York Times*, *The Washington Post*, *The Wall Street Journal*, *The Observer*, *The Sunday*

⁴⁰⁶ Kara Swisher & Kurt Wagner, *Here’s the transcript of Recode’s interview with Facebook CEO Mark Zuckerberg about the Cambridge Analytica controversy and more*, *Recode* (Mar. 22, 2018).

⁴⁰⁷ *Id.*

⁴⁰⁸ Kara Swisher & Kurt Wagner, *Mark Zuckerberg says he’s ‘open’ to testifying to Congress, fixes will cost ‘many millions’ and he ‘feels really bad’*, *Recode* (Mar. 21, 2018).

Times, *Sunday Mirror*, *Sunday Express* and *Sunday Telegraph*. These ads were signed by Zuckerberg, who stated with direct reference to the Cambridge Analytica scandal: “This was a breach of trust, and I’m sorry we didn’t do more at the time. We’re now taking steps to ensure this doesn’t happen again.” Zuckerberg further stated: “I promise to do better for you.”⁴⁰⁹

389. On April 4, 2018, in a Q&A session with members of the press, Zuckerberg admitted with respect to the Cambridge Analytica scandal, “it’s clear now that we didn’t do enough . . . [w]e didn’t take a broad enough view of what our responsibility is, and that was a huge mistake. It was my mistake.”⁴¹⁰ Zuckerberg elaborated by acknowledging that “it’s not enough to have rules requiring they [*i.e.*, app developers] protect information, it’s not enough to believe them when they tell us they’re protecting information—we actually have to ensure that everyone in our ecosystem protects people’s information.”

390. In an April 5, 2018 interview with NPR, Sandberg acknowledged that Facebook did not previously have sufficient privacy controls in place, and indicated awareness that Facebook was not in compliance with the FTC Consent Decree. Specifically, Sandberg stated: “[W]e’re in constant conversation with the FTC, and that consent decree was important, and we’ve taken every step we know how to make sure we’re in accordance with it. But the bigger answer is, ***should we have taken these steps years ago anyway? And the answer to that is yes. Like a very clear, a very firm, yes.***”

⁴⁰⁹ Sheena McKenzie, *Facebook’s Mark Zuckerberg says sorry in full-page newspaper ads*, CNN (Mar. 25, 2018).

⁴¹⁰ *Hard Questions: Q&A With Mark Zuckerberg on Protecting People’s Information*, Facebook Newsroom (Apr. 4, 2018).

391. Defendants’ orchestrated apology tour had its intended effect. Indeed, analysts responded by telling investors to expect only a relatively modest and short term impact from the revelations about Facebook’s failure to protect privacy or provide users control over their data.⁴¹¹

N. Defendants Recklessly and Falsely Assured Investors that the Cambridge Analytica Scandal Had Not Affected Facebook’s User Engagement or Financial Results, Reinflating Facebook’s Stock Price

392. As the first quarter drew to a close, investors and market analysts were justifiably concerned over the impact that Facebook’s past misrepresentations concerning the Cambridge Analytica data breach and the use of its platform to further election interference and other political activities by Russia would have on the Company’s users and advertisers. The impending launch of the General Data Protection Regulation (“GDPR”) in the E.U. added to these concerns.

⁴¹¹ See, e.g., Mark S.F. Mahaney, *Defending Facebook*, RBC Capital Markets (Mar. 21, 2018) (maintaining outperform rating and \$250 price target: “we view [Zuckerberg’s] statement . . . as delayed—but appropriate—responses and steps by Facebook”); Brian Nowak, C.F.A., *Our Thoughts on FB’s Public Statement*, Morgan Stanley (Mar. 21, 2018) (maintaining overweight and \$230 price target: “We look to these and further forthcoming data safeguards (expected in coming days) to reassure users that FB is acting more proactively and decisively to protect their data”); Ronald V. Josey, *Our Thoughts on Facebook’s Privacy and Data Issues*, JMP (Mar. 21, 2018) (“we expect this issue to be an overhang over the short-to-medium term, although we also do not believe these issues have impacted usage or advertiser demand”); Ken Sena, *FB: It’s Not You, It’s Us*, Wells Fargo Securities (Mar. 21, 2018) (“Constructive First Steps, Continue to View Business Impact as Likely Minimal”).

393. Nevertheless, analysts were cautiously optimistic that Facebook's promises of quick and decisive action to combat the threats would help it rebound quickly from the negative disclosures. As a Morningstar analyst wrote on March 26, 2018:⁴¹²

Facebook's latest data breach issue, which surfaced 11 days ago and involved Cambridge Analytica, was followed on March 25 by the Federal Trade Commission's announcement of an investigation into the company's abilities and willingness to protect user information. While this recent development may have brought forth further doubts regarding Facebook and its user growth and engagement, along with more demand for a GDPR type of regulation in the U.S., we remain confident that the firm is more likely to endure the short-term impact of the data breach issue and at this point do not expect a significant long-term negative effect on Facebook's platform and operations.

Other analysts made similar comments.⁴¹³

⁴¹² Ali Magharabi, *Many Downside Scenarios Are Priced In, Facebook Shares are now attractive*, Morningstar (Mar. 26, 2018).

⁴¹³ See, e.g., Lloyd Walmsley, *Attractive long-term but 1Q brings risks*, Deutsche Bank (Apr. 18, 2018) ("1Q likely to be heavily focused on fallout from CA and upcoming GDPR"); Youseff Squali, *1Q18 Likely Strong Despite CA Mishap; Investments to Pressure Margins S/M Term*, SunTrust Robinson Humphrey (Apr. 20, 2018) ("we believe the very recent negative publicity may have removed 'upside' ad revenue opportunities and likely added uncertainty around user engagement and growth"); Mark S.F. Mahaney, *Facebook, Inc. Q1 Preview & Cheat Sheet*, RBC Capital Markets (Apr. 23, 2018) ("The almost unanimous opinion from the executives we talked with at ad technology/consulting companies . . . was that the recent controversies would have no material impact on the relevance and attractiveness and importance of Facebook as a marketing platform. Facebook

1. Defendants Tout Facebook's 1Q18 Results as Demonstrating that Users Were Unconcerned with the Cambridge Analytica Scandal

394. When Facebook reported its first quarter results on April 25, 2018, investors were buoyed by revenues, earnings and DAU/MAU metrics that were all in line with estimates. Sandberg told investors “It was a great quarter for our business. Q1 ad revenue grew 50% year-over-year. Mobile ad revenue was \$10.7 billion, up 60% from last year and contributed approximately 91% of total ad revenue. Revenue growth was broad-based across regions, marketer segments and verticals.”

395. Sandberg further assured the market that there would not be a significant business impact from the March revelations regarding Cambridge Analytica, stating “we think the investigatory work we’re doing into APIs is very important and we don’t expect it have an impact on revenue.” Zuckerberg commented that “Despite the important issues that we faced . . . our community and our business continued to grow really well,” while Wehner assured investors that Facebook was “committed to transparency.”

396. As *The New York Times* reported on April 25, 2018:⁴¹⁴

Despite it all, the Facebook juggernaut marches on.

has been, is, and will remain for the foreseeable future a ‘must buy’ for most consumer-oriented marketers.”).

⁴¹⁴ Sheera Frenkel & Kevin Roose, *Facebook's Privacy Scandal Appears to Have Little Effect on Its Bottom Line*, N.Y. Times (Apr. 25, 2018).

The social network is undergoing its worst crisis in its 14-year history as it faces a torrent of criticism about its privacy practices and the way it handles user data.

But on Wednesday, Facebook showed that—as with past scandals—the controversy is so far doing little to hurt its bottom line.

The results sent Facebook’s shares up more than 7 percent in aftermarket trading on Wednesday.

397. The Company’s 1Q18 results together with management’s assurances on the 1Q18 conference call led many analysts to conclude that the disclosures concerning Cambridge Analytica had not impacted user’s engagement with the platform.⁴¹⁵

398. Bolstered by the 1Q18 results and defendants assurances of the strength of Facebook’s business in the face of the firestorm of criticism it was facing over its user data and privacy practices, the Company’s stock price began to recover. The price of Facebook’s share rose more than 9% immediately after 1Q18 results were released, and by late May the shares had recovered to the levels they were trading at before *The Guardian* and *The New York Times* articles about the Cambridge Analytica data breach broke.

⁴¹⁵ See, e.g., Jason Helfstein, *Strong 1Q Suggests Cambridge Analytica Soon to Be a Distant Memory; Maintain Outperform, \$225 PT*, Oppenheimer (Apr. 25, 2018) (“Most positive takeaway was constructive tone from mgmt”); Sam Kemp, *Strong Q1 + Cambridge Analytica & GDPR Set to Fade From Focus, Remain OW*, PiperJaffray (Apr. 25, 2018) (“Incremental news around impacts from the recent Cambridge Analytica (CA) debacle were nil and, **alongside mgmt commentary downplaying GDPR impact**, will likely accelerate the fading relevance of these topics from investor focus.”).

399. Thereafter, defendants continued to tout the 1Q18 results as a sign that the Company had weathered the storm, while assuring investors that there was no reason to be concerned that the past user privacy scandals or new privacy regulations would have a negative impact on Facebook's business.

400. In April 2018, Facebook shareholders made various proposals in response to the Cambridge Analytica scandal. For example, shareholders proposed that "Facebook's Board issue a report discussing the merits of establishing a Risk Oversight Board Committee."⁴¹⁶

401. In support of this proposal, on April 17, 2018, Facebook investors noted the fact that the Company faced "significant financial, reputational and regulatory risk" from events like "The Cambridge Analytica scandal and the misuse of data to influence elections around the world," which "cost Facebook investors \$90 billion in market value between March 16th and March 17th."⁴¹⁷ Facebook shareholders also proposed that "Facebook issue a report to shareholders . . . [*inter alia*] assessing the risks posed by content management controversies (including election interference . . .) to the company's finances operations and reputation."⁴¹⁸ In support of this proposal, on May 17, 2018, Facebook investors, including the Illinois State Treasurer explained that "Facebook's controversies

⁴¹⁶ Facebook's Proxy Statement Pursuant to Section 14(a) of the Securities Exchange Act of 1934 at 51 ("Proposal Four: Stockholder Proposal Regarding A Risk Oversight Committee") (Apr. 13, 2018).

⁴¹⁷ Letter from Jonas Kron, Snr. Vice President, Trillium Asset Management to Facebook Shareholders (Apr. 17, 2018).

⁴¹⁸ Facebook's Proxy Statement Pursuant to Section 14(a) of the Securities Exchange Act of 1934 at 55 ("Proposal Six: Stockholder Proposal Regarding A Content Governance Report") (Apr. 13, 2018).

have a direct impact on the Company's market value" including because "[f]ollowing the Cambridge Analytica disclosures, Facebook shares lost approximately \$100 billion in market value."⁴¹⁹ Defendants opposed both stockholder proposals, assuring investors that Facebook's risk oversight was fine and that there was no need for the requested report.

402. During Facebook's annual meeting on May 31, 2018, Natasha Lamb, managing partner of activist investor Arjuna Capital, said:⁴²⁰

From political subterfuge, fake news, hate speech and sexual harassment, it is clear that content that violates Facebook's own terms of service poses a risk to the Company's market value and brand. Last year, at this very meeting, we highlighted the risk posed by fake news propagated over the platform. And while our board opposed reporting, we learned [six] months later and only through congressional testimony that 126 million Americans may have viewed Russian propaganda prior to the 2016 U.S. presidential election. Four months later, we learned that 87 million Americans data was compromised by Cambridge Analytica with the intent to manipulate users for political gain. In the wake of that scandal, Facebook's market value dropped nearly \$100 billion. And while today's proposal is broader, I'm surprised to see a similar reaction from our board, a recommendation to vote against greater transparency and accountability to investors.

⁴¹⁹ Letter from Natasha Lamb, Managing Partner, Arjuna Capital and Michael W. Frerichs, Illinois State Treasurer (and others) to Facebook Shareholders (May 17, 2018).

⁴²⁰ Facebook, Inc. Annual Shareholders Meeting Tr. at 6 (May 31, 2018).

Fines and regulation by governments, lost advertising revenue and a soured brand may further impact investment returns. In fact, users may leave the social media platform if they feel its content lacked integrity.

403. Following comments like these, Zuckerberg took to the stage to tout the Company's 1Q18 results ("that shows a lot of good continued momentum" in the business) and assure investors that users were not changing their behavior in the wake of the scandals, and were still opting in to share their data with Facebook (the "vast majority of people say yes, they want that data used").⁴²¹ The shareholders proposals were defeated.

2. Zuckerberg Falsely Assures Investors that European Privacy Regulations Are Not Impacting the Business

404. Zuckerberg's assurance that the "vast majority" of users were opting into data sharing was particularly important to investors, as it came just after the launch of the General Data Protection Regulation ("GDPR") in the E.U. on May 25, 2018. The GDPR is a broad set of regulations governing the collection and use of personal data that is designed to protect the privacy of EU citizens. Significantly, and in addition to a host of disclosure and control requirements, the GDPR requires corporations to make their data collection and sharing policies opt-in, rather than opt-out, and limits the breadth and type of data collection and sharing by companies like Facebook.

405. The GDPR imposes several requirements on all entities (including Facebook) that process and target personal data from individuals located in the European Union. At bottom, the GDPR is designed to protect privacy

⁴²¹ *Id.* at 8, 16.

by giving people control over their personal data. For example, the GDPR requires, among other things, that the processor (*e.g.*, Facebook) disclose any data collection, disclose whether the data is being shared with any third parties, and to delete that data under certain circumstances. The GDPR also requires that any entities notify individuals in the European Union whose data may have been breached, compromised, or deleted. The GDPR also imposes significant reporting and internal control requirements, mandating companies like Facebook to appoint a data collection officer and to report its compliance to the GDPR's provisions to independent public authorities appointed by European Union member states. The GDPR further requires the processor to obtain a user's affirmative consent before using and distributing that user's personal data, as well as limiting the breadth of consent given.

406. The GDPR was adopted by the European Council and Parliament on April 14, 2016. All companies operating within the European Union had to comply with the GDPR by May 25, 2018 or face stiff penalties.

407. Defendants used the years between its passage and implementation to reassure investors that the GDPR would have little to no impact on Facebook's business. During quarterly conference calls and in investor presentations starting in mid-2017 and continuing into 2018, defendants used updates to their Terms of Service and Data Policy to claim that Facebook had already largely given its users the privacy controls necessary to comply with GDPR. In or around August 2017, Facebook began im-

plementing changes to its products, including the Platform, because of the GDPR.⁴²² According to a Facebook representative, Facebook had “assembled the largest cross-functional team in the history of the Facebook family of companies,” to implement these changes, including teams to conduct legal, product and engineering assessments on the GDPR’s impact.⁴²³ Facebook also created a “What is the [GDPR]?”⁴²⁴ page on its website touting the steps Facebook had already taken to give users’ control of their data in compliance with the GDPR, and which claimed that even under GDPR “Businesses that advertise with the Facebook Companies can continue to use Facebook platforms and solutions in the same way they do today.”⁴²⁵

408. During this time, defendants continually reassured investors that the GDPR would not have a material impact on Facebook’s business. For example, in an interview published by Axios on October 12, 2017, Sandberg claimed that Facebook was already adhering to GDPR requirements, stating “Europe has passed a single privacy law **and we are adhering to that** . . . privacy is something we take really seriously.”⁴²⁶ During the Company’s 3Q17 earnings call on November 1, 2017, Sandberg emphasized the point, claiming “On GDPR, the Facebook family of

⁴²² Aliya Ram, *Tech sector struggles to prepare for new EU data protection laws*, Fin. Times (Aug. 29, 2017).

⁴²³ *Id.*

⁴²⁴ *What is the General Data Protection Regulation (GDPR)?*, Facebook Business.

⁴²⁵ *Id.*

⁴²⁶ Mike Allen, *Exclusive interview with Facebook’s Sheryl Sandberg*, Axios (Oct. 12, 2017).

apps *already applies* the core principles in the framework because we built our services around transparency and control.” As noted below, Sandberg repeated similar statements during the Company’s January 31, 2018 earnings call, stating that “the Facebook family of apps already applies the core principles in the GDPR framework, which are transparency and control.”

3. Defendants Continued to Falsely Downplay Reports of Privacy Risks Ahead of Facebook’s 2Q18 Earnings Release

409. While the market was reassured by defendants’ comments, questions surrounding Facebook’s privacy practices continued to swirl. On June 8, 2018, Facebook responded to inquiries from numerous journalists seeking a response to *The New York Times*’ and *The Wall Street Journal*’s reporting about whitelisting and other unauthorized sharing of users’ data. Facebook issued the same statement to multiple outlets in response, which read:⁴²⁷

For the most part this is a rehash of last week-end’s New York Times story—namely that we built a set of device integrated APIs used by around 60 companies to create Facebook-like experiences. In April 2018, we announced that we were winding these down. In terms of our Platform APIs, the Journal has confused two points. In 2014, all developers were given a year to switch to the new, more restricted version of the API. . . . Per our testimony to Congress ‘We required developers to get approval from Facebook before they could request any data beyond a user’s public profile, friend list, and email address.’

⁴²⁷ Jack Morse, *Another day, another Facebook privacy scandal*, Mashable (June 8, 2018).

410. Journalists were skeptical of this response. *Axios*, after reviewing a timeline of Facebook’s half disclosures, concluded that “Each new admission—even of the kinds of small bugs and problems that are common across the industry—reinforces a view in Washington that Facebook has been unwilling to come fully clean.”⁴²⁸

411. On June 27, 2018, *The Wall Street Journal* reported that Facebook could not track where the data it had improperly disseminated—not just to Cambridge Analytica, but to developers and others writ large—had ended up.⁴²⁹

412. On June 29, 2018, Facebook responded in writing to outstanding questions put on the record to Zuckerberg by the members of the U.S. House of Representatives on April 11, 2018. The responses, which spanned more than 700 pages, stated that Apple, Amazon and the other device makers described herein were not the only developers that received special or extended access to users’ friends data. Facebook also conceded that “early records may have been deleted from our system,” and that “it is possible” that Facebook had failed to identify other developers who had also received extended access to users’ friends’ data.⁴³⁰

413. On July 1, 2018, after reviewing Facebook’s responses to written questions from members of Congress,

⁴²⁸ David McCabe, *The big picture: Facebook’s year of missteps*, *Axios* (June 9, 2018).

⁴²⁹ Deepa Seetharaman, *Facebook’s Latest Problem: It Can’t Track Where Much of the Data Went*, *Wall St. J.* (June 27, 2018).

⁴³⁰ Letter from Facebook, Inc. to Chairman Greg Walden, Ranking Member Frank Pallone, U.S. House of Representatives, Energy and Commerce Committee at 96 (June 29, 2018).

The Wall Street Journal, based in part on its earlier investigations in combination with a review of Facebook’s answers and earlier discussions, concluded that Facebook’s responses contradicted Zuckerberg’s previous statements to Congress:⁴³¹

Facebook . . . disclosed it gave dozens of companies special access to user data, detailing for the first time a spate of deals that *contrasted* with the social network’s previous public statements that it restricted personal information to outsiders in 2015.

* * *

The disclosure follows a Journal article in June that reported Facebook struck customized data-sharing deals that gave select companies such as Nissan Motor Co. access to user records for their apps well after the point in 2015 when it said it walled off that information. Nissan is listed in Friday’s document.

414. On July 2, 2018, *The Washington Post* reported that multiple federal agencies, including the FBI, the SEC, the FTC and the DOJ, were investigating Facebook related to the data-sharing scandal involving Cambridge Analytica: “The questioning from federal investigators centers on what Facebook knew three years ago and why the company [did not] reveal it at the time to its users or investors, as well as any discrepancies in more recent accounts, among other issues.”⁴³² Facebook confirmed the investigation and said it was cooperating with authorities.

⁴³¹ Georgia Wells, *Facebook Reveals Apps, Others That Got Special Access to User Data*, Wall St. J. (July 1, 2018).

⁴³² Craig Timberg, Elizabeth Dwoskin, et al., *Facebook’s disclosures under scrutiny as federal agencies join probe of tech giant’s*

415. On July 11, 2018, CNN revealed that Facebook had given a “Russian internet company with links to the Kremlin”:⁴³³

[The right] to collect data on unknowing users of the social network after a policy change supposedly stopped such collection. Facebook told CNN on Tuesday that apps developed by the Russian technology conglomerate Mail.Ru Group, were being looked at as part of the company’s wider investigation into the misuse of Facebook user data in light of the Cambridge Analytica scandal.

416. Mail.Ru Group was one of the developers granted extended access to users’ friends’ data as identified in the June 29, 2018 submission Facebook made to Congress, highlighting the risk in granting such extensions.

O. Facebook’s 2Q18 Financial Results Reveal the Huge Impact the Data Privacy Scandal Had on Facebook’s User Engagement, Advertising Revenues and Earnings, Leading to a Stunning \$100 Billion Loss in Facebook’s Value

417. Heading into Facebook’s 2Q18 earnings call, the Company’s share price was hovering around \$210 and many investors and analysts, buoyed by the Company’s

role in sharing data with Cambridge Analytica, Wash. Post (July 2, 2018).

⁴³³ Donie O’Sullivan, Drew Griffin & Curt Devine, *Russian company had access to Facebook user data through apps*, CNN Business (July 11, 2018).

1Q18 earnings report and defendants' assurances regarding the continued strength of the business in the wake of the scandal, remained strongly bullish on the Company.⁴³⁴

418. Investors and analysts were therefore stunned when Facebook issued its second quarter earnings on July 25, 2018, reporting flat to declining user growth, lower than expected revenues and earnings, contracting gross margins, and reduced guidance going forward, all as a substantial result of the fallout of the disclosures concerning Facebook's privacy practices, including its misrepresentations about its efforts to prevent and address events like the Cambridge Analytica data breach or the Russian attempts to influence election results in the U.S.

419. The Company reported having 1.47 billion average daily active users in June and quarterly revenues of \$13.2 billion, both of which were below average analyst estimates as compiled by *Bloomberg*. The revenue miss was Facebook's first since 2015. In addition the company reported that, after years of growth, its active user base

⁴³⁴ See, e.g., Michael J. Olsen, *Core Strength & LT "Call Options" Override Short-Term Concerns; OW & PT to \$250*, PiperJaffray (July 20, 2018) ("Regulatory Concerns Unlikely to Change the Big Picture"); Youseff Squali, *Strong 2Q18 Expected Despite Head Winds; Maintain Buy*, SunTrust Robinson Humphrey (July 20, 2018) ("Despite all the negative headlines, we believe ad revenue should continue to drive very healthy growth"); Michael Pachter, *Expect Another Strong Quarter Despite Negative Press and Privacy Overhang*, Wedbush (July 20, 2018) ("Notwithstanding heightened scrutiny and elevated legislative and regulatory risk, we expect Facebook to weather the controversy surrounding its Cambridge Analytica data breach and the implementation of GDPR in Europe."); Rob Sanderson, *Q2 Preview: Expecting Revenue Growth Upside, Remains a Top Pick*, MKM Partners (July 20, 2018) (Buy rating with \$255 price target); Mark S.F. Mahaney, *Q2 Preview & Cheat Sheet*, RBC Capital Markets (July 22, 2018) (outperform rating with \$250 price target).

(MAU and DAU) had declined in Europe, was flat in the U.S. and Canada, and was decelerating worldwide.

420. Facebook's failure to make any attempt to determine what data had been compromised, to verify that the data had been destroyed, or to notify affected users that their data had been compromised, was directly contrary to the repeated representations defendants had made about Facebook's response to the Cambridge Analytica data breach and its commitment to and the resources it had committed to protecting user privacy. The outrage sparked by the disclosure of Facebook's privacy practices and prior misrepresentations directly and proximately led users to disconnect from or reduce their use of Facebook's platform, and to take advantage of new tools and regulations giving them more control over the use of their data, including the right to opt out of tracking or sharing settings that were critical to the effectiveness of Facebook's targeted advertising programs.

421. It also caused advertisers to reduce or eliminate their spending on the platform, sparked numerous government investigations, and led to dramatic increases in spending on regulatory compliance and safety programs needed to correct the conditions that had led to the Cambridge Analytica data breach and permitted Russian agents to take advantage of Facebook's lax security measures to attempt to influence U.S. election results. All of these factors, individually and in combination, were the cause of the disappointing 2Q18 earnings report and reduced 2H18 guidance and of the resultant decline in the price of Facebook common stock.

422. During the 2Q18 conference call on July 25, 2018, Wehner told investors to expect revenue growth rates to decelerate in the second half of the year "by high single digit percentages from prior quarters sequentially."

Wehner said that one of the driving factors in the Company's declining revenue growth was that users were sharing less data with the Company and advertisers were reducing their spending on the platform in the wake of the privacy disclosures:⁴³⁵

In terms of what is driving the deceleration, . . . it's a combination of factors. . . . And then finally, we're giving people who use the . . . services more choice around privacy. And that's coming both in terms of impacts that could be ongoing from things like GDPR as well as other product options that we're providing that could have an impact on revenue growth.

423. As Wehner explained, users exercising their right to opt out of data sharing under the new European regulations, reduced ad spending based on less reliance on Facebook's data to support targeted advertising, and new product features that would give users even more control over data sharing and content viewing in the wake of the Cambridge Analytica and Russian interference investigations all contributed to driving the lowered growth estimates:⁴³⁶

We do think that there will be some modest impact [from GDPR]. And I don't want to overplay these factors, but you've got a couple things going on. You've got the impact of the opt-outs. And while we're very pleased with the vast majority of people opting into the third-party data use, some did not. So that'll [sic] have a small impact on revenue growth. And then we're also seeing some impact from how advertisers are using their own data for targeting, so again, that'll [sic] have a modest impact on growth. And then in addition,

⁴³⁵ Q2 2018 Facebook, Inc., Earnings Call Tr. at 9-10 (July 25, 2018).

⁴³⁶ *Id.* at 13.

we're continuing to focus our product development around putting privacy first, and that's going to, we believe, have some impact on revenue growth. So it's really a combination of kind of how we're approaching privacy as well as GDPR and the like. So I think all of those factors together are one of the factors that we're talking about

424. Market reaction to the Company's 2Q18 earnings report and conference call was swift and severe, causing the price of Facebook's common stock to drop by nearly 19% on July 26, 2018, another staggering loss of \$120 billion in market capitalization that was the largest such one-day drop in U.S. history.

425. In addition, the quarterly results reflected—for the first time—the economic impact of the damage caused to the Company's reputation by the disclosure of its past misrepresentations of the risks arising from the Cambridge Analytica data breach and what Facebook had done to address it. As *The New York Times* reported on July 25, 2018:⁴³⁷

Facebook reported on Wednesday that growth in digital advertising sales and in the number of its users had decelerated in the second quarter. The company's leaders, including its chief executive, Mark Zuckerberg, added that the trajectory was not likely to improve anytime soon, especially as Facebook spends to improve the privacy and security of users.

Facebook has grappled with months of scrutiny over Russian misuse of the platform in the 2016 American presidential campaign and the harvesting of its users'

⁴³⁷ Sheera Frenkel, *Facebook Starts Paying a Price for Scandals*, N.Y. Times (July 25, 2018).

data through the political consulting firm Cambridge Analytica. The results were among the first signs that the issues had pierced the company's image and would have a lasting effect on its moneymaking machine.

In response, Facebook's stock tumbled more than 23 percent in after-hours trading, erasing more than \$120 billion in market value in less than two hours.

426. *The Los Angeles Times* similarly reported on July 26, 2018:⁴³⁸

Facebook Inc. saw the first signs of user disenchantment in the midst of public scandals over privacy and content, with second-quarter revenue and average daily visitors missing analysts' projections.

Its stock sank as much as 25% in extended trading.

* * *

The company's user growth fell short of expectations in the same quarter Chief Executive Mark Zuckerberg testified for 10 hours in Congress on data privacy issues. It also came as Europe implemented strict new data laws, which Facebook had warned could lead to fewer daily visitors in that region. The company also was bombarded by public criticism over its content policies, especially in countries such as Myanmar and Sri Lanka where misinformation has led to violence.

"The core Facebook platform is declining," said Brian Wieser, an analyst at Pivotal Research Group.

427. On September 5, 2018, the Pew Research Center issued a report it conducted from May 29 to June 11, 2018,

⁴³⁸ *BUSINESS BEAT; Facebook shares sink after miss; Firm sees revenue and daily visitors fall in second quarter amid public scandals over privacy and content*, L.A. Times (July 26, 2018).

in the aftermath of the Cambridge Analytica scandal. The report, “Americans are changing their relationship with Facebook,” documented changes in Facebook user engagement in previous 12 months, and revealed substantial disengagement by Facebook users in that period, including that more than half (54%) of Facebook users had changed their privacy settings to share less with Facebook, 42% had taken extended breaks from engaging with Facebook, while more than a quarter (26%) had deleted the Facebook app from their cell phones. “All told, some 74% of Facebook users say they have taken at least one of these three actions in the past year,” with disengagement particularly pronounced among the younger users coveted by advertisers.⁴³⁹

P. Facebook’s Class Period False Statements Reflect the Anti-Privacy Corporate Culture that Has Always Existed at Facebook

428. The many Class Period false statements made by defendants regarding privacy, supposed user control over data and related issues were simply reflecting a culture that existed at Facebook since its founding and through at least the end of the Class Period. That culture was to pay lip service to concerns about privacy and misuse of user data while at every turn prioritizing growth and user revenue. Whenever they were forced to choose between providing meaningful privacy protections for user data or opportunities for growth, the most senior executives at Facebook (including Zuckerberg and Sandberg) consistently minimized privacy concerns in favor of expanding Facebook.

⁴³⁹ Andrew Perrin, *Americans are changing their relationship with Facebook*, Pew Research Center (Sept. 5, 2018).

429. These anti-privacy decisions created an internal tension with Facebook's public stance that it respected user privacy. To retain the illusion that Facebook was accurately representing the way in which it protected sensitive user data, defendants developed a playbook for how to respond to public stories relating to misuse of such data. Time and time again they would respond to reporter inquiries on upcoming stories by attacking the stories, accusing them of being wrong, and trying to keep them from being published. Then, after the stories were published (and almost uniformly proved to be accurate) defendants would embark on a public apology tour replete with admissions of "mistakes," promises to do better in the future, dressed up with lavish statements regarding Facebook's high respect for user privacy and assurances that it was the Company's top priority.

430. Inside Facebook, senior employees were fully aware that Facebook's public act was a sham. Both prior to and throughout the Class Period, serious privacy concerns were raised to the highest levels of Facebook by very senior employees. Facebook's lack of response to these concerns was not innocent: it was deliberate strategy aimed at utilizing sensitive user data in order to grow Facebook no matter what the cost for user privacy.

431. According to Parakilas, Facebook's former operations manager, who "led Facebook's efforts to fix privacy problems on its developer platform" in advance of its IPO, Facebook "prioritized data collection from its users over protecting them from abuse" because "[t]he more data [Facebook] has [to] offer, the more value it creates for ad-

vertisers,” meaning “it has no incentive to police the collection or use of that data—except when negative press or regulators [we]re involved.”⁴⁴⁰

432. Parakilas further explained that Facebook “allocated resources in a way that implied that they were almost entirely focused on growth and monetization at the expense of user protection” and that he “could not get engineers to build or maintain some of the compliance functions that [he] felt were necessary.”⁴⁴¹

433. Indeed, according to Parakilas it was “well known at the company” that user data was being shared with third-party app developers.⁴⁴² For example, Parakilas said that in 2012 he had expressed concerns about these privacy practices to some of “[the top five] executives at the Company,” including in a presentation that contained a “map of [data] vulnerabilities.”⁴⁴³ Further, Parakilas said in an interview that his presentation documented the “many gaps that left users exposed” in Facebook’s platform⁴⁴⁴ and, in particular, highlighted how “the Facebook platform allowed developers to access a huge

⁴⁴⁰ Sandy Parakilas, *We Can't Trust Facebook to Regulate Itself*, N.Y. Times (Nov. 19, 2017).

⁴⁴¹ Noah Kulwin, ‘Facebook Is a Fundamentally Addictive Product,’ *Intelligencer* (Apr. 2018).

⁴⁴² David Morgan, *Former manager says he warned Facebook about potential privacy risks in 2012*, CBS News (Apr. 9, 2018).

⁴⁴³ Noah Kulwin, ‘Facebook Is a Fundamentally Addictive Product,’ *Intelligencer* (Apr. 2018).

⁴⁴⁴ Sandy Parakilas, *I worked at Facebook. I know how Cambridge Analytica could have happened.*, Wash. Post (Mar. 20, 2018).

amount of Facebook’s data”—which Parakilas described as “one of the biggest vulnerabilities the company had.”⁴⁴⁵

434. As Parakilas later testified to the U.K. House of Commons Digital, Culture, Media and Sport Committee, “the concern I had was that they [*i.e.*, Facebook and its senior executives] had built this platform that would allow people to get all of this data on people who had not really explicitly authorized” it.⁴⁴⁶ Parakilas elaborated that “it was really personal data,” including names, emails and even private messages, and “they basically allowed that to leave Facebook’s servers intentionally.”⁴⁴⁷ Parakilas stated that, although “executives at Facebook were well aware that developers could, without detection, pass data to unauthorized fourth parties”—such as what happened with Cambridge Analytica—he “did not get much if any follow-up from the executives,” who were “*not . . . concerned about the vulnerabilities that the Company was creating; they were concerned about revenue growth and user growth.*”⁴⁴⁸ He stated that “[d]espite my attempts to raise awareness about this issue, nothing was done to close the vulnerability.”⁴⁴⁹ Parakilas confirmed

⁴⁴⁵ Noah Kulwin, *Facebook Is a Fundamentally Addictive Product*, *Intelligencer* (Apr. 2018).

⁴⁴⁶ Parakilas testified to the House of Commons’ Digital, Culture, Media and Support Committee in the U.K. on March 21, 2018 (“Parakilas U.K. Test.”) at Q1206.

⁴⁴⁷ *Id.*

⁴⁴⁸ James Jacoby and Anya Bourg, *Facebook Insider Says Warning About Data Safety Went Unheeded By Executives*, *PBS Frontline* (Mar. 20, 2018).

⁴⁴⁹ *Id.*

that his warnings went to Facebook executives who were **“among the top five executives in the company.”**⁴⁵⁰

435. Moreover, Facebook executives knew that once the app developers had this unauthorized data, there was essentially nothing that Facebook could do to control how it was used. Confirming this, Parakilas testified that “there were not any controls once the data had left [Facebook] to ensure that it was being used in an appropriate way.”⁴⁵¹ Likewise, Parakilas stated to *The Guardian*,⁴⁵² that Facebook had **“Zero. Absolutely no[]”** control over the data once it left “Facebook servers.” So, Facebook **“had no idea what developers were doing with the data,”** according to Parakilas.

436. Parakilas could not recall “the company conducting a single audit of a developer where the company inspected the developer’s data storage.”⁴⁵³ Parakilas also said he had told other Facebook executives to audit its app developers to find out “what’s going on with the data” they were collecting from users, to which one executive responded, “Do you really want to see what you’ll find?”⁴⁵⁴ **“They felt that it was better not to know,”** Parakilas told

⁴⁵⁰ See, e.g., James Jacoby & Anya Bourg, *Facebook Insider Says Warnings About Data Safety Went Unheeded By Executives*, Frontline (Mar. 20, 2018); see also *id.* at 4:01 of the embedded video (Mr. Parakilas is asked, “And how senior were the senior executives?” He responds, “Very senior. Like, among the top five executives in the Company.”).

⁴⁵¹ Parakilas U.K. Test. at Q1206.

⁴⁵² Paul Lewis, ‘Utterly Horrifying’: ex-Facebook insider says covert data harvesting was routine, *Guardian* (Mar. 20, 2018).

⁴⁵³ *Id.*

⁴⁵⁴ *Id.*

The Guardian.⁴⁵⁵ “The company just wanted negative stories to stop,” he said. “It didn’t really care how the data was used.”⁴⁵⁶

437. Despite Facebook’s many assurances to the contrary—including its April 2014 false promise to eliminate third-party sharing of data—Facebook’s deliberately lax privacy practices continued even *after* discovery of the Cambridge Analytica issues. According to a June 18, 2016 memorandum posted on the Company’s internal website by Facebook VP Andrew Bosworth, who has been described as one of “Zuckerberg’s most trusted lieutenants”.⁴⁵⁷

The ugly truth is that we believe in connecting people so deeply that anything that allows us to connect more people more often is *de facto* good. It is perhaps the only area where the metrics do tell the true story as far as we are concerned.

⁴⁵⁵ Paul Lewis, *Utterly horrifying: ex-Facebook insider says covert data harvesting was routine*, *Guardian* (Mar. 20, 2018).

⁴⁵⁶ Sandy Parakilas, *We Can’t Trust Facebook to Regulate Itself*, *N.Y. Times* (Nov. 19, 2017).

⁴⁵⁷ The description was in an article by *Buzzfeed News* accompanying the memo, both of which were published on March 29, 2018. *Buzzfeed* reported that, as of the time its article was published, the memo was still available and regularly accessed on Facebook’s internal website. Ryan Mac, Charlie Warzel and Alex Kantrowitz, *Top Facebook Executive Defended Data Collection in 2016 Memo—And Warned That Facebook Could Get People Killed*, *Buzzfeed* (Mar. 29, 2018); Gideon Lichfield, *Watch Sheryl Sandberg’s technique for shielding Facebook from hard questions*, *Quartz at Work* (Oct. 13, 2017); Sandy Parakilas, *We Can’t Trust Facebook to Regulate Itself*, *N.Y. Times* (Nov. 19, 2017); Noah Kulwin, *Facebook Is a Fundamentally Addictive Product*, *Intelligencer* (Apr. 10, 2018).

That isn't something we are doing for ourselves. Or for our stock price (ha!). It is literally just what we do. We connect people. Period.

That's why all the work we do in growth is justified. ***All the questionable contact importing practices.*** All the subtle language that helps people stay searchable by friends. All of the work we do to bring more communication in. The work we will likely have to do in China some day. All of it.

* * *

I know a lot of people don't want to hear this. Most of us have the luxury of working in the warm glow of building products consumers love. But make no mistake, ***growth tactics are how we got here.*** If you joined the company because it is doing great work, that's why we get to do that great work. We do have great products but we still wouldn't be half our size without pushing the envelope on growth. Nothing makes Facebook as valuable as having your friends on it, and no product decisions have gotten as many friends on as the ones made in growth.

438. The memo, originally posted to “rally the troops” in response to controversy sparked by the live streaming of a shooting death on Facebook, stated that collateral damage to users was irrelevant: “So we connect more people. That can be bad if they make it negative. Maybe it costs a life by exposing someone to bullies. Maybe someone dies in a terrorist attack coordinated on our tools. And still we connect people.”⁴⁵⁸

⁴⁵⁸ Ryan Mac, Charlie Warzel and Alex Kantrowitz, *Top Facebook Executive Defended Data Collection in 2016 Memo—And Warned That Facebook Could Get People Killed*, BuzzFeed (Mar. 29, 2018).

439. In December 2017, Alex Stamos, Facebook’s Chief Information Security Officer (and a co-author of the white paper described above), was forced out of his job as a result of “internal disagreements over how the social network should deal with its role in spreading disinformation.”⁴⁵⁹

440. Tellingly, Stamos’ departure was not reported until March 19, 2018—*after* it was publicly revealed that the Company had failed to verify that user data had been deleted by Cambridge Analytica and other third parties or notify the affected users that their privacy had been compromised. *The New York Times* reported that Stamos had clashed with top executives, including Sandberg, because he had “advocated more disclosure around Russian interference.”⁴⁶⁰ The article said that the Company wanted to handle his departure quietly because “executives thought his departure would look bad” in light of the circumstances surrounding the investigations into Russian hacking.

441. In a follow-up article, *The New York Times* reported.⁴⁶¹

After a breach of the Democratic National Committee in June 2016, Mr. Stamos pulled together a team to investigate Russian interference on Facebook. The findings pit him against executives in the company’s legal and communications groups. While Mr. Stamos

⁴⁵⁹ Joseph Menn, *UPDATE 1-Facebook’s security chief to depart, source says*, Reuters (Mar. 19, 2018).

⁴⁶⁰ Sheera Frenkel, Nicole Perlroth and Scott Shane, *Facebook Exit Hints and Dissent on Handling of Russian Trolls*, N.Y. Times (Mar. 19, 2018).

⁴⁶¹ Sheera Frenkel and Nicole Perlroth, *The End for Facebook’s Security Evangelist*, N.Y. Times (Mar. 20, 2018).

argued to disclose more, others said that by proactively disclosing what they had found, Facebook had become a target for further public ire, according to seven current and former Facebook employees.

442. In an internal memo circulated at Facebook on March 23, 2018 in response to *The New York Times* report, Stamos acknowledged that he had disagreements with other executives over information security. Although Stamos denied that he had been forced out, he went on to criticize a corporate culture at Facebook regarding the protection of user data.⁴⁶²

“We need to build a user experience that **conveys honesty and respect**, not one optimized to get people to click yes to giving us more access,” Stamos wrote. We need to intentionally **not collect data** where possible, and to keep it **only as long as we are using it** to serve people.”

* * *

We need to **find and stop adversaries** who will be copying the playbook they saw in 2016. We need to **listen to people** (including internally) when they tell us a feature is creepy or point out a negative impact we are having in the world. We need to **deprioritize short-term growth** and revenue and to explain to Wall Street why that is ok. We need to be **willing to pick sides** when there are clear moral or humanitarian issues. And we need to be **open, honest and transparent** about challenges and what we are doing to fix them. (Emphasis in original).

⁴⁶² Ryan Mac and Charlie Warzel, *Departing Facebook Security Officer’s Memo: “We Need To Be Willing To Pick Sides.”* BuzzFeed (July 29, 2018).

443. As *Business Insider* reported on April 9, 2018, Facebook employees are “quitting or asking to switch departments over ethical concerns.”⁴⁶³ These “dissatisfied Facebook engineers are reportedly attempting to switch divisions to work on Instagram or WhatsApp, rather than continue work on the platform responsible for the Cambridge Analytica scandal.” Indeed, “[a]s it became evident that Facebook’s core product might be to blame” for the data security breach, “engineers working on it reportedly found it increasingly difficult to stand by what it built.”⁴⁶⁴

V. Facts Revealed Through Recent Regulatory Actions, Investigations and Other Proceedings Have Further Confirmed Defendants’ Deliberate Misconduct During the Class Period

444. Facebook’s misconduct as alleged herein has been confirmed and corroborated by specific facts uncovered in multiple governmental and regulatory investigations both in the United States and abroad, as well as by court proceedings throughout the country. These proceedings and investigations have been detailed and extensive and include review or access to previously-unavailable internal Facebook documents, direct interviews or sworn testimony from Facebook executives and Facebook’s past interactions with regulators.

445. They have resulted in specific findings that: (i) Facebook knowingly made materially false and misleading statements during the Class Period relating to its risk disclosures and about its purported response to the

⁴⁶³ Prachi Bhardwaj, *Some Facebook employees are reportedly quitting or asking to switch departments over ethical concerns*, *Business Insider* (Apr. 9, 2018).

⁴⁶⁴ *Id.*

Cambridge Analytica data scandal, *SEC v. Facebook, Inc.*, 3:19-cv-04241-JD (N.D. Cal.) (defined above as the “SEC Complaint”); (ii) Facebook made repeated misrepresentations regarding its handling of user data and deliberately violated the 2012 FTC Consent Decree, *United States of America v. Facebook*, Case No. 19-cv-2184 (D.D.C.) (defined above as the “FTC Complaint”); (iii) Facebook’s users could proceed with the vast majority of their privacy lawsuit against Facebook, including on claims that specifically sound in fraud, *In re Facebook, Inc. Consumer Privacy User Profile Litig.*, 2019 WL 4261048 (N.D. Cal. Sept. 9, 2019) (defined above as the “Consumer Case”) (“plaintiffs have also adequately alleged that Facebook intended to defraud its users regarding this conduct”); and (iv) concluded that “Facebook *intentionally and knowingly violated both data privacy* and anti-competition laws,” Final Report of the Digital, Cultural, Media and Sport Committee of the British House of Commons (defined below as the “Final Report”).

A. Defendants’ Liability for Securities Fraud Is Confirmed in Actions Filed by the SEC and the FTC

446. As noted above, after extensive investigations the SEC and the FTC both concluded that Facebook engaged in significant misconduct with respect to its representations regarding user data and privacy.

1. Facebook Paid \$100 Million Dollars to Settle SEC Charges that Facebook Committed Securities Fraud

447. In late July 2019, following an extensive, year-long investigation,⁴⁶⁵ the SEC announced that defendant Facebook had agreed to pay \$100 million to resolve SEC charges that Facebook had made, *inter alia*, “untrue statements of material fact” or material omissions that operated “as a ***fraud or deceit upon purchasers***” of its securities.⁴⁶⁶ The SEC’s case was based on a review of internal documents and supported by specific facts uncovered in its investigation.

448. **False Risk Disclosures.** The SEC charged Facebook with making materially false and misleading statements in the “risk factors” section of its SEC filings, including its filings during the Class Period. Specifically, the SEC charged that “[i]n its quarterly and annual reports filed between January 28, 2016 and March 16, 2018, Facebook did not disclose that a researcher had, in violation of the company’s policies, transferred data relating to [tens of millions of Facebook users] to Cambridge Analytica. Instead, Facebook misleadingly presented the potential for misuse of user data as merely a hypothetical risk.”⁴⁶⁷

⁴⁶⁵ On July 12, 2018, *The Wall Street Journal* reported that the SEC was investigating “whether Facebook Inc. adequately warned investors that developers and other third parties may have obtained users’ data without their permission or in violation of Facebook policies.” See Dave Michaels & Georgia Wells, *SEC Probes Why Facebook Didn’t Warn Sooner on Privacy Lapse*, Wall St. J. (July 12, 2018).

⁴⁶⁶ SEC Complaint at ¶153.

⁴⁶⁷ *Id.* at ¶16.

449. The SEC concluded “Facebook knew, or should have known, that its Risk Factor disclosures in its annual reports on Form 10-K for the fiscal years ended . . . December 31, 2016, and December 31, 2017, and its quarterly reports on Form 10-Q filed in . . . 2017 . . . were materially misleading.”⁴⁶⁸

450. **False Statements Regarding Cambridge Analytica.** The SEC also charged Facebook with making materially misleading statements about “its investigation into the Cambridge Analytica matter.” Specifically, the SEC charged Facebook with “falsely claim[ing] the company found no evidence of wrongdoing,” which “reinforce[ed] the misleading statements in its periodic filings.”⁴⁶⁹ The SEC pointed to the fact that, when asked by reporters about its investigation into the Cambridge matter, authorized Facebook representatives stated “Our investigation to date has not uncovered anything that suggests wrongdoing.”⁴⁷⁰ As the SEC charged, this “was misleading because Facebook had, in fact, determined that [Kogan’s] transfer of user data to Cambridge violated the Company’s Platform Policy.”⁴⁷¹

451. **The SEC Relied on Numerous Facts.** In support of its charges, the SEC pointed to multiple facts, including the following. First, as early as September 2015, Facebook “was already familiar with Cambridge and had suspicions that Cambridge had misused user data.”⁴⁷²

⁴⁶⁸ *Id.* at ¶144.

⁴⁶⁹ *Id.*

⁴⁷⁰ *Id.* at ¶149.

⁴⁷¹ *Id.* at ¶134.

⁴⁷² *Id.*

Second, in December 2015, Facebook learned that Cambridge Analytica had improperly bought Facebook user data from Kogan in violation of Facebook’s policies. At that time, Kogan and Cambridge Analytica “confirmed to Facebook that [Kogan] had used a Facebook app to collect user data and then used that data to create personality scores, which were then shared with Cambridge.”⁴⁷³ Facebook determined that this transfer to Cambridge Analytica “violated the Company’s Platform Policy”⁴⁷⁴ and disseminated this conclusion widely within Facebook, including to “Facebook’s communications, legal, operations, policy, privacy and research groups.”⁴⁷⁵

452. Third, in June 2016, Facebook learned that Kogan and Cambridge Analytica lied about the improper transfer and purported deletion of Facebook user data. In particular, in June 2016, Kogan revealed to Facebook that “contrary to [Kogan’s] and Cambridge [Analytica’s] representations in December 2015,” it was not only user “personality scores” had been improperly sold to Cambridge Analytica. Instead, Kogan had also improperly shared “actual Facebook user data, including names, birthdays, location, and certain page likes.”⁴⁷⁶ This also revealed that Cambridge Analytica had lied to Facebook when it represented in December 2015 that it had deleted the Facebook user data that it had received from Kogan.⁴⁷⁷ Following exposure of these lies in June 2016,

⁴⁷³ *Id.* at ¶129.

⁴⁷⁴ *Id.* at ¶130. The SEC defined Facebook’s “Platform Policy” as “a set of rules governing what developers are allowed to do with the apps they create and the data that they gather.” *Id.*

⁴⁷⁵ *Id.*

⁴⁷⁶ *Id.*

⁴⁷⁷ *Id.* (noting that, in December 2015, “Cambridge . . . told Facebook that it had deleted the data received from [Kogan]”).

it was not until nearly one year later in April 2017 that Facebook received from Cambridge Analytica another representation that the improperly-shared Facebook user data was purportedly deleted.⁴⁷⁸

453. Fourth, the SEC noted that “[t]hroughout 2016, red flags were raised to Facebook suggesting that Cambridge was potentially misusing Facebook user data.”⁴⁷⁹ These red flags included Facebook’s awareness of “a video of a marketing presentation by Cambridge’s chief executive officer about the firm’s ability to target voters based on personality,” and the Company’s knowledge of the fact that “Cambridge named Facebook and Instagram advertising audiences by personality trait for certain clients”—coupled with Facebook’s awareness of media reports of Cambridge’s use of personality profiles to target advertising in summer and fall 2016.⁴⁸⁰

454. Fifth, the SEC explained that it was not until March 16, 2018 that Facebook “publicly acknowledged, **for the first time**, that it had confirmed that [Kogan] had transferred user data to Cambridge, in violation of its Platform Policy, and that the company had told [Kogan] and Cambridge to delete the data in December 2015.”⁴⁸¹

455. On August 22, 2019, Judge James Donato entered a final judgment as to defendant Facebook in the SEC Action, which, *inter alia*, permanently enjoined Facebook from further: (i) selling securities “by means of any untrue statement of a material fact” or “any omission

⁴⁷⁸ *Id.* at ¶32.

⁴⁷⁹ *Id.* at ¶35.

⁴⁸⁰ *Id.*

⁴⁸¹ *Id.* at ¶51.

of material fact”; and (ii) operating a “fraud or deceit upon the purchaser” of its securities.⁴⁸²

2. Facebook Paid a Record-Setting \$5 Billion Dollar Penalty to Settle FTC Charges that Facebook Violated User Privacy and the FTC Consent Decree

456. On July 24, 2019, following a detailed investigation spanning more than one year, the FTC announced that Facebook had agreed to “pay a record-breaking \$5 billion penalty and submit to new restrictions and a modified corporate structure that will hold the company accountable for the decisions it makes about its users’ privacy,” in order to “settle [FTC] charges that [Facebook] violated a 2012 FTC order by deceiving users about their ability to control the privacy of their information.”⁴⁸³

457. The \$5 billion penalty against Facebook was the **“largest ever imposed on any company for violating consumers’ privacy,”** was “almost **20 times greater** than the largest privacy or data security penalty ever imposed worldwide” and was “one of the **largest penalties ever assessed by the U.S. government for any violation.**”⁴⁸⁴

⁴⁸² SEC Action, ECF No. 11 at 1-2.

⁴⁸³ Press Release, *FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, Federal Trade Commission (July 24, 2019).

⁴⁸⁴ *Id.*

a. The FTC Imposed Privacy Reforms Designed to Remove Zuckerberg’s “Unfettered Control” over “Decisions Affecting User Privacy”

458. In addition to a record-setting penalty, the FTC also forced Facebook to implement significant privacy reforms in order to “prevent Facebook from deceiving its users about privacy in the future” and, in particular, to remove Zuckerberg’s “unfettered control” over privacy-related decisions at Facebook. Indeed, as described by the FTC: “The [new FTC] order creates greater accountability at the board of directors level. It establishes an independent privacy committee of Facebook’s board of directors, *removing unfettered control by Facebook’s CEO Mark Zuckerberg over decisions affecting user privacy.*”

459. These far-reaching privacy reforms were set forth in a stipulated order (the “Stipulated Order”) signed by Zuckerberg. Among other things, the reforms included:

- Prohibitions on Facebook engaging in further misrepresentations concerning its privacy practices, including misrepresentations about Facebook’s “collection, use or disclosure of [user personal information],” the “extent to which a consumer can control the privacy of [user personal information],” “the extent to which [Facebook] makes or has made [user personal information] accessible to third parties,” and the “steps [Facebook] takes or has taken to verify the privacy or security protections that any third party provides”;⁴⁸⁵

⁴⁸⁵ Stipulated Order, §I (“Prohibition Against Misrepresentations”).

- Requiring Facebook to obtain a “User’s affirmative express consent” prior to sharing user personal information with third parties;⁴⁸⁶
- Requiring Facebook to establish and implement a “comprehensive privacy program” to protect user personal information, including the appointment of a “Chief Privacy Officer,” rigorous documentation requirements and regular privacy audits at least every 12 months;⁴⁸⁷ and
- Requiring Facebook to establish an “Independent Privacy Committee” consisting of Independent Directors to assess the state of Facebook’s privacy program, its compliance with the Stipulated Order and the existence and mitigation of any “material risks to the privacy, confidentiality, and Integrity” of user personal information.⁴⁸⁸

460. Facebook is required to comply with the Stipulated Order and its privacy reforms for the next 20 years.

b. The FTC Charged Facebook with Violating the 2012 FTC Consent Decree Through “Deceptive Privacy Settings and Statements”

461. The FTC charged Facebook with violating the 2012 FTC Consent Decree by “subvert[ing] users’ privacy choices to serve its own business interests” through “at least June 2018”⁴⁸⁹—which covers nearly the entire Class Period here. As explained by the FTC, Facebook made

⁴⁸⁶ *Id.*, §II (“Changes To Sharing Of Nonpublic User Information”).

⁴⁸⁷ *Id.*, §VII (“Mandated Privacy Program”).

⁴⁸⁸ *Id.*, §X (“Mandated Independent Privacy Committee And Other Governance Matters”).

⁴⁸⁹ FTC Complaint at ¶4.

“deceptive privacy . . . statements” regarding its users’ ability to restrict “the sharing of their information to their Facebook Friends, when, in fact, third-party developers could access and collect their data through their Friends’ use of third-party developers’ apps.”⁴⁹⁰ Among other statements, the FTC devoted considerable focus to the fact that defendants had “misrepresent[ed] ‘the extent to which a consumer can control the privacy of their personal information,’”⁴⁹¹ which violated Parts I.B and I.C of the 2012 Consent Decree.

462. Moreover, the FTC charged Facebook with knowingly or recklessly violating the FTC Consent Decree by depriving users of control over their personal information. For example, the FTC stated that “Facebook knew or should have known that its conduct violated the 2012 [Consent Decree] because it was engaging in the very same conduct that the [FTC] alleged was deceptive in Count One of the original Complaint that led to the 2012 Order.”⁴⁹²

463. In support of these charges, the FTC relied on the fact that, from “April 30, 2015, to at least June 2018” Facebook misrepresented that users could “control” the privacy of their data, when, in fact, “regardless of the privacy settings a user checked, Facebook continued to provide access to [user personal information] to Whitelisted Developers.”⁴⁹³ These Whitelisted Developers with undisclosed access to user friend information included more

⁴⁹⁰ *Id.* at ¶19.

⁴⁹¹ *See, e.g., id.* at ¶¶16, 155, 160, 166.

⁴⁹² *Id.*

⁴⁹³ *See, e.g., id.* at ¶¶106-113, 166-175.

than two dozen “gaming, retail, and technology companies, as well as third-party developers of dating apps and other social media services”;⁴⁹⁴

464. According to the FTC, Facebook also knowingly or recklessly violated the FTC Consent Decree by:

- Publicly misrepresenting that it would “no longer allow third-party developers to access [user friend data]” when, in fact, “Facebook continued to allow millions of third-party developers access to [user friend data] for at least another year”;⁴⁹⁵ and
- “[R]epresenting to consumers that they could control the privacy of their data by using desktop and mobile privacy settings to limit the information Facebook could share with their Facebook Friends” when, in fact, “Facebook did not limit its sharing of consumer information with third-party developers based on the privacy settings.”⁴⁹⁶

c. The FTC Charged Facebook with Violating the 2012 Consent Decree by Failing to Maintain a Reasonable Privacy Program

465. The FTC also charged that Facebook violated the 2012 Consent Decree because it “failed to maintain a reasonable privacy program that safeguarded the privacy, confidentiality, and integrity of user information, as required by Part IV of the 2012 Order.”⁴⁹⁷ This violated Part IV of the 2012 Consent Decree.

⁴⁹⁴ *Id.* at ¶108.

⁴⁹⁵ *Id.* at ¶¶160-165.

⁴⁹⁶ *Id.* at ¶¶155-159.

⁴⁹⁷ *Id.* at ¶10.

466. Specifically, Facebook failed to “vet third-party developers before granting them access to consumer data”⁴⁹⁸ and, then, Facebook’s “enforcement of its policies, terms and conditions . . . was inadequate and was influenced by the financial benefit that violator third-party app developers provided to Facebook.” As the FTC stated: “This conduct was unreasonable.”⁴⁹⁹

d. The FTC Charged Facebook with Violating the 2012 Consent Decree by Misusing User Information Provided for Account Security

467. The FTC also charged Facebook with violating users’ privacy by engaging in “deceptive practices” in violation of §5(a) of the *Federal Trade Commission Act* (the “FTC Act”). Among other things, Facebook violated §5(a) of the FTC Act because it represented that users’ “phone numbers provided for two-factor authentication would be used for security purposes.”⁵⁰⁰ In reality, and contrary to its representations, “Facebook would also use [those] phone numbers . . . for targeting advertisements to those users.”⁵⁰¹

e. Defendants Facebook and Zuckerberg Agreed that the Facts in the FTC Complaint Would Be “Taken as True” in Any Subsequent FTC Enforcement Action

468. In the Stipulated Order, which was signed by Zuckerberg himself, Facebook agreed that “the facts alleged in the [FTC’s] Complaint *will be taken as true*,

⁴⁹⁸ *Id.* at ¶¶11-12.

⁴⁹⁹ *Id.* at ¶12; *see also id.* at ¶¶176-182.

⁵⁰⁰ *Id.* at ¶187.

⁵⁰¹ *Id.* at ¶188.

without further proof” in any “subsequent” litigation by the FTC to enforce its rights under the Stipulated Order.⁵⁰²

B. Defendants’ Privacy Violations and Misuse of User Data Are Confirmed by Multiple Courts Nationwide

1. Another Court in This District Has Sustained Claims Against Facebook for Improperly Sharing Users’ Personal Information with Third Parties

469. On September 9, 2019, in a related MDL privacy case against Facebook, Judge Chhabria issued an opinion and order largely denying Facebook’s motion to dismiss. In that opinion he addressed several factual issues that are also relevant to this securities litigation. *See In re Facebook Inc., Consumer Privacy User Profile Litig.*, 2019 WL 4261048 (N.D. Cal. Sept. 9, 2019) (Chhabria, J.) (defined above as the “Consumer Case”).

470. Judge Chhabria stated that “[b]roadly speaking, this [consumer] case is about whether Facebook acted unlawfully in making user information widely available to third parties. It’s also about whether Facebook acted unlawfully in failing to do anything meaningful to prevent third parties from misusing the information they obtained.”⁵⁰³

471. The plaintiffs in the Consumer Case pursued four main categories of wrongdoing against Facebook: (1) giving app developers unauthorized access to sensitive user information; (2) continued disclosure by Facebook through at least June 2018 of sensitive user information

⁵⁰² Stipulated Order at 3 at ¶E.

⁵⁰³ *Id.* at *2.

to “whitelisted” apps; (3) sharing sensitive user information with business partners through at least June 2018; and (4) failing to prevent third parties from misusing the information Facebook allowed them to access.⁵⁰⁴

472. Facebook argued in its motion to dismiss that all of the claims asserted in the Consumer Case failed because Facebook users purportedly had agreed that “Facebook could disseminate their ‘friends only’ information in the way it has done.”⁵⁰⁵ The court rejected this argument on several grounds.

473. First, the court was forced to apply a “fiction” created by California law, which “requires the Court to *pretend* that users actually read Facebook’s contractual language before clicking their acceptance, *even though we all know virtually none of them did.*”⁵⁰⁶

474. The court expressly doubted that any Facebook user had consented to this practice in *reality*, as opposed to the legal fiction created by operation of California law. The court stated that “in reality, virtually no one ‘consented’ in a layperson’s sense to Facebook’s dissemination of this information to app developers.”⁵⁰⁷

475. Moreover, the court distinguished its ruling under California law from the FTC lawsuit. The court noted that “the FTC’s claims against Facebook are not based on California law; they are based on alleged violations of the

⁵⁰⁴ *Id.* at *4-*5.

⁵⁰⁵ *Id.* at *4.

⁵⁰⁶ *Id.* at *12.

⁵⁰⁷ *Id.* (“for the rare person who actually read the contractual language, it would have been difficult to isolate and understand the pertinent language among all of Facebook’s complicated disclosures.”).

Federal Trade Commission Act and the earlier FTC consent order from 2012.”⁵⁰⁸ According to the court.⁵⁰⁹

While California law, for better or worse, allows Facebook to ***bury a disclosure*** of its information-sharing practices in the fine print of its contractual language, the ***FTC consent order required Facebook to disclose such practices prominently, in a way that would likely come to the attention of Facebook users***. More broadly, the consent order precluded Facebook from explicitly or implicitly misrepresenting the extent to which the company protects user privacy.

476. Second, the court found it “easy to conclude” that users could pursue claims against Facebook based on Facebook’s post-2014 disclosure of information to whitelisted apps, which the consumer plaintiffs alleged was done because these apps generated revenue for Facebook.⁵¹⁰ The court noted that “thousands of companies were allegedly on this list, including Airbnb, Netflix, UPS, Hot or Not, Salesforce, Lyft, Telescope, and Spotify.”⁵¹¹

477. Third, the court rejected Facebook’s argument that users had consented to Facebook’s disclosure of sensitive information to a wide range of other enormous companies. While Facebook contended that its Data Use Policy disclosed this practice, the court held that it “does not come close to disclosing the ***massive information-sharing program*** with business partners that plaintiffs allege.”⁵¹² As the court noted, Facebook itself had since

⁵⁰⁸ *Id.* at *13 n.13.

⁵⁰⁹ *Id.*

⁵¹⁰ *Id.* at *25.

⁵¹¹ *Id.* at *8.

⁵¹² *Id.* at *25.

identified a “non-exclusive list of companies” that includes such giants as Blackberry, Samsung, Yahoo, the Russian search engine Yandex, Amazon, Microsoft, and Sony.⁵¹³

478. Finally, the court allowed the consumer plaintiffs to pursue claims based on allegations that although Facebook had a policy preventing app developers from using information for improper purposes, “Facebook did nothing to enforce this policy, thus giving users the impression that their information was protected, while in reality countless app developers were using it for other purposes.”⁵¹⁴ The court noted that Facebook interpreted its policy to mean, in essence, “we tell app developers that they can only use your information to facilitate their interactions with your friends, but you can’t really be sure they’ll honor that.”⁵¹⁵ The court characterizes this as a view that the Facebook user “assumed the risk that app developers would misuse [their] information.”⁵¹⁶

479. The court rejected Facebook’s argument, noting that its Data Use Policy could reasonably be interpreted to mean that “Facebook is actively policing the activities of app developers . . . and thereby successfully preventing sensitive information from being misappropriated.”⁵¹⁷ The Court also noted that the Data Use Policy could be interpreted by a reasonable user to mean that the “Facebook platform has the ability to *physically prevent* app

⁵¹³ *Id.* at *8.

⁵¹⁴ *Id.* at *9 (using Cambridge Analytica as an example).

⁵¹⁵ *Id.* at *28.

⁵¹⁶ *Id.*

⁵¹⁷ *Id.*

developers from being able to ‘see’ friend information outside the context of their interactions with users.”⁵¹⁸

480. Based on these findings, the court concluded that the consumer plaintiffs had successfully pled a number of privacy-related claims, including claims based on concealment and deceit that “sound in fraud,” and had to satisfy the strict pleading requirements of Rule 9(b).⁵¹⁹ For these claims, the court held:⁵²⁰

The plaintiffs have also adequately alleged that Facebook *intended to defraud its users* regarding this conduct: the plaintiffs contrast Facebook’s *public-facing statements about protecting privacy* and restricting information-sharing with the *reality of Facebook’s alleged practices*, and that contrast is a sufficient basis from which to infer fraudulent intent at the pleading stage.

2. The Court of Chancery of the State of Delaware

481. On May 30, 2019, Vice Chancellor Joseph R. Slight of the Delaware Court of Chancery (the “Delaware Court”) issued an opinion in the action captioned *In re Facebook, Inc. Section 220 Litig.* (the “Delaware Opinion”). In the Delaware Opinion, “[a]fter carefully reviewing the evidence and the arguments of counsel” submitted in a one-day trial, the Delaware Court concluded that the plaintiffs there had “demonstrated, by a preponderance of the evidence, a credible basis [to] infer that *wrongdoing occurred at the Board level in connection with data privacy breaches*” by Facebook and its executives. Thus,

⁵¹⁸ *Id.* at *28-*29.

⁵¹⁹ *Id.* at *37

⁵²⁰ *Id.*

the Delaware Court ordered Facebook to produce certain books and records documents sought by the plaintiffs.

482. In reaching this conclusion, the Delaware Court relied on evidence that Facebook and its directors knowingly violated the FTC Consent Decree. For example, the Delaware Court found evidence that Facebook’s Board of Directors “knew the Company had not implemented or maintained” measures required by the FTC Consent Decree but “nevertheless condoned the Company’s monetization of its users’ private data in violation of the Consent Decree.” Notably, both defendants Zuckerberg and Sandberg sat on Facebook’s Board during the Class Period.

483. The Delaware Court further noted that the “Cambridge Analytica Scandal was facilitated by Facebook’s policies” and it “would not have happened” if Facebook had complied with the FTC Consent Decree. The Delaware Court also explained that Facebook’s practice of entering into so-called “whitelist” agreements with device manufacturers, providing the latter with “the personal data of hundreds of millions of [Facebook’s] users” without user consent or knowledge. Specifically, the Delaware Court found evidence that Facebook gave these “whitelisted” device makers “unauthorized access to the Facebook platform and Facebook’s user data for a substantial fee” but “[a]ll the while, its users were left in the dark.”

484. The Delaware Court also relied on evidentiary-based conclusions by the United Kingdom’s Parliamentary Committee that “emails from Zuckerberg and Sandberg” showed that “**Facebook ‘intentionally and knowingly’ violated both data privacy and competition laws.**” Indeed, the Delaware Court cited the U.K. Parliamentary Committee’s conclusion that Facebook’s

Board—which as noted above included both defendants Zuckerberg and Sandberg—“was aware of data privacy breaches but attempted to ‘deflect attention’ from those breaches to avoid scrutiny.” The Delaware Court also found a “credible basis to infer [Facebook’s] Board knew the Company was allowing unauthorized third-party access to user data.”

485. Finally, the Delaware Opinion discusses the fact that, in July 2018, Facebook suffered “one of the sharpest single-day market value declines in history when its stock price dropped 19%, wiping out \$120 billion of shareholder wealth.” The Court concluded that this “unprecedented misfortune followed new reports that, in 2015, the private data of 50 million Facebook users had been poached by Cambridge Analytica.”

3. The Superior Court of the District of Columbia

486. On May 31, 2019, the Honorable Fern Flanagan Saddler of the Superior Court of the District of Columbia (the “D.C. Court”) released an opinion (the “D.C. Opinion”) in the action captioned *District of Columbia v. Facebook, Inc.*, No. 2018 CA 8715B (D.C. Sup. Ct.). The D.C. Opinion also authorized discovery into Facebook’s privacy practices and potential misconduct, based on the D.C. Court’s conclusion that the District of Columbia’s Office of the Attorney General “allege[d] sufficient facts to demonstrate that Facebook’s alleged statements, actions, or omissions could be interpreted . . . as material and misleading.”

C. Defendants' Privacy Violations and Misuse of User Data Are Confirmed in Multiple Investigations by Other Nations

1. United Kingdom's House of Commons Digital, Culture, Media and Sport Committee

487. On February 19, 2019, the Digital, Cultural, Media and Sport Committee (“DCMSC” or the “Committee”) of the British House of Commons issued its “Disinformation and ‘fake news’: Final Report” (the “Final Report”), a scathing condemnation of Facebook’s privacy practices and its misuse of user data. The DCMSC concluded, “[I]t is evident that *Facebook intentionally and knowingly violated both data privacy* and anti-competition laws.”⁵²¹ The Committee also concluded, “The Cambridge Analytica scandal was facilitated by Facebook’s policies.”⁵²²

2. Joint Investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia

488. On April 25, 2019, the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia (the “Commissions”) issued their Report of Findings (“Report”), outlining the conclusions of their joint investigation into Facebook’s compliance with Canada’s Personal Information Protection and Electronic Documents Act (“PIPEDA”) and British Columbia’s Personal Information Protection Act (“PIPA”). The Commissions determined that Facebook failed to protect

⁵²¹ U.K. Parliamentary Comm. Final Rep. at 41, 91.

⁵²² *Id.* at 26.

the personal information of users from unauthorized disclosure. Specifically, the Report concluded that: “(i) Facebook failed to obtain valid and meaningful consent of installing users”; “(ii) Facebook also failed to obtain meaningful consent from friends of installing users”; “(iii) Facebook had inadequate safeguards to protect user information”; and “(iv) Facebook failed to be accountable for the user information under its control.”⁵²³

D. Post-Class Period Events Confirm Defendants’ Privacy Violations and Misuse of User Data During the Class Period

1. Defendants’ Internal Investigation Reveals that “Tens of Thousands” of Apps Abused User Data

489. On September 20, 2019, defendants announced an “update on our ongoing App Developer Investigation, which we began in March of 2018 as part of our response to the episode involving Cambridge Analytica.”⁵²⁴ The investigation concerned “apps that had access to large amounts of information before we changed our platform policies in 2014,” and Facebook revealed: “To date, this investigation has addressed *millions of apps*. Of those, *tens of thousands have been suspended for a variety of reasons* while we continue to investigate. Specifically, Facebook investigated and suspended apps “for any number of reasons including *inappropriately sharing data obtained from us, making data publicly available* without

⁵²³ Joint Investigation of the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia, “Report of findings,” Overview (Apr. 25, 2019).

⁵²⁴ Ime Archibong, *An Update on Our App Investigation and Audit*, Facebook Newsroom (Sept. 20, 2019).

protecting people’s identity or *something else that was in clear violation* of our policies.”⁵²⁵

490. Defendants noted that the banned apps came from about 400 developers, though they only identified a handful by name in the announcement. For instance, defendants announced that they banned an app called my-Personality, “which *shared information with researchers and companies* with only limited protections in place”—the exact same abuse of user data that triggered the Cambridge Analytica scandal. Facebook similarly suspended apps like Rankwave for failing to cooperate with its investigation, LionMobi and JediMobi for “infect[ing] users’ phones with malware in a profit-generating scheme,” and others for “using quiz apps to scrape users’ data off our platform.”⁵²⁶

491. As part of the App Developer Investigation, defendants announced:⁵²⁷

[W]e are far from finished. . . . We’ve also improved the ways we investigate and enforce against potential privacy policy violations that we find. . . .

[W]e’ve made widespread improvements to how we evaluate and set policies for all developers that build on our platforms. We’ve removed a number of APIs, the channels that developers use to access various types of data. We’ve grown our teams dedicated to investigating and enforcing against bad actors. This will allow us to, on an annual basis, review every active app with access to more than basic user information. And

⁵²⁵ *Id.*

⁵²⁶ *Id.*

⁵²⁷ *Id.*

when we find violators, we'll take a range of enforcement actions.

* * *

And we will not allow apps on Facebook that request a disproportionate amount of information from users relative to the value they provide.

492. While defendants' announcement was light on specifics, the same day, a state court in Massachusetts unsealed documents in the Massachusetts Attorney General's investigation into Facebook's potential violation of state consumer protection laws. The unsealed documents showed that Facebook had suspended 69,000 apps—the majority of which Facebook flagged for failing to cooperate with the investigation, and about 10,000 of which had potentially misappropriated users' data.⁵²⁸

493. *The New York Times* described Facebook's announcement as “a tacit admission that the scale of its data privacy issues was far larger than it had previously acknowledged. . . . The disclosures about app suspensions renew questions about whether people's personal information on Facebook is secure, even after the company has been under fire for more than a year for its privacy practices.”⁵²⁹

⁵²⁸ Kate Conger, Gabriel J.X. Dance & Mike Issac, *Facebook's Suspension of 'Tens of Thousands' of Apps Reveals Wider Privacy Issues*, N.Y. Times (Sept. 20, 2019).

⁵²⁹ *Id.*

2. Defendants Revise Facebook’s Business Model to Respect Privacy and Reverse Their Prior Privacy Abuses

494. In response to the privacy misconduct at issue in this case, throughout 2019, defendants announced sweeping revisions to the Facebook platform that they intended would make Facebook more “privacy-focused.”

495. On March 6, 2019, defendant Zuckerberg announced specifically that Facebook’s “vision and principles” would support a newly “privacy-focused messaging and social networking platform.”⁵³⁰ In his statement on Facebook.com, Zuckerberg admitted that Facebook’s privacy practices had been too lax, stating: “I understand that many people don’t think Facebook can or would even want to build this kind of privacy-focused platform—because frankly we don’t currently have a strong reputation for building privacy protective services, and we’ve historically focused on tools for more open sharing.”⁵³¹ Zuckerberg committed to several principles around which Facebook “plann[ed] to rebuild more of our services,” including.⁵³²

- “People should have . . . clear control over who can communicate with them and confidence that no one else can access what they share.”
- “People’s private communications should be secure. End-to-end encryption prevents anyone—including us—from seeing what people share on our services.”

⁵³⁰ Mark Zuckerberg, *A Privacy-Focused Vision for Social Networking*, Facebook (Mar. 6, 2019).

⁵³¹ *Id.*

⁵³² *Id.*

- “People . . . should not have to worry about what they share coming back to hurt them later. So we won’t keep messages or stories around for longer than necessary to deliver the service or longer than people want them.”
- “People should expect that we will do everything we can to keep them safe on our services within the limits of what’s possible in an encrypted service.”
- “People should be able to use any of our apps to reach their friends, and they should be able to communicate across networks easily and securely.”
- “People should expect that we won’t store sensitive data in countries with weak records on human rights like privacy and freedom of expression in order to protect data from being improperly accessed.”

496. Defendant Zuckerberg broached these issues again on Facebook’s earnings call for the first quarter of 2019 on April 24, 2019. He opened the call by reiterating his “privacy-focused vision for the future of social networking,” and he described the changes that Facebook would be implementing to “build[] this privacy-focused platform.”⁵³³ In addition, defendant Sandberg explained, “We’re making significant investments in safety and security while continuing to grow our community and our business. This quarter once again shows that we can do both. ***As we prepare to build more services around our privacy roadmap, we’re changing the way we run the company. We are committed to earning back trust through the actions we take.*** A key part of earning back trust is increasing transparency.”⁵³⁴

⁵³³ Q1 2019 Facebook, Inc., Earnings Call Tr. at 2 (Apr. 24, 2019).

⁵³⁴ *Id.* at 5.

497. One week later, on April 30, 2019, Facebook held its annual F8 conference. In his keynote address on the first day of the conference, defendant Zuckerberg stated:⁵³⁵

Privacy gives us the freedom to be ourselves. . . . The future is private. This is the next chapter for our services. . . . Over time, I believe that a private social platform will be even more important in our lives than our digital town squares. So today, we're going to start talking about what this could look like as a product. . . . [H]ow we need to change how we run this company in order to build this. . . . I know that we don't exactly have the strongest reputation on privacy right now to put it lightly, but I'm committed to doing this well. . . .

498. At the F8 conference, defendants unveiled the privacy-focused redesign of Facebook's desktop website and mobile app. *The New York Times* described, "[T]he revisions add new features to promote group-based communications instead of News Feed, where people publicly post a cascade of messages and status updates. And it unveiled a spare, stark white look for Facebook, a departure from the site's largely blue-tinted design. . . . The redesign is the most tangible sign of how the privacy scandals and user-data issues that have roiled Facebook are forcing change at the company."⁵³⁶ In an interview with *The*

⁵³⁵ *Day 1 of F8 2019: Building New Products and Features for a Privacy-Focused Social Platform*, Facebook Newsroom (Apr. 30, 2019).

⁵³⁶ Mike Issac, *Facebook Unveils Redesign as It Tries to Move Past Privacy Scandals*, N.Y. Times (Apr. 30, 2019).

New York Times, Zuckerberg explained that the platform's new features "will end up creating a more trustworthy platform."⁵³⁷

VI. Materially False and Misleading Statements and Omissions Made with Scienter During the Class Period

499. During the Class Period, Facebook, Zuckerberg, Sandberg, and Wehner violated the federal securities laws by knowingly or recklessly making untrue statements of material fact or omitting to state material facts necessary to make the statements made, in the light of the circumstances under which they were made, not misleading.

A. Defendants Made Materially False and Misleading Statements Concerning Facebook Users' "Control" over Their Data

500. During the Class Period, defendants knowingly or recklessly made materially false and misleading statements concerning Facebook users' control over their data and information, including the statements set forth below.

501. From the start of the Class Period through May 25, 2018, inclusive, under the heading "SHARING YOUR CONTENT AND INFORMATION, in its *Statement of Rights and Responsibilities* published on the Company's corporate website, Facebook stated: "You own all of the content and information you post on Facebook, and ***you can control how it is shared through your privacy and application settings.***"⁵³⁸

⁵³⁷ *Id.*

⁵³⁸ Facebook's *Statement of Rights and Responsibilities* was published on Facebook's corporate website starting on January 30, 2015 and ending May 25, 2018 inclusive.

502. On October 12, 2017, during a public interview with Axios, Sandberg stated:⁵³⁹

[W]hen you share on Facebook you need to know ***No one is going to get your data that shouldn't have it.*** That we're not going to make money in ways that you would feel uncomfortable with off your data. And that ***you're controlling who you share with.*** . . . Privacy for us is making sure that you feel secure, sharing on Facebook.

503. On November 1, 2017, during Facebook's earnings call for the third quarter of 2017, Sandberg stated: ". . . the Facebook family of apps already applies the core principles in the [GDPR] framework because we built our services around transparency and control."⁵⁴⁰

504. On January 23, 2018, during an appearance at the Facebook Gather Conference in Brussels, Belgium, Sandberg stated: "Our apps have long been focused on giving people ***transparency and control***"⁵⁴¹

505. On January 31, 2018, during Facebook's earnings call for the fourth quarter of 2017, Sandberg stated: ". . . the Facebook family of apps ***already applies*** the core principles in the GDPR framework, which are ***transparency and control.***"⁵⁴²

506. On February 28, 2018, during an appearance at the Morgan Stanley Technology, Media & Telecom Conference, Wehner stated: "So we think with transparency

⁵³⁹ Mike Allen, *Exclusive interview with Facebook's Sheryl Sandberg*, Axios (Oct. 12, 2017).

⁵⁴⁰ Q3 2017 Facebook, Inc. Earnings Call Tr. at 11 (Nov. 1, 2017).

⁵⁴¹ Facebook Gather Conference, Brussels, Belgium (Jan. 23, 2018).

⁵⁴² Morgan Stanley Technology, Media & Telecom Conference Tr. at 9 (Feb. 28, 2018).

and **control**, we're set up well to be in a position where we're compliant with GDPR when the regulation goes into effect in May."⁵⁴³

507. On March 16, 2018, in a post on its corporate website titled *Suspending Cambridge Analytica and SCL Group From Facebook*, 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. This is just one of the many ways **we give people the tools to control their experience**. 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."⁵⁴⁴

508. On April 4, 2018, during a telephonic press conference with journalists and members of the press, Zuckerberg stated: "[T]he main principles are, **you have control over everything you put on the service**, and most of the content Facebook knows about you it [*sic*] because you chose to share that content with your friends and put it on your profile."⁵⁴⁵

509. On April 24, 2018, in a public post on Facebook.com, Facebook stated: "You've been hearing a lot about Facebook lately and how your data is being used. While this information can sometimes be confusing and technical, it's important to know that **you are in control**

⁵⁴³ Paul Grewal, *Suspending Cambridge Analytica and SCL Group From Facebook*, Facebook Newsroom (Mar. 16, 2018).

⁵⁴⁴ *Hard Questions: Q&A With Mark Zuckerberg on Protecting People's Information*, Facebook Newsroom (Apr. 4, 2018).

⁵⁴⁵ *How to Take Control of Your Facebook*, Facebook Newsroom (Apr. 24, 2018).

of your Facebook, what you see, what you share, *and what people see about you.*⁵⁴⁶

510. On June 29, 2018, in its *Responses to the U.S. House of Representatives Energy and Commerce Committee’s Questions for the Record*, Facebook stated: “We already show people what apps their accounts are connected to and *allow them to control what data they’ve permitted those apps to use.*”⁵⁴⁷

511. In the same document discussed immediately above, Facebook further stated:⁵⁴⁸

Privacy is at the core of everything we do, and our approach to privacy starts with *our commitment to transparency and control*. [. . .] Our approach to control is based on the belief that people should be able to choose who can see what they share and how their data shapes their experience on Facebook. *People can control the audience for their posts and the apps that can receive their data.*

512. On April 10, 2018, during his live oral testimony before the Joint Commerce and Judiciary Committees of the U.S. Senate, Zuckerberg made the following statements:⁵⁴⁹

(a) “This is the most important principle for Facebook: Every piece of content that you share on Facebook, you own and you have *complete control*

⁵⁴⁶ Q4 2017 Facebook, Inc. Earnings Call Tr. at 9 (Jan. 30, 2018).

⁵⁴⁷ Facebook, Responses to House Energy and Commerce, Questions for the Record addressed Chairman Walden (June 29, 2018) at 9.

⁵⁴⁸ *Id.* at 25.

⁵⁴⁹ *Transcript of Mark Zuckerberg’s Senate hearing*, Wash. Post (Apr. 10, 2018).

over who sees it and—and how you share it, and you can remove it at any time. That’s why every day, about 100 billion times a day, people come to one of our services and either post a photo or send a message to someone, because ***they know that they have that control and that who they say it’s going to go to is going to be who sees the content.*** And I think that that control is something that’s important that I think should apply to—to every service.”

(b) “That’s what the [Facebook] service is, right? It’s that you can connect with the people that you want, and you can share whatever content matters to you, whether that’s photos or links or posts, and ***you get control over it.***”

(c) “The two broad categories that I think about are content that a person is[sic] chosen to share and that they have complete control over, they get to control when they put into the service, when they take it down, who sees it. And then the other category are data that are connected to making the ads relevant. ***You have complete control over both.***”

(d) “Every person gets to ***control who gets to see their content.***”

(e) “But, Senator, the—your point about surveillance, I think that there’s a very important distinction to draw here, which is that when—when organizations do surveillance[,] people don’t have control over that. ***But on Facebook, everything that you share there[,] you have control over.***”

513. On April 11, 2018, during his live testimony before the U.S. House of Representatives’ Energy and Commerce Committee, Zuckerberg stated.⁵⁵⁰

(a) “[. . .] on Facebook, you have control over your information.”

(b) “[. . .] every single time that you share something on Facebook or one of our services, right there is a control in line, where you control who—who you want to share with.”

(c) “Congresswoman, giving people control of their information and how they want to set their privacy is foundational to the whole service [on Facebook]. It’s not just a—kind of an add-on feature, something we have to . . . comply with . . . ***all the data that you put in, all the content that you share on Facebook is yours. You control how it’s used.***”

514. On June 8, 2019, in its Responses to Additional Question from the Senate Commerce Committee, Facebook stated: “Privacy is at the core of everything we do, and our approach to privacy starts with our commitment to transparency and control. [. . .] Our approach to control is based on the belief that people should be able to choose who can see what they share and how their data shapes their experience on Facebook. People can control the audience for their posts and the apps that can receive their data.”⁵⁵¹

⁵⁵⁰ *Transcript of Zuckerberg’s appearance before House committee*, Wash. Post (Apr. 11, 2018).

⁵⁵¹ Facebook, Responses to U.S. Senate Committee on the Judiciary, Questions for the Record addressed Chairman Grassley (June 8, 2018) at 4.

515. The statements concerning user control set forth in ¶¶501-514, *supra*, were materially false and misleading because, when they were made, Facebook users could not control their data, including because:

(a) Defendants publicly stated in April 2014 that Facebook would stop providing third parties with access to user friends' data, but continued to secretly provide that data to numerous third parties, including app developers, "whitelisted" third parties, mobile device makers and others;

(b) Defendants were overriding user privacy settings to provide user friends' data to third parties;

(c) Defendants knew that bad actors were able to access data; and

(d) Defendants knew that users could not control their data that Facebook had given to third parties without user knowledge or consent.

516. In addition, the FTC has confirmed that Facebook made materially false and misleading statements concerning Facebook users' control over their data by charging that Facebook's conduct, including during the Class Period, violated Parts I.B and I.C of the FTC Consent Decree because Facebook misrepresented the extent to which users could "control the privacy" of their data and the extent to which Facebook "makes or has made [user data] accessible to third parties," respectively. In charging Facebook, the FTC relied on the fact that, *inter alia*, "regardless of the privacy settings a user checked, Facebook continued to provide access to [user data] to

Whitelisted Developers” from at least the start of the Class Period through to at least June 2018.⁵⁵²

517. Facebook paid \$5 billion to settle the FTC’s charges and stipulated that it “agrees that the ***facts alleged in the [FTC] Complaint will be taken as true . . .*** in any subsequent civil litigation by [the FTC] to enforce its rights . . .” to the \$5 billion penalty that Facebook was required to pay.⁵⁵³ Zuckerberg personally signed this stipulation on July 23, 2019.

518. The statements concerning user control set forth in ¶¶501-514, *supra*, were also materially false and misleading because they omitted to state material facts necessary to make them, in the light of the circumstances under which they were made, not misleading, including that:

(a) Users did not have control over their data on Facebook;

(b) Contrary to their public statements in April 2014 that Facebook would stop providing third parties with access to user friends’ data, defendants continued to secretly provide that data to numerous third parties, including app developers, “whitelisted” third parties, mobile device makers and others;

(c) Defendants were overriding user privacy settings to provide user friends’ data to third parties;

(d) Bad actors were able to access data on Facebook; and

⁵⁵² FTC Complaint at ¶174.

⁵⁵³ Stipulated Order at 3, ¶I.E.

(e) Users could not control their data that Facebook had given to third parties without user knowledge or consent.

B. Defendants Made Materially False and Misleading Statements About Respecting Users' Privacy Settings

519. On March 17, 2018, Facebook made the following statement and provided the following information to a reporter for the *The Washington Post*, with the knowledge and expectation that it would be communicated to the public, as it was on that date, “***We respected the privacy settings that people had in place.*** Privacy and data protections are fundamental to every decision we make.”⁵⁵⁴

520. The statement set forth in ¶519, *supra*, was materially false and misleading because, when it was made, Facebook did not respect the privacy settings that people had in place, including because:

(a) Defendants publicly stated in April 2014 that Facebook would stop providing third parties with access to user friends' data, but continued to secretly provide that data to numerous third parties, including app developers, “whitelisted” third parties, mobile device makers and others;

(b) Defendants were overriding user privacy settings to provide user friends' data to third parties; and

(c) Defendants knew that bad actors were able to access data.

⁵⁵⁴ Craig Timberg & Tony Romm, *Facebook May Have Violated FTC Privacy Deal, Say Former Federal Officials, Triggering Risk Of Massive Fines*, Wash. Post (Mar. 18, 2018).

521. In addition, the FTC has confirmed that this statement was materially false and misleading because, in charging Facebook with violations of the FTC Consent Decree, the FTC relied on the fact that, *inter alia*, “regardless of the privacy settings a user checked, Facebook continued to provide access to [user data] to Whitelisted Developers” from at least the start of the Class Period through to at least June 2018.⁵⁵⁵

522. Defendant Facebook paid \$5 billion to settle the FTC’s charges and stipulated that it “agrees that the ***facts alleged in the [FTC] Complaint will be taken as true . . .*** in any subsequent civil litigation by [the FTC] to enforce its rights . . .” to the \$5 billion penalty that Facebook was required to pay.⁵⁵⁶ Zuckerberg personally signed this stipulation on July 23, 2019.

523. The statement set forth in ¶519, *supra*, was also materially false and misleading because its omitted to state material facts necessary to make it, in the light of the circumstances under which it was made, not misleading, including that:

- (a) Defendants did not respect the privacy settings that people had in place;
- (b) Defendants were overriding user privacy settings to provide user friends’ data to third parties;
- (c) Contrary to their public statements in April 2014 that Facebook would stop providing third parties with access to user friends’ data, defendants continued

⁵⁵⁵ FTC Complaint at ¶174.

⁵⁵⁶ Stipulated Order at 3, ¶I.E.

to secretly provide that data to numerous third parties, including app developers, “whitelisted” third parties, mobile device makers and others; and

(d) Bad actors were able to access data on Facebook.

C. Defendants Made Materially False and Misleading Statements Concerning Risks to Facebook’s Business

524. During the Class Period, defendants knowingly or recklessly made materially false and misleading statements concerning the business risks facing Facebook, including the statements set forth below.

525. On February 3, 2017, Facebook filed its annual report on Form 10-K for the fiscal year ended December 31, 2016 with the SEC (the “2016 Form 10-K”), which was signed by Zuckerberg, Sandberg and Wehner, among others, and made available on Facebook’s investor relations website. Facebook’s 2016 Form 10-K included the following statements concerning risks facing the Company:

(a) “Security breaches and improper access to or disclosure of our data or user data, or other hacking and phishing attacks on our systems, **could** harm our reputation and adversely affect our business”;

(b) “Any failure to prevent or mitigate security breaches and improper access to or disclosure of our data or user data **could** result in the loss or misuse of such data, which could harm our business and reputation and diminish our competitive position”;

(c) “We provide limited information to . . . third parties based on the scope of services provided to us. However, **if** these third parties or developers fail to

adopt or adhere to adequate data security practices . . . our data or our users' data *may be* improperly accessed, used, or disclosed.”⁵⁵⁷

526. The statements quoted in ¶525, *supra*, were repeated or incorporated by reference into Facebook's other reports on Forms 10-K and 10-Q that the Company filed with the SEC during the Class Period, including its quarterly reports filed on May 4, 2017 (the “1Q17 10-Q”), July 27, 2017 (the “2Q17 10-Q”), November 2, 2017 (the “3Q17 10-Q”), and its annual report filed on February 1, 2018 (the “2017 Form 10-K”), each of which was signed by Zuckerberg, Sandberg and Wehner, among others, and made available on Facebook's investor relations website.

527. The risk factor statements set forth in ¶¶525-526, *supra*, were materially false and misleading because, when they were made because:

(a) Defendants did not disclose, but knew or recklessly disregarded, the fact that Kogan had violated the Company's policies by improperly transferring data relating to tens of millions of Facebook users to Cambridge Analytica;

(b) Defendants misleadingly presented the potential for improper access to or disclosure of user data as merely a hypothetical investment risk;

(c) Defendants misleadingly presented the potential for misuse of user data as merely a hypothetical investment risk;

⁵⁵⁷ FY 2016 Facebook, Inc. Form 10-K at 12-13 (Feb. 3, 2017).

(d) Defendants created the false impression that Facebook had not suffered a significant episode of improper access to or disclosure of user data by a developer;

(e) Defendants created the false impression that Facebook had not suffered a significant episode of misuse of user data by a developer;

(f) Defendants publicly stated in April 2014 that Facebook would stop providing third parties with access to user friends' data, but continued to improperly provide access to that data to numerous third parties, including app developers, "whitelisted" third parties, mobile device makers and others, throughout the Class Period;

(g) Defendants were overriding user privacy settings to provide third parties with improper access to user friends' data throughout the Class Period;

(h) Defendants knew that bad actors were able to access data;

(i) Defendants knew that bad actors Cambridge Analytica and its affiliates had accessed the data;

(j) Defendants knew that Cambridge Analytica continued to make use of improperly accessed data on Facebook's platform, including in high profile elections; and

(k) Defendants knew that bad actors, including Cambridge Analytica, had provided false, mutually contradictory, and self-serving assurances and certifications, including falsely assuring Facebook that those bad actors had never received improperly obtained data, had never paid for such data, had never used such data, and had destroyed such data.

528. In addition, the SEC has confirmed that the statements set forth in ¶¶525-526, *supra*, were materially misleading because it charged, *inter alia*, that:

(a) “In its quarterly and annual reports filed between January 28, 2016 and March 16, 2018 [*i.e.*, including those set forth above], Facebook did not disclose that a researcher [*i.e.*, Kogan] had, in violation of the company’s policies, transferred data relating to approximately 30 million Facebook users to Cambridge Analytica. Instead, Facebook misleadingly presented the potential for misuse of user data as merely a hypothetical risk”;⁵⁵⁸

(b) “Facebook’s Risk Factor disclosures [including those set forth above] misleadingly suggested that the company faced merely the risk of [user data] misuse and any harm to its business that might flow from such an incident;”⁵⁵⁹ and

(c) “Facebook knew, or should have known, that its Risk Factor disclosures in its annual reports on Form 10-K for the fiscal years ended . . . December 31, 2016 and December 31, 2017, and in its quarterly reports on Form 10-Q filed in . . . 2017 . . . were materially misleading.”⁵⁶⁰

529. The risk factor statements set forth in ¶¶525-526, *supra*, were also materially false and misleading because they omitted to state material facts necessary to make them, in the light of the circumstances under which they were made, not misleading, including that:

⁵⁵⁸ SEC Complaint at ¶6.

⁵⁵⁹ *Id.* at ¶39.

⁵⁶⁰ *Id.* at ¶44.

(a) Kogan had violated the Company's policies by improperly transferring data relating to tens of millions of Facebook users to Cambridge Analytica;

(b) Facebook had in fact suffered a significant episode of improper access to or disclosure of user data caused by a developer;

(c) Facebook had in fact suffered a significant episode of misuse of user data caused by a developer;

(d) Defendants publicly stated in April 2014 that Facebook would stop providing third parties with access to user friends' data, but continued to secretly provide that data to numerous third parties, including app developers, "whitelisted" third parties, mobile device makers and others, throughout the Class Period;

(e) Defendants were overriding user privacy settings to provide user friends' data to third parties throughout the Class Period;

(f) Defendants knew that bad actors were able to access data;

(g) Defendants knew that bad actors Cambridge Analytica and its affiliates had accessed the data;

(h) Defendants knew that Cambridge Analytica continued to make use of improperly accessed data on Facebook's platform, including in high profile elections; and

(i) Defendants knew that bad actors, including Cambridge Analytica, had provided false, mutually contradictory, and self-serving assurances and certifications, including falsely assuring Facebook that those bad actors had received improperly obtained data, had never paid for such data, had never used such data, and had destroyed such data.

530. Facebook’s 2016 Form 10-K also stated “Although *we have developed systems and processes that are designed to protect our data and user data, to prevent data loss and to prevent or detect security breaches*, we cannot assure you that such measures will provide absolute security.”⁵⁶¹ This statement was repeated or incorporated by reference into the other reports on Forms 10-K and 10-Q that Facebook filed with the SEC during the Class Period, including the 1Q17 10-Q, 2Q17 10-Q, 3Q17 10-Q, and the 2017 Form 10-K.

531. These statements were false and misleading for the reasons cited above, including that they:

- (a) Misleadingly presented the potential for improper access to or disclosure of user data as merely a hypothetical investment risk;
- (b) Defendants did not employ the “systems and processes” purportedly developed to protect user data;
- (c) Created the false impression that Facebook had not suffered a significant episode of improper disclosure and misuse of user data.

532. The statement set forth in ¶530, *supra*, was also materially false and misleading because it omitted to state material facts necessary to make it, in the light of the circumstances under which it was made, not misleading, including that:

- (a) Kogan had violated the Company’s policies by improperly transferring data relating to tens of millions of Facebook users to Cambridge Analytica;

⁵⁶¹ FY 2016 Facebook, Inc. Form 10-K at 13 (Feb. 3, 2017).

(b) Facebook had in fact suffered a significant episode of improper access to or disclosure of user data caused by a developer; and

(c) Facebook had in fact suffered a significant episode of misuse of user data caused by a developer.

533. In addition, the 2016 Form 10-K also included the following statements concerning the risks to the Company from a loss of user trust in Facebook's ability to protect their privacy, as could occur following public reports or investigations into breaches of those privacy policies, or the Company's past failures to address known breaches of those policies:

If we fail to retain existing users or add new users, or if our users decrease their level of engagement with our products, our revenue, financial results, and business may be significantly harmed.

The size of our user base and our users' level of engagement are critical to our success. Our financial performance has been and will continue to be significantly determined by our success in adding, retaining, and engaging active users of our products, particularly for Facebook and Instagram. We anticipate that our active user growth rate will continue to decline over time as the size of our active user base increases, and as we achieve higher market penetration rates. ***If people do not perceive our products to be useful, reliable, and trustworthy, we may not be able to attract or retain users or otherwise maintain or increase the frequency and duration of their engagement. . . .***

Any number of factors could potentially negatively affect user retention, growth, and engagement, including if:

there are decreases in user sentiment about the quality or usefulness of our products or ***concerns related to privacy and sharing, safety, security***, or other factors.⁵⁶²

These statements were repeated or incorporated by reference into the other reports on Forms 10-K and 10-Q that Facebook filed with the SEC during the Class Period, including the 1Q17 10-Q, 2Q17 10-Q, 3Q17 10-Q, and the 2017 Form 10-K.

534. These statements were false and misleading for the reasons cited above, including that they:

(a) Misleadingly presented the risks to Facebook's business and reputation arising from "concerns related to privacy and sharing, safety [and] security" as merely hypothetical investment risks; and

(b) Created the false impression that Facebook had not suffered a significant episode of improper disclosure and misuse of user data.

535. The statements set forth in ¶533, *supra*, were also materially false and misleading because they omitted to state material facts necessary to make them, in the light of the circumstances under which they were made, not misleading, including that:

(a) Kogan had violated the Company's policies by improperly transferring data relating to tens of millions of Facebook users to Cambridge Analytica;

(b) Facebook had in fact suffered a significant episode of improper access to or disclosure of user data caused by a developer; and

⁵⁶² FY 2016 Facebook, Inc. Form 10-K at 13 (Feb. 3, 2017).

(c) Facebook had in fact suffered a significant episode of misuse of user data caused by a developer.

D. Defendants Made Materially False and Misleading Statements Concerning the Results Of Facebook’s Investigation into Cambridge Analytica’s Data Misuse

536. During the Class Period, defendants knowingly or recklessly made materially false and misleading statements concerning the results of Facebook’s investigation into Cambridge Analytica’s data misuse.

537. On March 4, 2017, Facebook made the following statement through an authorized spokesperson to reporters from *The Guardian* with the knowledge and expectation that it would be communicated to the public, as it was on that date in an article titled: “Watchdog to launch inquiry into misuse of data in politics,” “[o]ur investigation to date has not uncovered anything that suggests wrongdoing with respect to Cambridge Analytica’s work on the [Brexit] and Trump campaigns.”⁵⁶³

538. On March 30, 2017, Facebook made the following statement through an authorized spokesperson to a reporter from *The Intercept* with the knowledge and expectation that it would be communicated to the public, as it was on that date in an article titled: “Facebook Failed To Protect 30 Million Users From Having Their Data Har-

⁵⁶³ Jamie Doward, Carole Cadwalladr & Alice Gibbs, *Watchdog to launch inquiry into misuse of data in politics*, *Guardian* (Mar. 4, 2017).

vested By A Trump Campaign Affiliate,” “[o]ur investigation to date has not uncovered anything that suggests wrongdoing” with respect to Cambridge Analytica.⁵⁶⁴

539. The statements set forth in ¶¶537-538, *supra*, were materially false and misleading because, when they were made because:

(a) Facebook did not disclose, but knew or recklessly disregarded, the fact that Facebook had determined by no later than December 2015 that Kogan had violated the Company’s policies by improperly transferring data relating to tens of millions of Facebook users to Cambridge Analytica;

(b) Facebook’s investigation into the Cambridge Analytica matter had found evidence of wrongdoing because Facebook had determined that Kogan violated Facebook’s policies such as the prohibition on transferring or selling Facebook user data to other parties when he sold the data of tens of millions of Facebook users to Cambridge Analytica;

(c) Facebook’s investigation into the Cambridge Analytica matter had found evidence of wrongdoing because Facebook had determined that Cambridge Analytica violated Facebook’s policies, such as the prohibition on transferring or selling Facebook user data to other parties, when Cambridge Analytica, through SCL, bought the data of tens of millions of Facebook users from GSR; and

⁵⁶⁴ Mattathias Schwartz, *Facebook Failed To Protect 30 Million Users From Having Their Data Harvested By A Trump Campaign Affiliate*, Intercept (March 30, 2017).

(d) Facebook’s investigation into the Cambridge Analytica matter and direct work with Cambridge Analytica as a Facebook advertiser during the U.S. elections revealed evidence of wrongdoing because Facebook had determined that Cambridge Analytica continued to violate Facebook’s policies by utilizing improperly obtained user data to target Facebook users for disinformation and voter suppression advertisements on Facebook.

540. In addition, the SEC has confirmed that the statements set forth in ¶¶537-538, *supra*, were materially misleading because it charged, *inter alia*, that:

(a) “[W]hen asked by reporters in 2017 about its investigation into the Cambridge Analytica matter, Facebook falsely claimed the company found no evidence of wrongdoing;⁵⁶⁵ and

(b) “[I]n March 2017, Facebook’s communications group provided the following quote to reporters: ‘Our investigation to date has not uncovered anything that suggests wrongdoing.’ This was misleading because Facebook had, in fact, determined that [Kogan’s] transfer of user data to Cambridge violated the company’s Platform Policy.”⁵⁶⁶

541. The statements set forth in ¶¶537-538, *supra*, were also materially false and misleading because they omitted to state material facts necessary to make them, in the light of the circumstances under which they were made, not misleading, including that:

⁵⁶⁵ SEC Complaint at ¶6.

⁵⁶⁶ *Id.* at ¶49.

(a) Facebook had determined by no later than December 2015 that Kogan had violated the Company's policies by improperly transferring data relating to tens of millions of Facebook users to Cambridge Analytica; and

(b) Facebook's investigation into the Cambridge Analytica matter had found evidence of wrongdoing.

E. Defendants Made Materially False and Misleading Statements Concerning Facebook's Response to Instances of Data Misuse

542. During the Class Period, defendants recklessly made materially false and misleading statements concerning Facebook's response to instances of data misuse.

543. On or about February 16, 2017, Facebook made the following statement and provided the following information to *BuzzFeed News*, with the knowledge and expectation that it would be communicated to the public, as it was on that date in an article titled *The Truth About The Trump Data Team That People Are Freaking Out About*: “[A]s a general rule, Andy Stone, a Facebook spokesperson, said, ‘**Misleading people or misusing their information is a direct violation of our policies and we will take swift action against companies that do, including banning those companies from Facebook and requiring them to destroy all improperly collected data.**’”⁵⁶⁷

544. On or about June 8, 2017, Facebook made the following statement and provided the following information to Newsweek, with the knowledge and expectation that it would be communicated to the public, as it was on that date in an article titled *How Big Data Mines Personal*

⁵⁶⁷ Kendall Taggart, *The Truth About the Trump Data Team That People are Freaking Out About*, BuzzFeed (Feb. 16, 2017).

*Info to Craft Fake News and Manipulate Voters: “Misleading people or misusing their information is a direct violation of our policies and we will take swift action against companies that do, including banning those companies from Facebook and requiring them to destroy all improperly collected data.”*⁵⁶⁸

545. Throughout the Class Period, under the heading “PROTECT DATA,” Facebook’s Data Policy published on the Company’s corporate website stated the following concerning Facebook’s response to instances of policy violations: “Enforcement is both automated and manual, and can include disabling your app, restricting you and your app’s access to platform functionality, **requiring that you delete data**, terminating our agreements with you or any other action that we deem appropriate.”⁵⁶⁹

546. The statements about taking “swift action against companies that [misuse people’s information]” in ¶¶543-545, *supra*, were materially misleading because, among other things, Facebook did not take “swift action” when it learned that Kogan had improperly sold user data to Cambridge Analytica. Instead, after learning that both Kogan and Cambridge Analytica had lied about the nature of the data transferred to Cambridge Analytica and about all the data being deleted, Facebook waited nearly one year (from June 2016 to April 2017) for a certification from SCL, which did not mention Cambridge Analytica, reporting deletion of the purloined data.

547. The statements about Facebook “requiring [data misusers] to destroy all improperly collected data” or “requiring that [policy violators] delete data” in ¶¶543-545,

⁵⁶⁸ Nina Burleigh, *How Big Data Mines Personal Info to Craft Fake News and Manipulate Voters*, Newsweek (June 8, 2017).

⁵⁶⁹ Facebook Platform Policies (Jan. 11, 2017).

supra, were materially misleading because Facebook could not “require” data misusers to “destroy” or “delete” improperly collected data. Facebook simply did not have the technical ability to “automat[ically]” “require” deletion of misused user data. Defendants knew that once user data was in the hands of a third party—Facebook had no ability to control that data or “require” that third party to do anything.

548. For example, even though Facebook *knew* that both Kogan and Cambridge Analytica had lied about the nature of the data transferred to Cambridge Analytica and about whether all of the data had been deleted, Facebook could do nothing to “require” deletion of the data. As such, Facebook knowingly or recklessly relied on unsupported certifications from known liars stating that the data had been deleted. Further, even when confronted with red flags that Cambridge Analytica was still using the purloined data, Facebook had no ability to “require” destruction or deletion of the data.

549. To be sure, as discussed above, Zuckerberg has admitted that Facebook’s failure to follow-up on the Cambridge Analytica data misuse and require the data to be deleted was the “biggest mistake[]” Facebook ever made.⁵⁷⁰ Zuckerberg also admitted that Facebook “should have been doing more all along” to protect users’ privacy. Sandberg also admitted that it was a “mistake that [Facebook] did not verify” whether Cambridge Analytica had deleted the user data⁵⁷¹ and acknowledged that

⁵⁷⁰ Nicholas Thompson, *Mark Zuckerberg Talks to Wired About Facebook’s Privacy Problem*, *Wired* (Mar. 21, 2018).

⁵⁷¹ *CNBC Exclusive: CNBC Transcript: Sheryl Sandberg Sits Down with CNBC’s Julia Boorstin Today*, *CNBC* (Mar. 22, 2018).

the Company should have “checked”⁵⁷² and “follow[ed]-up”⁵⁷³ to ensure Facebook user’s personal data was, in fact, protected. She stated that Facebook was “not focused enough on the possible misuses of data” and “protecting people’s data” at the time.⁵⁷⁴ Sandberg has also admitted that Facebook “could have done . . . two and a half years ago” what it is doing today.⁵⁷⁵

550. The statements set forth in ¶¶543-545, *supra*, were also materially false and misleading because they omitted to state material facts necessary to make them, in the light of the circumstances under which they were made, not misleading, including that:

(a) Facebook did not take swift action against third parties who had misused user information; and

(b) Facebook could not and did not (especially under its selective enforcement for non-competing advertisers policy) “require” data misusers to “destroy” or “delete” improperly collected data.

551. On March 16, 2018, defendants posted a statement on Facebook.com entitled “Suspending Cambridge Analytica and SCL Group From Facebook,” which stated:

We are committed to vigorously enforcing our policies to protect people’s information. We will take

⁵⁷² Eun Kyung Kim, *Sheryl Sandberg on TODAY: Other Facebook data breaches ‘possible’*, Today (Apr. 6, 2018).

⁵⁷³ Steve Inskeep, *Full Transcript: Facebook COO Sheryl Sandberg On Protecting User Data*, NPR (Apr. 5, 2018).

⁵⁷⁴ Judy Woodruff, *Sheryl Sandberg: Facebook ‘made big mistakes’ on protecting user data*, PBS (Apr. 5, 2018).

⁵⁷⁵ Eun Kyung Kim, *Sheryl Sandberg on TODAY: Other Facebook data breaches ‘possible’*, Today (Apr. 6, 2018).

whatever steps are required to see that this happens. We will take legal action if necessary to hold them responsible and accountable for any unlawful behavior.

* * *

On an ongoing basis, ***we also do a variety of manual and automated checks to ensure compliance with our policies and a positive experience for users.*** These include steps such as random audits of existing apps along with the regular and proactive monitoring of the fastest growing apps.

We enforce our policies in a variety of ways—from working with developers to fix the problem, to suspending developers from our platform, to pursuing litigation.⁵⁷⁶

552. The statement about Facebook being “committed to vigorously enforcing our policies to protect people’s information” and take “whatever steps are required to see that this happens” in ¶551, *supra*, was materially misleading because, among other things, Facebook did not “vigorously enforce [its] policies” and nor did it “take whatever steps are required” to do so when it learned that Kogan had improperly sold user data to Cambridge Analytica. Instead, after learning that both Kogan and Cambridge Analytica had lied about the nature of the data transferred to Cambridge Analytica and about all the data being deleted, Facebook waited nearly one year (from June 2016 to April 2017) for a certification from SCL, which did not mention Cambridge Analytica, reporting deletion of the purloined data.

⁵⁷⁶ Paul Grewal, *Suspending Cambridge Analytica and SCL Group From Facebook*, Facebook Newsroom (Mar. 16, 2018).

553. Further, defendants did not require or confirm that the data had in fact been destroyed by Cambridge Analytica. Defendants knew that once user data was in the hands of a third party—Facebook had no ability to control that data or “require” that third party to do anything. As such, Facebook knowingly or recklessly relied on unsupported certifications from known liars stating that the data had been deleted. Further, even when confronted with red flags that Cambridge Analytica was still using the purloined data, Facebook had no ability to “require” destruction or deletion of the data.

554. The statement set forth in ¶551, *supra*, was also materially false and misleading because it omitted to state material facts necessary to make them, in the light of the circumstances under which it was made, not misleading, including that:

(a) Defendants did not “vigorously enforce [Facebook’s] policies” and nor did they “take whatever steps are required” against third parties who had misused user information; and

(b) Defendants did not require or confirm that the data sold to Cambridge Analytica had in fact been destroyed—even after Cambridge Analytica had been exposed as a liar and Facebook was confronted with multiple red flags that the data was not deleted.

F. Defendants Made Materially False and Misleading Statements Concerning Facebook Users Consenting to, or Knowingly, Providing Their Information to Kogan

555. On March 17, 2018, Facebook provided an addendum to Facebook’s March 16, 2018 statement posted on its corporate website (*see* ¶507, *supra*), which stated:

The claim that this is a data breach is completely false. Aleksandr Kogan requested and gained access to information from ***users who chose to sign up to his app, and everyone involved gave their consent. People knowingly provided their information,*** no systems were infiltrated, and no passwords or sensitive pieces of information were stolen or hacked.⁵⁷⁷

556. The above statement concerning user choice, consent and knowledge was materially false and misleading because, when it was made, defendants knew that Kogan was one of the app developers who was secretly grandfathered into the “user friends’ data” sharing program that defendants had told the public was discontinued in April 2014. Thus, over 87 million Facebook users who had their personal data harvested by Kogan due to defendants decision to continue to secretly give Kogan access to user friend data did **not** “cho[o]se to sign up to his app”—indeed, they did not even sign up at all. Nor did these users “g[i]ve their consent” or “knowingly provide[] their information” to Kogan.

557. The statement set forth in ¶555, *supra*, was also materially false and misleading because it omitted to state material facts necessary to make it, in the light of the circumstances under which it was made, not misleading, including that:

- (a) Kogan was one of the app developers who was secretly grandfathered into the “user friends’ data” sharing program that defendants had told the public was discontinued in April 2014; and

⁵⁷⁷ Paul Grewal, *Suspending Cambridge Analytica and SCL Group from Facebook*, Facebook Newsroom (Mar. 16, 2018).

(b) Over 86 million Facebook users who had their personal data harvested by Kogan did *not* “cho[o]se to sign up to his app,” did *not* “g[i]ve their consent” and did *not* “knowingly provide[] their information” to Kogan.

558. On March 21, 2018, Zuckerberg posted an update to his personal Facebook.com page, which Facebook uses to disseminate public information regarding the Company,⁵⁷⁸ in which he stated in part:

The good news is that the most important actions to prevent this from happening again today we have already taken years ago. . . . In 2014, to prevent abusive apps, we announced that we were *changing the entire platform to dramatically limit the data apps could access. . . .* In this case, we already took the most important steps a few years ago in 2014 to prevent bad actors from accessing people’s information in this way.⁵⁷⁹

559. The above statement was materially false and misleading when it was made because Zuckerberg knew that, after the purported 2014 changes, Facebook continued to secretly provide that user friend data to numerous third parties, including app developers, “whitelisted” third parties, mobile device makers and others. Zuckerberg also knew that Facebook was overriding user privacy settings to provide user friends’ data to third parties.

⁵⁷⁸ Facebook stated in all its Class Period press releases announcing earnings results and guidance, “Facebook uses the investor.fb.com and newsroom.fb.com websites as well as Mark Zuckerberg’s Facebook Page (facebook.com/zuck) as means of disclosing material non-public information and for complying with its disclosure obligations under Regulation FD.”

⁵⁷⁹ Mark Zuckerberg, Facebook (Mar. 21, 2018).

560. In addition, the FTC has confirmed that “Facebook continued to allow millions of third-party developers access to [user friends’ data] for at least one year.”⁵⁸⁰ The FTC Complaint notes that “Facebook did not disclose this fact to its users”—thereby depriving users of knowledge and the ability to consent to the disclosure of their data.⁵⁸¹ This conduct violated Parts I.B and I.C of the FTC Consent Decree, which prohibited Facebook from misrepresenting “the extent to which a consumer can control the privacy of [their personal information]” and “the extent to which [Facebook] makes or has made covered information accessible to third parties.”⁵⁸²

561. Facebook paid \$5 billion to settle the FTC’s charges and stipulated that it “agrees that the *facts alleged in the [FTC] Complaint will be taken as true . . .* in any subsequent civil litigation by [the FTC] to enforce its rights . . .” to the \$5 billion penalty that Facebook was required to pay.⁵⁸³ Zuckerberg personally signed this stipulation on July 23, 2019.

562. The statement set forth in ¶558, *supra*, was also materially false and misleading because it omitted to state material facts necessary to make it, in the light of the circumstances under which it was made, not misleading, including that, after Facebook announced in April 2014 that

⁵⁸⁰ FTC Complaint at ¶164.

⁵⁸¹ *Id.* at ¶100. To the contrary, in September 2015, Facebook launched a “Privacy Checkup” tool as a means to help users “be in control” of their data and included a list of apps that users had installed. But this tool failed to list the apps that had access to user data based on their friends’ consent and did not disclose that Facebook was continuing to share that data with “millions of third-party developers.” *Id.* at ¶¶101-105.

⁵⁸² *Id.*, Count I at ¶¶160-165.

⁵⁸³ Stipulated Order at 3, ¶I.E.

access to “user friends’ data” was discontinued, Facebook continued to secretly provide that user friend data to numerous third parties, including app developers, “white-listed” third parties, mobile device makers and others. Indeed, Facebook was even overriding users’ privacy settings in order to provide user friend data to these white-listed third parties.

G. Defendants Made Materially False and Misleading Statements Concerning Facebook’s Compliance with the 2012 FTC Consent Decree

563. Throughout the Class Period, defendants recklessly made materially false and misleading statements concerning Facebook’s compliance with the FTC Consent Decree.

564. On February 2, 2017, Facebook filed its FY16 Form 10-K, which was signed by Zuckerberg, Sandberg and Wehner, among others, and made available on Facebook’s investor relations website. Facebook’s FY16 Form 10-K stated: “Violation of existing or future regulatory orders or *consent decrees* could subject us to substantial monetary fines and other penalties that could negatively affect our financial condition and results of operations.”⁵⁸⁴

565. Substantially similar statements were included in the MD&A sections of Facebook’s May 4, 2017 (1Q17), July 27, 2017 (2Q17) and November 2, 2017 (3Q17), reports on Form 10-Q and its February 1, 2018 (FY17 10-K) report on Form 10-K.

566. On July 26, 2017, in Facebook’s earnings call for the second quarter of 2017, Sandberg stated: “[W]e *respect local laws and regulations* Certainly, regulation is always an area of focus that we work hard to make

⁵⁸⁴ FY 2016 Facebook, Inc. Form 10-K at 7 (Feb. 3, 2017).

sure that we are explaining our business clearly and making sure regulators know the steps we take to protect privacy as well *as making sure that we're in compliance*.”⁵⁸⁵

567. On March 17, 2018, Facebook made the following statement and provided the following information to a reporter for *The Washington Post*, with the knowledge and expectation that it would be communicated to the public, as it was on that date, “*We reject any suggestion of violation of the consent decree*.”⁵⁸⁶

568. On April 4, 2018, in a telephonic press conference with journalists and members of the press, Zuckerberg stated: “You asked about the *FTC consent order*. *We've worked hard to make sure that we comply with it*.”⁵⁸⁷

569. On April 5, 2018, in an interview on National Public Radio, Sandberg stated: “We're in constant conversation with the FTC, and *that consent decree was important*, and *we've taken every step we know how to make sure we're in accordance with it*.”⁵⁸⁸

570. On April 10, 2018, in his live testimony before the Joint Commerce and Judiciary Committees of the U.S. Senate, Zuckerberg stated: “Our view is that—is that we

⁵⁸⁵ Q2 2017 Facebook, Inc. Earnings Call Tr. at 17 (July 26, 2017).

⁵⁸⁶ Craig Timberg & Tony Romm, *Facebook May Have Violated FTC Privacy Deal, Say Former Federal Officials, Triggering Risk Of Massive Fines*, Wash. Post (Mar. 18, 2018).

⁵⁸⁷ *Hard Questions: Q&A With Mark Zuckerberg on Protecting People's Information*, Facebook Newsroom (Apr. 4, 2018).

⁵⁸⁸ Steve Inskeep, *Full Transcript: Facebook COO Sheryl Sandberg On Protecting User Data*, NPR (Apr. 5, 2018).

believe that *we are in compliance with the consent order*, but I think we have a broader responsibility to protect people’s privacy even beyond that.”⁵⁸⁹

571. Defendants’ statements in ¶¶564-570, *supra*, were materially false and misleading when made because they denied violations of the FTC Consent Decree—or presented such violations as hypothetical risks—when defendants knew or recklessly disregarded the fact that Facebook was violating Parts I.B and I.C of the FTC Consent Decree, including by:

- (a) Publicly stating in April 2014 that Facebook would stop providing third parties with access to user friends’ data, when they continued to secretly provide that data to numerous third parties, including app developers, “whitelisted” third parties, mobile device makers and others;
- (b) Overriding user privacy settings to provide user friends’ data to third parties; and
- (c) Knowingly allowing bad actors to access data.

572. Indeed, the FTC has confirmed that Facebook knowingly violated Parts I.B and I.C of the FTC Consent Decree, including because:⁵⁹⁰

At least tens of millions of American users relied on Facebook’s deceptive privacy settings and statements to restrict the sharing of their information to their Facebook Friends, when, in fact, third-party developers could access and collect their data through their Friends’ use of third-party developers’ apps.

⁵⁸⁹ *Transcript of Mark Zuckerberg’s Senate hearing*, Wash. Post (Apr. 10, 2018).

⁵⁹⁰ FTC Complaint at ¶9.

Facebook knew or should have known that its conduct violated the 2012 [Consent] Order because it was *engaging in the very same conduct that the [FTC] alleged was deceptive* in Count one of the original Complaint that led to the 2012 [Consent] Order.

573. In addition, the FTC has confirmed that Facebook made materially false and misleading statements concerning Facebook users' control over their data by charging that Facebook's conduct, including during the Class Period, violated Parts I.B and I.C of the FTC Consent Decree because Facebook misrepresented the extent to which users could "control the privacy" of their data and the extent to which Facebook "makes or has made [user data] accessible to third parties," respectively. In charging Facebook, the FTC relied on the fact that, *inter alia*, "regardless of the privacy settings a user checked, Facebook continued to provide access to [user data] to Whitelisted Developers" from at least the start of the Class Period through to at least June 2018.⁵⁹¹

574. Facebook paid \$5 billion to settle the FTC's charges and stipulated that it "agrees that the *facts alleged in the [FTC] Complaint will be taken as true . . .* in any subsequent civil litigation by [the FTC] to enforce its rights . . ." to the \$5 billion penalty that Facebook was required to pay.⁵⁹² Zuckerberg personally signed this stipulation on July 23, 2019.

575. The statements set forth in ¶¶564-570, *supra*, were also materially false and misleading because they omitted to state material facts necessary to make them, in the light of the circumstances under which they were

⁵⁹¹ *Id.* at ¶174.

⁵⁹² Stipulated Order at 3, ¶I.E.

made, not misleading, including that defendants knew or recklessly disregarded the fact that Facebook was violating Parts I.B and I.C of the FTC Consent Decree, including by:

- (a) Stating publicly in April 2014 that Facebook would stop providing third parties with access to user friends' data—but secretly continuing to provide that data to numerous third parties, including app developers, “whitelisted” third parties, mobile device makers and others;
- (b) Secretly overriding user privacy settings to provide user friends' data to third parties; and
- (c) Knowingly allowing bad actors to access data.

576. Facebook's 2016 Form 10-K also stated:

Affected users or government authorities could initiate legal or regulatory actions against us in connection with any security breaches or ***improper disclosure of data***, which could cause us to incur significant expense and liability or result in orders or ***consent decrees forcing us to modify our business practices***. Any of these events could have a material and adverse effect on our business, reputation, or financial results.

This statement was repeated or incorporated by reference into the other reports on Forms 10-K and 10-Q that Facebook filed with the SEC during the Class Period, including the 1Q17 10-Q, 2Q17 10-Q, 3Q17 10-Q, and the 2017 Form 10-K.

577. Defendants' statement above was materially false and misleading when made because:

- (a) It presented improper disclosures of data and violations of the FTC Consent Decree as hypothetical risks when defendants knew or recklessly disregarded

the fact that Facebook was violating Parts I.B and I.C of the FTC Consent Decree; and

(b) The Company had suffered a significant episode involving an improper disclosure of data.

578. The statement set forth in ¶576, *supra*, was also materially false and misleading because it omitted to state material facts necessary to make it, in light of the circumstances under which it was made, not misleading, including that:

(a) Defendants knew or recklessly disregarded the fact that Facebook was violating Parts I.B and I.C of the FTC Consent Decree; and

(b) The Company had suffered a signature episode involving an improper disclosure of data.

H. Defendants Made Materially False and Misleading Statements Concerning Notifying Facebook Users Whose Accounts Were Compromised or at Risk of Being Compromised

579. Throughout the Class Period, defendants made materially false and misleading statements concerning providing notice to Facebook users whose accounts were compromised or at risk of being compromised.

580. On April 27, 2017, Facebook published on its corporate website a document titled *Information Operations and Facebook* to describe what it was doing to “help[] people protect their accounts from compromise.”⁵⁹³ In this document, Facebook stated: “**We notify our users** with context around the status of their account and actionable recommendations if we assess they are at increased risk

⁵⁹³ Jen Weedon, William Nuland and Alex Stamos, Information Operations and Facebook, Facebook Newsroom at 7 (Apr. 27, 2017).

of future account compromise by sophisticated actors **or when we have confirmed their accounts have been compromised.**⁵⁹⁴

581. Facebook also stated that it would provide:⁵⁹⁵

(a) “**Notifications to specific people** if they have been targeted by sophisticated attackers; with custom recommendations depending on the threat models”; and

(b) “**Proactive notifications to people** who have yet to be targeted, but whom we believe may be **at risk** based on the behavior of particular malicious actors.”

582. The foregoing statements were materially false and misleading because, as defendants knew or recklessly disregarded, defendants did not “notify” Facebook users whose accounts were compromised or at risk of being compromised; did not provide “notifications to specific people” whose accounts or data had been targeted or compromised; and did not provide “proactive notifications to people” whose data may be at risk. On the contrary, the Company did not take any of these steps in response to the biggest data breach in its history—or with respect to any of the other app developers who gained unauthorized access to user information.

583. In fact, Zuckerberg admitted in his Senate testimony that defendants made a conscious decision **not** to

⁵⁹⁴ *Id.* at 7 n.6.

⁵⁹⁵ *Id.* at 7.

notify the tens of millions of users whose data was compromised when Kogan improperly sold that data to Cambridge Analytica.⁵⁹⁶

HARRIS: So there was a decision made on that basis not to inform the users. Is that correct?

ZUCKERBERG: That's my understanding. Yes.

Further, Zuckerberg admitted that he “got it wrong” and “didn’t do enough” in deliberately deciding not to notify those users, which was a “huge mistake [and] [i]t was my mistake [*i.e.*, Zuckerberg’s mistake].”⁵⁹⁷

584. Sandberg also acknowledged that defendants “have the responsibility ***to disclose to people when problems occur[]***,” admitting that the Company failed to meet its disclosure responsibility with respect to the Cambridge Analytica data misuse.⁵⁹⁸ Further, when asked directly whether Facebook should have timely disclosed that Facebook users’ data had been stolen, Sandberg admitted, “[y]es, you are right and we should have done that Of course you are right, and we should have done it.”⁵⁹⁹

⁵⁹⁶ *Transcript of Mark Zuckerberg’s Senate hearing*, Wash. Post (Apr. 10, 2018).

⁵⁹⁷ Interview by Laurie Segall with Mark Zuckerberg, CNN Business (Mar. 22, 2018); Toby Shapshak, *It Was My Mistake Zuckerberg Admits, While Facebook Didn’t Do Enough To Prevent Abuse*, Forbes (Apr. 4, 2018).

⁵⁹⁸ *CNBC Exclusive: CNBC Transcript: Sheryl Sandberg Sits Down with CNBC’s Julia Boorstin Today*, CNBC (Mar. 22, 2018).

⁵⁹⁹ Eun Kyung Kim, Sheryl Sandberg on TODAY: Other Facebook data breaches ‘possible’, Today (Apr. 6, 2018).

585. The statements set forth in ¶¶580-584, *supra*, were also materially false and misleading because they omitted to state material facts necessary to make them, in the light of the circumstances under which they were made, not misleading, including that defendants did not notify users whose accounts had been compromised or who were at risk of having their accounts compromised, did not provide “notifications to specific people” whose accounts or data had been targeted or compromised; and did not provide “proactive notifications to people” whose data may be at risk. On the contrary, the Company did not take any of these steps in response to the biggest data breach in its history—or with respect to any of the other app developers who gained unauthorized access to user information. On the contrary, Zuckerberg admitted that defendants made a conscious decision *not* to notify the tens of millions of users whose data was compromised when Kogan improperly sold that data to Cambridge Analytica. Defendants also later admitted that they “should have” notified users whose accounts were compromised in the Cambridge Analytica scandal, but they “didn’t do enough” to do so.

I. Defendants Made Materially False and Misleading Statements Concerning Facebook’s GDPR Compliance

586. On October 12, 2017, during an interview with Axios, Sandberg stated: “Europe[] has passed a single privacy law [*i.e.*, the GDPR] and *we are adhering to that*. But privacy is something we take really seriously.”⁶⁰⁰

587. The statement set forth in ¶586, *supra*, was materially false and misleading because Facebook was not at

⁶⁰⁰ Mike Allen, *Exclusive interview with Facebook’s Sheryl Sandberg*, Axios (Oct. 12, 2017).

the time “adhering to” the GDPR. On the contrary, defendants were depriving users of control over their data, were sharing it without knowledge or consent and, even worse, were overriding users’ privacy settings when doing so.

588. The statement set forth in ¶586, *supra*, was also materially false and misleading because it omitted to state material facts necessary to make it, in light of the circumstances under which it was made, not misleading, including that Facebook was not adhering to the European privacy law.

J. Defendants Made Materially False and Misleading Statements Concerning Use of Facebook’s Platform to Influence Elections

589. In prepared remarks to the U.S. Senate Committee on the Judiciary Subcommittee on Crime and Terrorism, and the U.S. House of Representatives Permanent Select Committee on Intelligence delivered on October 31 and November 1, 2017 respectively, Facebook General Counsel Stretch stated: “Though the volume of these posts was a tiny fraction of the overall content on Facebook, any amount is too much. Those accounts and Pages violated Facebook’s policies—which is why we removed them, as we do with all fake or malicious activity we find.”⁶⁰¹

590. During his oral testimony before the House subcommittee on November 1, 2017, Stretch participated in

⁶⁰¹ Social Media Influence in the 2016 US Elections: Hearing before the Select Comm. on Intelligence, 115th Cong. (Nov. 1, 2017) at 6 (Prepared Testimony of Colin Stretch, General Counsel, Facebook, Inc.).

the following exchange with Representative Eric Swalwell and Twitter's Deputy General Counsel Sean Edgett:⁶⁰²

SWALWELL: Can each of you assure the American people that you have fully searched your platforms and disclosed to this committee every Russian effort to influence the 2016 election? Mr. Edgett?

EDGETT: *We've provided everything we have to date*, and we're continuing to look at this. So there will be more information that we share.

SWALWELL: Mr. Stretch?

STRETCH: *The same is true*, particularly in connection with, as I mentioned earlier, some of the threat sharing that the companies are now engaged in.

591. In response to a follow-up Question for the Record from U.S. Sen. Dianne Feinstein delivered on January 8, 2018, Stretch further stated:⁶⁰³

Feinstein QFR #4: Facebook confirmed in the House Intelligence committee hearing that they found no

⁶⁰² Russia Investigative Task Force Hearing with Social Media Cos.: Hearing before the H. Rep. Permanent Select Comm. on Intelligence, 115th Cong. (Nov. 1, 2017) at 54 (Testimony of Colin Stretch, General Counsel, Facebook, Inc.).

⁶⁰³ Letter from Colin Stretch, General Counsel, Facebook, Inc. to Chairman Richard Burr, U.S. Senate Select Committee on Intelligence at 8 (Jan. 8, 2018).

overlap in the groups targeted by the Trump campaign's advertisements, and the advertisements tied to the Russia-linked accounts identified thus far. . . .

Does this assessment extend to both the content used and groups targeted by the companies associated with the campaign—like Cambridge Analytica—and Russian accounts?

Stretch: ***We have seen only what appears to be insignificant overlap*** between the targeting and content used by the IRA and that used by the Trump campaign (including its third-party vendors). We are happy to schedule a meeting with your staff to discuss our findings in more detail.

592. Each of these statements was materially false and misleading as a result of defendants' continuing omission to investigate or disclose the extent of the Cambridge Analytica data breach, to notify affected users that their data had been compromised, or to reveal that the Company had no reliable or reasonable basis on which to conclude that the data exposed by Cambridge Analytica had been deleted or recovered, or was otherwise unavailable for use in activities by foreign agents seeking to influence U.S. elections.

593. At the time the statement was made, defendants knew user data had repeatedly been used to design effective political advertising, including by Cambridge Analytica, which was known to have been actively working on behalf of the Trump campaign in the 2016 election. Defendants also knew that Facebook had failed to recover or delete—or even fully investigate the extent of—the Cambridge Analytica data breach. As a result, defendants knew or recklessly disregarded that their testimony about the use of Facebook would be misleading in the absence of a disclosure of the risk that the data of more than 50

million users that had previously been compromised was still available and had been used in targeted political advertising to influence the outcome of the 2016 election.

594. By reason of their claimed investigation into and response to the 2015 report of the data breach, as well as Facebook’s hiring of Chancellor to work in its headquarters, defendants knew or recklessly disregarded that Kogan had worked closely with Russian operatives in the past, giving rise to a heightened risk that data provided to Cambridge Analytica had been obtained by Russian agents either before or after the data breach was originally reported. Russia’s likely targeting of and use of the data exposed by Cambridge Analytica was obvious to anyone who had looked into the matter, as defendants claimed to have done before they testified to Congress. For example, when the Cambridge Analytica scandal was exposed in March 2018, Zuckerberg—in contrast to the testimony above—readily acknowledged that Russia could have targeted the data that Facebook had failed to recover or delete.⁶⁰⁴ Just months later the connection was confirmed by a Member of Parliament, following that body’s investigation in the Cambridge Analytica scandal, further demonstrating the connection was apparent and readily discoverable by those professing to have investigated the matter.

K. Defendants Made Materially False and Misleading Statements Concerning DAU and MAU Metrics

595. Facebook repeatedly touted its quarterly DAU and MAU metrics to assure investors that users would remain engaged with its social media platforms, despite any

⁶⁰⁴ *Transcript of Mark Zuckerberg’s Senate hearing*, Wash. Post (Apr. 10, 2018).

concerns raised over the privacy of their data. For example:

(a) On May 3, 2017, defendants published a press release entitled: “Facebook Reports First Quarter 2017 Results,” in which they stated: “**Daily active users (DAUs)**—DAUs were 1.28 billion on average for March 2017, an increase of 18% year-over-year. **Monthly active users (MAUs)**—MAUs were 1.94 billion as of March 31, 2017, an increase of 17% year-over-year.”⁶⁰⁵ The same day, Zuckerberg posted an update to his personal Facebook.com page, in which he stated: “Our community now has more than 1.9 billion people, including almost 1.3 billion people active every day.”⁶⁰⁶

(b) On July 26, 2017, defendants published a press release entitled: “Facebook Reports Second Quarter 2017 Results,” in which they stated: “**Daily active users (DAUs)**—DAUs were 1.32 billion on average for June 2017, an increase of 17% year-over-year. **Monthly active users (MAUs)**—MAUs were 2.01 billion as of June 30, 2017, an increase of 17% year-over-year.”⁶⁰⁷ The same day, Zuckerberg posted an update to his personal Facebook.com page, in which he stated: “Our community is now more than 2 billion people, including more than 1.3 billion people who use Facebook every day.”⁶⁰⁸

⁶⁰⁵ Press Release, *Facebook Reports First Quarter 2017 Results*, Facebook Investor Relations (May 3, 2017).

⁶⁰⁶ Mark Zuckerberg, Facebook (May 3, 2017).

⁶⁰⁷ Press Release, *Facebook Reports Second Quarter 2017 Results*, Facebook Investor Relations (July 26, 2017).

⁶⁰⁸ Mark Zuckerberg, Facebook (July 26, 2017).

(c) On November 1, 2017, defendants published a press release entitled: “Facebook Reports Third Quarter 2017 Results,” in which they stated: “**Daily active users (DAUs)**—DAUs were 1.37 billion on average for September 2017, an increase of 16% year-over-year. **Monthly active users (MAUs)**—MAUs were 2.07 billion as of September 30, 2017, an increase of 16% year-over-year.”⁶⁰⁹ The same day, Zuckerberg posted an update to his personal Facebook.com page, in which he stated: “Our community continues to grow, now with nearly 2.1 billion people using Facebook every month, and nearly 1.4 billion people using it daily. Instagram also hit a big milestone this quarter, now with 500 million daily actives.”⁶¹⁰

(d) On January 31, 2018, defendants published a press release entitled: “Facebook Reports Fourth Quarter and Full Year 2017 Results,” in which they stated: “**Daily active users (DAUs)**—DAUs were 1.40 billion on average for December 2017, an increase of 14% year-over-year. **Monthly active users (MAUs)**—MAUs were 2.13 billion as of December 31, 2017, an increase of 14% year-over-year.”⁶¹¹ The same day, Zuckerberg posted an update to his personal Facebook.com page, in which he stated: “Our community continues to grow with more than 2.1 billion people

⁶⁰⁹ Press Release, *Facebook Reports Third Quarter 2017 Results*, Facebook Investor Relations (Nov. 1, 2017).

⁶¹⁰ Mark Zuckerberg, Facebook (Nov. 1, 2017).

⁶¹¹ Press Release, *Facebook Reports Fourth Quarter and Full Year 2017 Results*, Facebook Investor Relations (Jan. 31, 2018).

now using Facebook every month and 1.4 billion people using it daily. Our business grew 47% year-over-year to \$40 billion.”⁶¹²

596. Defendants also touted their active monitoring of engagement and these metrics. For example:

(a) Wehner: “***We monitor the sentiment and engagement of people engaging in News Feed.*** We’re really pleased with the strength of sentiment and engagement as we’ve ramped up News Feed ads.”⁶¹³

(b) Sandberg: “Because your experience on Facebook or Instagram is about the quality of what you see . . . what we do is ***we monitor it carefully.*** We ramp slowly. We monitor engagement sentiment, quality of ads. ***We get a lot of feedback directly from people*** who use Facebook. . . . ***And we just continue to monitor the metrics.***”⁶¹⁴

(c) Wehner: “Improving the quality and the relevance of the ads has enabled us to show more of them, without harming the experience. And, our focus really remains on the experience. So, ***we’ll continue to monitor engagement and sentiment very carefully.***”⁶¹⁵

(d) Sandberg: “When we introduce ads into feed and continue to increase the ad load, ***we monitor really carefully. We’re looking at user engagement on the platform.*** We also look at the quality of ads.”⁶¹⁶

⁶¹² Mark Zuckerberg, Facebook (Jan. 31, 2018).

⁶¹³ Q2 2014 Facebook, Inc. Earnings Call Tr. at 16 (July 23, 2014).

⁶¹⁴ Q3 2015 Facebook, Inc. Earnings Call Tr. at 15 (Nov. 4, 2015).

⁶¹⁵ Q4 2015 Facebook, Inc. Earnings Call Tr. at 9 (Jan. 27, 2016).

⁶¹⁶ *Id.* at 10.

(e) Analyst: “Can you just talk about some of the biggest trends you’re monitoring?” Wehner: “Yes, I can start with the stats. So on—yes, Mark, on the engagement front, we’re seeing time spent growth per DAU across the Facebook family of apps and that includes Facebook itself.”⁶¹⁷

(f) Wehner: “We have also increased our estimate for inauthentic accounts to approximately 2% to 3% of worldwide MAUs. . . . **We continuously monitor** and aggressively take down those accounts. These accounts tend to be less active and thus, we believe, impact DAU less than MAU.”⁶¹⁸

597. The statements set forth in ¶¶595-596, *supra*, and the statistics provided therein, were misleading in the context of the surrounding information, because privacy violations had been deliberately concealed from users, such that their active engagement with the Company’s social media platforms was not an accurate or reliable indicator of user response to privacy concerns.

598. The quarterly DAU and MAU metrics set forth above were materially false and misleading for additional reasons. For instance, the DAU and MAU figures reported for Q1 2017 and Q2 2017 were materially false and misleading because, at the time, Facebook was using an incorrect methodology to calculate duplicate accounts, which caused the Company to overstate DAUs and MAUs and understate duplicate accounts. Facebook admitted to this reality on November 1, 2017, when it implemented a “new methodology for duplicate accounts that included

⁶¹⁷ Q1 2017 Facebook, Inc. Earnings Call Tr. at 9 (May 3, 2017).

⁶¹⁸ Q3 2017 Facebook, Inc. Earnings Call Tr. at 7 (Nov. 1, 2017).

improvements to the data signals we rely on to help identify such accounts.”⁶¹⁹

599. All of the above DAU and MAU figures were materially false and misleading because they failed to account for the number of fake accounts on Facebook. In May 15, 2018, Facebook announced for the first time that it had deleted a total of **1.277 billion fake accounts** during the period from Q4 2017 to Q2 2018.

600. The statements set forth in ¶¶595-596, *supra*, were also materially false and misleading because they omitted to state material facts necessary to make them, in the light of the circumstances under which they were made, not misleading, including that defendants had knowingly or recklessly misrepresented Facebook’s privacy practices, including by violating Parts I.B and I.C of the FTC Consent Decree, which, when revealed, would (and did) erode user trust in Facebook and cause a decline in daily and monthly active users. Further, given their privacy misconduct, defendants omitted the fact that they knew or recklessly ignored that active user engagement metrics were not accurate or reliable indicators of the health or strength of Facebook’s business.

601. The statements set forth in ¶¶595-596, *supra*, were also materially false and misleading because they omitted to state material facts necessary to make them, in the light of the circumstances under which they were made, not misleading, including the fact that Facebook was using an incorrect methodology to calculate duplicate accounts and the fact that hundreds of millions of the accounts were fake. Indeed, Facebook eventually revealed

⁶¹⁹ *Id.*

that it had deleted a total of **1.277 billion fake accounts** during the period from Q4 2017 to Q2 2018.

L. Defendants Made Materially False and Misleading Statements Concerning Facebook’s 1Q18 Financial Results and the Impact of the Privacy Disclosures on Facebook’s Business

602. On April 25, 2018, defendants published a press release entitled: “Facebook Reports First Quarter 2018 Results,” in which they stated: “**Daily active users (DAUs)**—DAUs were 1.45 billion on average for March 2018, an increase of 13% year-over-year. **Monthly active users (MAUs)**—MAUs were 2.20 billion as of March 31, 2018, an increase of 13% year-over-year.”⁶²⁰ The same day, Zuckerberg posted an update to his personal Facebook.com page, in which he stated: “Despite facing important challenges, our community continues to grow. More than 2.2 billion people now use Facebook every month and more than 1.4 billion people use it daily.”⁶²¹

603. The Company’s earnings release and 10-Q report highlighted the growth in MAUs and DAUs as a sign of the success of its business, while its officers touted the strength of the Company’s business as an indicator of the purported lack of meaningful impact resulting from the controversy. “Despite facing important challenges, our community and business are off to a strong start in 2018,” Zuckerberg told investors in Facebook’s first quarter of 2018 earnings release. On April 25, 2018, during Facebook’s earnings call for the first quarter of 2018, Zuckerberg added that “sharing and interaction” and other indicators of user engagement were increasing as a result of

⁶²⁰ Press Release, *Facebook Reports First Quarter 2018 Results*, Facebook Investor Relations (Apr. 25, 2018).

⁶²¹ Mark Zuckerberg, Facebook (Apr. 25, 2018).

changes in the platforms' ranking and sharing algorithms. "[W]e're optimistic about what we're seeing here," he said. During the first quarter conference call, Wehner told investors that the first quarter of 2018 results "demonstrated [that] growth in our business and global community remains strong," while telling them "we do not anticipate [that new European privacy regulations] will significantly impact advertising revenues."⁶²²

604. Even when defendants acknowledged impacts of the Cambridge Analytica data scandal, they assured investors that any negative effect would be short-lived and manageable without negative impact to the business. Wehner told investors on the earnings call that the increased spending needed to beef up data security programs in the wake of the scandal were already included in the first quarter of 2018 results, and the increase in the lower limit of the Company's spending guidance simply reflected that it was "putting more" investment into that category "more quickly than we anticipated." Sandberg allowed that a "handful" of advertisers had "paused spend" immediately after the Cambridge Analytica scandal broke, but encouraged investors to take an optimistic outlook by telling them that one of the advertisers that reduced spend "has already come back" and assuring investors that "we haven't seen a meaningful trend or anything much since then."⁶²³

605. On Facebook's April 25, 2018 first quarter earnings call, Sandberg stated:⁶²⁴

⁶²² Q1 2018 Facebook, Inc. Earnings Call Tr. at 6, 7, 9 (Apr. 25, 2018).

⁶²³ *Id.* at 8, 12.

⁶²⁴ *Id.* at 4-6.

Before going through our results, I want to take a minute to talk about ads and privacy. [. . .]

We also believe that people should control their advertising experience. For every ad we show, there's an option to find out why you're seeing that ad and to turn off ads from that advertiser entirely. And you can opt out of being targeted based on certain information like the websites you visit or your relationship status.

Advertising and protecting people's information are not at odds. We do both. Targeted ads that respect people's privacy are better ads. They show people things that they're more likely to be interested in. We regularly hear from people who use Facebook that they prefer to see ads that are relevant to them and their lives.

Effective advertising is also critical to helping businesses grow.

* * *

In the coming months, GDPR will give us another opportunity to make sure people fully understand how their information is used by our services. It's an EU regulation, but as Mark said a few weeks ago, we're going to extend these controls to everyone who uses Facebook, regardless of where in the world they live. Our commitment to you is that we will continue to improve our ads model by strengthening privacy and choice while giving businesses of all sizes new and better tools to help them grow.

* * *

Going forward, we will continue to focus on these 3 priorities and ensure that people's privacy is protected on Facebook.

606. On the same April 25, 2018 call, Wehner stated:⁶²⁵

The changes that Mark and Sheryl described will, we believe, benefit our community and our business and will serve to strengthen Facebook overall. At the highest level, we believe that we can continue to build a great ads business while protecting people's privacy.

* * *

So on GDPR, I think fundamentally, we believe we can continue to build a great ads business while protecting the privacy of the people that use Facebook. As part of the rollout of GDPR, we're providing a lot of control to people around their ad settings. And we're committed, as Sheryl and Mark mentioned, to providing the same controls worldwide. And while we don't expect these changes will significantly impact advertising revenue, there's certainly potential for some impact. Any change of our—of the ability for us and our advertisers to use data can impact our optimizational potential at the margin, which could impact our ability to drive price improvements in the long run. So we'll just have to watch how that plays out over time. I think it's important to note that GDPR is affecting the entire online advertising industry. And so what's really most important in winning budgets is our relative performance versus other opportunities presented to marketers, and that's why it will be important to watch kind of how this plays out at the industry level.

* * *

I don't know that we really see a doomsday scenario here. I think what we think is that depending on how people react to the controls and the ad settings, there

⁶²⁵ *Id.* at 6, 8, 15.

could be some limitations to data usage. We believe that those will be relatively minor. But depending on how broadly the controls are adopted and set, there is a potential to impact targeting for our advertisers. Obviously, if they are less able to target effectively, they'll get a lower ROI on their advertising campaigns. They'll then bid differently into the auction. That ultimately will flow through into how we can realize price on the impressions that we're selling. So I think that's the mitigating issue that we could see, depending on how GDPR and our broader commitment to providing these same controls worldwide could play out. We think that there is a great case for not just our business but also for the user experience on Facebook to have targeting because we think it's a better experience for the people who use Facebook to have targeted ads. We think we can do that in a privacy-protected way, and it's just a better experience. You get more relevant ads, and it's—and I think overall benefits that only the advertisers but also the people who use Facebook. So I don't think see a real doomsday scenario here. We see an opportunity to really make the case.

607. Defendants' effort to tout the first quarter of 2018 results in a manner meant to assure investors that the Cambridge Analytica data scandal had not, and would not, have a meaningful financial impact on the business was misleading, because they knew or recklessly disregarded that those results were not reflective of the true impact that disclosure of the Cambridge Analytica data breach was having on the Company's business:

(a) To begin with, the quarterly results only included two weeks of user data post-disclosure of the wider scope of the Cambridge Analytica data breach.

Nevertheless, defendants, who knew or recklessly disregarded that assessment of the true impact would become apparent in the current quarter (based in part on their active monitoring of user engagement, *see* ¶1596, assured investors that the first quarter results were sufficient to conclude that the disclosures would not have a meaningful financial impact.

(b) In addition, defendants concealed that the loss of advertisers was far more significant than Sandberg’s “handful . . . one of whom has already come back” statement suggested. For example, Italy’s biggest bank, UniCredit, had terminated all of its advertising and partnerships with Facebook at the end of March as a result of the scandal. The action did not come to light until August 2018, when *The Guardian* published an article about it.⁶²⁶ “Facebook is not acting in an ethical way,” the bank’s CEO, Jean Pierre Mustier, told the newspaper. “We will not use it until it has proper ethical behavior.” As revealed on the second quarter of 2018 earnings call, this was not an isolated incident, as many other advertisers had similarly cut ties with Facebook, or reduced spending on its platform.

(c) Finally, defendants knew that massive increases in spending would be required to improve the security of user data and Facebook’s platform, which further made the first quarter of 2018 results not reflective of the true impact that the data breach scandal would have on Facebook’s financial condition and results.

⁶²⁶ Rupert Neate, *UniCredit cuts ties with Facebook over data breach scandal*, *Guardian* (Aug. 7, 2018).

608. Thereafter, defendants continued to mislead investors, analysts, users and others about the risks of user dis-engagement and the financial impact of the disclosures about the Company's privacy practices. In numerous public comments, defendants falsely assured investors that the privacy disclosures had not impacted, and could not reasonably be expected to impact the Company's business.

609. On May 1, 2018, Zuckerberg gave his keynote address at Facebook's annual F8 Developer Conference. In that appearance, Zuckerberg stated:⁶²⁷

I also want to talk about data privacy. And what happened with Cambridge Analytica was a major breach of trust. An app developer took data that people had shared with them and sold it. So we need to make sure that this never happens again, so we're taking a number of steps here.

First, as you all know we're restricting the data that developers will be able to request from people. ***Now the good news here is that back in 2014, we already made a major change to how the platform works to prevent people from sharing a lot of their friends' information. So this specific situation could not happen again today.***

610. The above statements were materially misleading because they assured investors that data breaches like the Cambridge Analytica scandal were behind the Company and the consequences of that breach would be minimal because Facebook had been protecting privacy for years. In reality, Facebook had not been protecting privacy and the consequences of Facebook's data protection

⁶²⁷ F8 2018 Developer Conference Tr. at 9 (May 1, 2018).

misconduct would not be fully revealed until July 25, 2018, when Facebook disclosed, *inter alia*, heightened privacy-related expenses and declining active user figures.

611. In addition, the statements set forth in ¶609, *supra*, were materially false and misleading because they omitted the following material facts necessary in order to make those statements, in light of the circumstances under which they were made, not misleading: (i) Facebook had violated the 2012 FTC Consent Decree; (ii) Facebook's privacy misconduct would impact the Company's bottom line by destroying its reputation as a company that protected privacy and by requiring the Company to incur billions in expenses to become privacy compliant, including with respect to the GDPR; and (iii) as a result, Facebook's user numbers, revenue growth, operating margins and business prospects would materially decline. Defendants' knowledge or reckless disregard that these statements would be, and were, misleading to investors may be inferred from the same facts that support a strong inference of scienter with respect to the assurances about Facebook's purported commitment to enforcement of its privacy policies.

612. On May 31, 2018, Facebook held its Annual Stockholders Meeting. At this event, Zuckerberg stated:⁶²⁸

So we recently went through this process of rolling out our flows and settings for GDPR compliance, first, in Europe, and we're going to do it around the world. And one of the settings that we ask people proactively to make a decision on is, do you want your ads, for how we do ad targeting, to be informed by the other apps

⁶²⁸ Facebook, Inc., Annual Shareholders Meeting Tr. at 16-17 (May 31, 2018).

and websites that you use? ***People have to proactively make a decision. Yes or no. Do they want that data used? And the majority, I think we can even say vast majority of people say, yes, they want that data used.*** Because if they're going to see ads, you want to see good ads, right? So I think that this is one of the core questions that society faces and individuals face across the different services that we use, are how do we want our data to be used and where? . . . This is going to be a core thing that we need to think about going forward, but we think about it very deeply as this is a—just a core part of the value that we're trying to provide.

613. The above statement was materially misleading because: (i) it falsely and without a reasonable basis assured investors that GDPR had not caused, and would not cause, a decline in active use of Facebook's social media platforms; and (ii) it portrayed Facebook as adhering to and prepared to meet the requirements of the GDPR, when in reality Facebook was not.

614. In addition, the statements set forth in ¶612, *supra*, were materially false and misleading because they omitted the following material facts necessary in order to make those statements, in light of the circumstances under which they were made, not misleading: (i) Facebook had violated the 2012 FTC Consent Decree; (ii) Facebook's privacy misconduct would impact the Company's bottom line by destroying its reputation as a company that protected privacy and by requiring the Company to incur billions in expenses to become privacy compliant, including with respect to the GDPR; and (iii) as a result, Facebook's user numbers, revenue growth, operating margins and business prospects would materially decline. Defend-

ants' knowledge or reckless disregard that these statements would be, and were, misleading to investors may be inferred from the same facts that support a strong inference of scienter with respect to the assurances about Facebook's purported commitment to enforcement of its privacy policies.

615. On June 8, 2018, Facebook provided additional responses to questions posed to the Company by the members of the Senate Committee on Commerce, Science, and Transportation. In their responses to these questions, defendants stated.⁶²⁹

Privacy is at the core of everything we do, and our approach to privacy starts with our commitment to transparency and control. Our threefold approach to transparency includes, first, whenever possible, providing information on the data we collect and use and how people can control it in context and in our products. Second, we provide information about how we collect and use data in our user agreements and related educational materials. And third, we enable people to learn more about the specific data we have about them through interactive tools such as Download Your Information, which lets people download a file containing data that they may want to take to another service, and Access Your Information, a tool we are launching that will let people more easily access and manage their data on Facebook.

Our approach to control is based on the belief that people should be able to choose who can see what

⁶²⁹ Facebook, Responses to U.S. Senate Committee on the Judiciary, Questions for the Record addressed Chairman Grassley (June 8, 2018).

they share and how their data shapes their experience on Facebook. People can control the audience for their posts and the apps that can receive their data. They can see and delete the history of their activities on Facebook, and, if they no longer want to use Facebook, they can delete their account and the data associated with it. Of course, we recognize that controls are only useful if people know how to find and use them. That is why we continuously deliver in-product educational videos in people's News Feeds on important privacy topics. We are also inviting people to take our Privacy Checkup—which prompts people to review key data controls—and we are sharing privacy tips in education campaigns off of Facebook, including through ads on other websites. To make our privacy controls easier to find, we are launching a new settings menu that features core privacy settings in a single place. We are always working to help people understand and control how their data shapes their experience on Facebook.

* * *

Like many other free online services, we sell advertising space to third parties. Doing so enables us to offer our services to consumers for free. This is part of our mission to give people the power to build community and bring the world closer together.

* * *

We believe that everyone has the right to expect strong protections for their information, and that we also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations.

616. On June 29, 2018, Facebook provided further responses to questions posed to the Company by the members of the Senate Committee on Commerce, Science, and Transportation. In their responses to these questions, defendants stated:⁶³⁰

We maintain our commitment to privacy by not telling advertisers who users are or selling people’s information to anyone. That has always been true. We think relevant advertising and privacy are not in conflict, and we’re committed to doing both well.

* * *

We believe targeted advertising creates value for people and advertisers who use Facebook. Being able to target ads to the people most likely to be interested in the products, service or causes being advertised enables businesses and other organizations to run effective campaigns at reasonable prices.

* * *

We do not have a “business reason” to compromise the personal data of users; we have a business reason to protect that information.

617. The above statements were materially misleading because they assured investors that data breaches like the Cambridge Analytica scandal were behind the Company and the consequences of that breach would be minimal because Facebook had been protecting privacy for years. In reality, Facebook had not been protecting privacy and the consequences of Facebook’s data protection misconduct would not be fully revealed until July 25, 2018,

⁶³⁰ Facebook, Responses to House Energy and Commerce, Questions for the Record addressed Chairman Walden (June 29, 2018).

when Facebook disclosed, *inter alia*, heightened privacy-related expenses and declining active user figures.

618. The statements set forth in ¶615, *supra*, were also materially false and misleading because, contrary to Facebook’s representations that, for example, users had “control” over their data and “choice” over to whom it was disclosed, app developers had collected vast amounts of Facebook users’ friends’ personal data without their knowledge or consent prior to 2014—and still possessed that data. Further, as set forth above, during the Class Period, Facebook was still engaged in harvesting and using Facebook users’ data without their knowledge or consent and, as such, depriving users of control over their personal data.

619. In addition, the statements set forth in ¶615, *supra*, were materially false and misleading because they omitted the following material facts necessary in order to make those statements, in light of the circumstances under which they were made, not misleading: (i) Facebook had violated the 2012 FTC Consent Decree; (ii) Facebook’s privacy misconduct would impact the Company’s bottom line by destroying its reputation as a company that protected privacy and by requiring the Company to incur billions in expenses to become privacy compliant, including with respect to the GDPR; and (iii) as a result, Facebook’s user numbers, revenue growth, operating margins and business prospects would materially decline. Defendants’ knowledge or reckless disregard that these statements would be, and were, misleading to investors may be inferred from the same facts that support a strong inference of scienter with respect to the assurances about Facebook’s purported commitment to enforcement of its privacy policies.

M. Defendants Made Materially False and Misleading Statements that Facebook Does Not “Sell” Users’ Data

620. Throughout the Class Period, defendants made materially false and misleading statements that Facebook does not “sell” users’ data. In reality, defendants were using user friend data as consideration for a reciprocal exchange of value with third-party app developers and other companies who were “whitelisted” for secret access to user friend data. Thus, defendants engaged in selling user friend data in exchange for reciprocal benefits. For defendants, “reciprocity” came in various forms, including an exchange of data between an app developer and Facebook, by Facebook requiring the third party to spend substantial sums on advertising at Facebook or by a third party enhancing Facebook’s brand and platform to make it more attractive to users, as in the case of the dozens of major phone device makers that Facebook whitelisted during the Class Period.

621. On or about November 27, 2017, defendants posted a notification on Facebook.com titled “Our Advertising Principles,” in which they stated in relevant part: **“We don’t sell your data.** We don’t sell personal information like your name, Facebook posts, email address, or phone number to anyone. Protecting people’s privacy is central to how we’ve designed our ad system.”⁶³¹

622. On January 31, 2018, during Facebook’s earnings call for the second quarter of 2017, Sandberg stated in relevant part, “These principles are our commitment to the

⁶³¹ Rob Goldman, *Our Advertising Principles*, Facebook Newsroom (Nov. 27, 2017).

people who use our services. They are: We build for people first. ***We don't sell your data.***⁶³²

623. On March 22, 2018, during an interview on the CNBC television program “Closing Bell,” Sandberg again stated: “We provide a free service that’s an ad-based business model, and in order to do that, ***we do not sell your data.***”⁶³³

624. On April 4, 2018, during a teleconference with members of the press, Zuckerberg stated:⁶³⁴

There are other internet companies or data brokers or folks that might try to track and sell data, ***but we don't buy and sell.*** [. . .] The second point, which I touched on briefly there: for some reason ***we haven't been able to kick this notion for years that people think we will sell data to advertisers. We don't. That's not been a thing that we do. Actually it just goes counter to our own incentives.*** . . . And we're going to use data to make those services better but ***we're never going to sell your information.***

625. The same day, defendants posted a notification on Facebook.com titled: “We’re Making Our Terms and Data Policy Clearer, Without New Rights to Use Your Data on Facebook,” in which they stated in relevant part: “**What we share: *We will never sell your information to***

⁶³² Q4 2017 Facebook, Inc. Earnings Call Tr. at 6 (Jan. 31, 2018).

⁶³³ *CNBC Exclusive: CNBC Transcript: Sheryl Sandberg Sits Down with CNBC's Julia Boorstin Today*, CNBC (Mar. 22, 2018).

⁶³⁴ *Hard Questions: Q&A With Mark Zuckerberg on Protecting People's Information*, Facebook Newsroom (Apr. 4, 2018).

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.*”⁶³⁵

626. On April 5, 2018, Sandberg stated during an interview on National Public Radio: “It’s a good opportunity to remind everyone what we say all the time, but we need to keep saying so people understand it—which is that *we don’t sell data, period*, . . . And again, we do not sell data, ever.”⁶³⁶

627. The same day, during an interview with PBS NewsHour, Sandberg stated: “*We do not sell data* or give your personal data to advertisers, *period.*”⁶³⁷

628. On April 10, 2018, Zuckerberg appeared to testify before the Joint Commerce, Science, and Transportation and Judiciary Committees of the United States Senate, during which he stated: “I want to be clear. *We don’t sell information. So regardless of whether we could get permission to do that, that’s just not a thing we’re going to go do.*” Zuckerberg further stated: “Well, Senator, once again, *we don’t sell any data to anyone. We don’t sell it to advertisers, and we don’t sell it to developers.*” During the same hearing, Zuckerberg stated: “*We don’t sell data to anyone.*”⁶³⁸

⁶³⁵ Erin Egan and Ashlie Beringer, *We’re Making Our Terms and Data Policy Clearer, Without New Rights to Use Your Data on Facebook*, Facebook Newsroom (Apr. 4, 2018).

⁶³⁶ Steve Inskeep, *Full Transcript: Facebook COO Sheryl Sandberg On Protecting User Data*, NPR (Apr. 5, 2018).

⁶³⁷ Judy Woodruff, *Sheryl Sandberg: Facebook ‘made big mistakes’ on protecting user data*, PBS (Apr. 5, 2018).

⁶³⁸ *Transcript of Mark Zuckerberg’s Senate Hearing*, Wash. Post (Apr. 10, 2018).

629. On April 11, 2018, Zuckerberg appeared before the Energy and Commerce Committee of the United States House of Representatives, during which hearing he stated: “Mr. Chairman, ***you’re right that we don’t sell any data.*** . . . There is a common misperception, as you say, that is just reported—often keeps on being reported, that, for some reason, we sell data. ***I can’t be clearer on this topic. We don’t sell data.***” And he reiterated, “***Congressman, we don’t sell people’s data.*** So I think that’s an important thing to clarify up front.”⁶³⁹

630. On April 25, 2018, during Facebook’s earnings call for the first quarter of 2018:⁶⁴⁰

(a) Zuckerberg stated: “We use the information you provide and that we receive from websites to target ads for advertisers, but we don’t tell them who you are. ***We don’t sell your information to advertisers or anyone else.***”

(b) Sandberg stated: “***At Facebook, we have always built privacy protection into our ads system. . . . We don’t sell your information to advertisers or anyone else.***”

631. On May 24, 2018, defendants posted to Facebook.com their follow up to Zuckerberg’s testimony before the European Parliament, in which they stated in relevant part, “We don’t tell advertisers who you are; and ***we don’t sell your data.***”⁶⁴¹

⁶³⁹ *Id.*

⁶⁴⁰ Q1 2018 Facebook, Inc. Earnings Call, Tr. at 4 (Apr. 25, 2018).

⁶⁴¹ Facebook Brussels, *Follow-up questions from EP* (May 24, 2018).

632. On June 29, 2018, defendants filed written responses to additional questions posed to them by the Energy and Commerce Committee of the U.S. House of Representatives, in which they stated: “**Facebook does not sell people’s information to anyone, and we never will.**” Defendants further stated: “When the individual is a Facebook user, we are also able to use this information to personalize their experiences on Facebook, whether or not they are logged out, but we will not target ads to users relying on this information unless the user allows this in their privacy settings. **We don’t sell or share this information with third parties.**”⁶⁴²

633. On July 18, 2018, in an interview with Recode, Zuckerberg stated: “**We don’t sell data.** . . . So while it may seem like a small difference to you, this distinction on “selling data,” I actually think to people it’s like the whole game, right? **So we don’t sell data, we don’t give the data to anyone else,** but overwhelmingly people do tell us that if they’re going to see ads on Facebook, they want the ads to be relevant; they don’t want bad ads.”⁶⁴³

634. Defendants’ statements in ¶¶621-633, *supra*, were materially false and misleading when made. In reality, defendants were using user friend data as consideration for a reciprocal exchange of value with third-party app developers and other companies who were “whitelisted” for secret access to user friend data. Thus, defendants engaged in selling user friend data in exchange for reciprocal benefits. For defendants, “reciprocity” came in

⁶⁴² Facebook, Responses to House Energy and Commerce, Questions for the Record addressed Chairman Walden (June 29, 2018) at 62.

⁶⁴³ Kara Swisher, *Full Transcript: Facebook CEO Mark Zuckerberg on Recode Decode*, Recode (July 18, 2018).

various forms, including an exchange of data between an app developer and Facebook, by Facebook requiring the third party to spend substantial sums on advertising at Facebook or by a third party enhancing Facebook's brand and platform to make it more attractive to users, as in the case of the dozens of major phone device makers that Facebook whitelisted during the Class Period.

635. Indeed, as noted by Slate, Facebook's whitelisting "private agreements were conditional on the third party sending over its own valuable user data to Facebook, or on the company making big advertising purchases with Facebook," which constitutes a "business in selling or bartering data."⁶⁴⁴

636. Defendants' statements in ¶¶621-633, *supra*, were also materially false and misleading because they omitted to state material facts necessary to make them, in the light of the circumstances under which they were made, not misleading, including the fact that defendants were using user friend data as consideration for a reciprocal exchange of value with third-party app developers and other companies who were "whitelisted" for secret access to user friend data. Thus, defendants engaged in selling user friend data in exchange for reciprocal benefits. For defendants, "reciprocity" came in various forms, including an exchange of data between an app developer and Facebook, by Facebook requiring the third party to spend substantial sums on advertising at Facebook or by a third party enhancing Facebook's brand and platform to make it more attractive to users, as in the case of the dozens of major phone device makers that Facebook whitelisted during the Class Period.

⁶⁴⁴ Elena Botella, *Facebook Earns \$132.80 From Your Data Per Year*, Slate (Nov. 15, 2018).

N. Additional False and Misleading Statements

637. Lead Plaintiffs acknowledge that the Court’s August 7, 2019 Order Granting Defendants’ Motion to Dismiss with Leave to Amend (ECF No. 137) (the “MTD Order”) found the following statements not to have been false and misleading. For the avoidance of doubt, Lead Plaintiffs stand on the prior allegations in their Second Amended Consolidated Class Action Complaint (ECF No. 123) and preserve their right to appeal these dismissed statements.

1. Statements in Facebook’s September 29, 2016 Privacy Policy

638. Among the Privacy Policies publicized by Facebook that, read in conjunction with the risk warnings, caused investors to be misled were the following: “PROMOTE SAFETY AND SECURITY. We use the information we have to help verify accounts and activity, and to promote safety and security on and off of our Services, such as by investigating suspicious activity or violations of our terms or policies.”⁶⁴⁵

639. The Privacy Policy additionally stated: “We work hard to protect your account using teams of engineers, automated systems, and advanced technology such as encryption and machine learning.”⁶⁴⁶

640. The Privacy Policy additionally stated: “These partners must adhere to strict confidentiality obligations

⁶⁴⁵ Facebook Data Policy (Sept. 29, 2016) (The Court’s MTD Order identified this statement as Statement 3).

⁶⁴⁶ *Id.* (The MTD Order identified this statement as Statement 4.).

in a way that is consistent with this Data Policy and the agreements we enter into with them.”⁶⁴⁷

641. The foregoing privacy policies were misleading in and of themselves because defendants failed to disclose that Facebook had repeatedly failed to adhere to them. As a result, the magnitude of the risks facing the Company from negative press reports, government and regulatory investigations, and user disengagement arising from disclosure of the massive amount of user data that had already been compromised was materially and substantially greater than investors understood based on the information available at the time the risk warnings were provided.

642. For example, contrary to the assurance that Facebook “investigat[ed] suspicious activity or violations of our terms or policies,” the Company had deliberately ignored information brought to its attention about such risks and violations. In particular, during the Class Period, defendants were still concealing that they had failed to fully or promptly investigate or address the Cambridge Analytica data breach, and continued to cover up the fact that the Company had repeatedly failed to respond to, and had deliberately ignored, thousands of reports of violations of its terms of use and policies regarding user data. Defendants were also knowingly or recklessly providing unauthorized access to user friend data to numerous third parties, including app developers, whitelisted third parties and others.

643. Contrary to the assertion that defendants “work hard to protect your account using teams of engineers, automated systems, and advanced technology,” the Com-

⁶⁴⁷ *Id.* (The MTD Order identified this statement as Statement 5.).

pany had no ability to track the user data provided to developers or others, much less any ability to determine whether that information had been used or shared beyond the extent authorized by the user, or what user data had been compromised, who had it, or how it was being used. In particular, during the Class Period, the Company was still concealing that it was unaware of how much data had been compromised or how many users had been affected by the Cambridge Analytica data breach, or what other developers or third parties had improperly accessed, used or distributed user data, or where or how any of that data was being used. Defendants were also knowingly or recklessly providing unauthorized access to user friend data to numerous third parties, including app developers, whitelisted third parties and others.

644. Contrary to the warning to app developers that the Company would enforce its Platform Policies to prevent app developers from selling or transferring user data, or from using their customers' friend data outside of their customer's use of the app, Facebook had failed to make any effort to verify that user data compromised in the Cambridge Analytica data breach had been deleted, and its enforcement of the Platform Policies regarding user data was limited, haphazard and inconsistent. Defendants were also knowingly or recklessly providing unauthorized access to user friend data to numerous third parties, including app developers, whitelisted third parties and others.

645. Contrary to the assertions that the Company's vendors, service providers and other partners "must adhere to strict confidentiality obligations in a way that is consistent with" Facebook's terms of use and privacy policies, and that the Company "require[s] applications to respect [user] privacy, and [the user's] agreement with that

application will control how the application can use, store, and transfer that content and information,” or that the Company expected app developers and others to protect user’s rights by making it clear what information is being collected and how it is being used, Facebook had repeatedly ignored information brought to its attention about violations of those policies, and repeatedly authorized developers and others to use information in ways that were directly contrary to those policies. Defendants were also knowingly or recklessly providing unauthorized access to user friend data to numerous third parties, including app developers, whitelisted third parties and others.

646. Defendants’ knowledge or reckless disregard that these statements would be, and were, misleading to investors may be inferred from the same facts that support a strong inference of scienter with respect to the assurances about Facebook’s purported commitment to enforcement of its privacy policies.

647. Further, the statements set forth above were materially false and misleading because they omitted the following material facts necessary in order to make those statements, in light of the circumstances under which they were made, not misleading: (i) the Company had knowingly or recklessly allowed third parties other than Cambridge Analytica and its affiliates to harvest and misuse users’ data without their knowledge or consent; (ii) Facebook had taken no action against those other malicious actors upon learning that user data had been compromised in violation of Facebook’s terms of service; (iii) Facebook had waited six months before asking Cambridge Analytica and other entities to certify that all user data had been destroyed and then failed to take any steps to confirm destruction; (iv) Facebook had made no effort to identify

what data had been compromised from what users; (v) Facebook had violated the FTC Consent Decree; (vi) Facebook had made no effort to notify users that Cambridge Analytica or the other app developers had, without users' knowledge or consent, collected and still possessed vast amounts of Facebook users' friends' personal data; and (vii) a major risk to Facebook's business model, finances and reputation existed.

2. Statements in Facebook's February 3, 2017 10-K Report

648. Facebook's 2016 Form 10-K, dated February 3, 2017, contained the following statements concerning the risks to Facebook's business due to a loss of user trust in Facebook's ability to protect users' privacy, as could occur following public reports or investigations into breaches of Facebook's privacy policies, or the Company's past failures to address known breaches of those policies:

(a) “[T]echnical or other problems prevent us from delivering our products in a rapid and reliable manner or otherwise affect the user experience, such as security breaches or failure to prevent or limit spam or similar content”;⁶⁴⁸

(b) “[W]e, developers whose products are integrated with our products, or other partners and companies in our industry are the subject of adverse media reports or other negative publicity”;⁶⁴⁹

⁶⁴⁸ FY 2016 Facebook, Inc. Form 10-K at 8 (Feb. 3, 2017) (The MTD Order identified this statement as Statement 16.).

⁶⁴⁹ *Id.* at 9 (The MTD Order identified this statement as Statement 17.).

(c) “Unfavorable media coverage could negatively affect our business”;⁶⁵⁰ and

(d) “We have been subject to regulatory investigations and settlements, and we expect to continue to be subject to such proceedings and other inquiries in the future, which could cause us to incur substantial costs or require us to change our business practices in a manner materially adverse to our business.”⁶⁵¹

649. The statements quoted above were repeated or incorporated by reference into the other reports on Forms 10-K and 10-Q that Facebook filed with the SEC during the Class Period, including its reports filed on May 4, 2017 (1Q17 10-Q), July 27, 2017 (2Q17 10-Q), November 2, 2017 (3Q17 10-Q), and February 1, 2018 (FY17 10-K), each of which were materially false and misleading for the same reasons as set forth below.

650. Each of these statements was materially false or misleading because they described the risks to Facebook’s business and reputation arising from its privacy practices and from developers’ and other third parties’ use of Facebook user data as hypothetical, contingent and based on events that had not yet occurred, while omitting to disclose that the Company’s previously reported data breaches were much broader than the Company had disclosed, such that the risks of negative media reports and regulatory investigations that could harm Facebook’s reputation and negatively impact its user engagement, growth, and financial condition were materially greater than investors would reasonably understand based on the

⁶⁵⁰ *Id.* at 13 (The MTD Order identified this statement as Statement 18.).

⁶⁵¹ *Id.* at 16 (The MTD Order identified this statement as Statement 19.).

foregoing statements. Defendants were also knowingly or recklessly providing unauthorized access to user friend data to numerous third parties, including app developers, whitelisted third parties and others. Defendants' knowledge or reckless disregard that these statements would be, and were, misleading to investors may be inferred from the same facts that support a strong inference of scienter with respect to the assurances about Facebook's purported commitment to enforcement of its privacy policies.

651. The misleading impact of these statements was heightened by the other statements Facebook and its officers made about protecting user data, including in the Company's terms of use and privacy policies and the other systems, controls and procedures that defendants regularly touted regarding the purported strength of their efforts to protect users from harm resulting from the unauthorized disclosure of their data, and their purported commitment to vigorously enforcing policies designed to prevent that from occurring, including by notifying affected users and banning or taking legal action against those who had disseminated their data without consent.

652. Further, the statements set forth above were materially false and misleading because they omitted the following material facts necessary in order to make those statements, in light of the circumstances under which they were made, not misleading: (i) the Company had knowingly or recklessly allowed third parties other than Cambridge Analytica and its affiliates to harvest and misuse users' data without their knowledge or consent; (ii) Facebook had taken no action against those other malicious actors upon learning that user data had been compromised in violation of Facebook's terms of service; (iii) Facebook

had waited six months before asking Cambridge Analytica and other entities to certify that all user data had been destroyed and then failed to take any steps to confirm destruction; (iv) Facebook had made no effort to identify what data had been compromised from what users; (v) Facebook had violated the FTC Consent Decree; (vi) Facebook had made no effort to notify users that Cambridge Analytica or the other app developers had, without users' knowledge or consent, collected and still possessed vast amounts of Facebook users' friends' personal data; and (vii) a major risk to Facebook's business model, finances and reputation existed.

3. Additional Statements in Facebook's March 16, 2018 Post

653. Facebook's March 16, 2018 public post on Facebook.com entitled: "Suspending Cambridge Analytica and SCL Group From Facebook" contained the following statement: "These include steps such as random audits of existing apps along with the regular and proactive monitoring of the fastest growing apps. We enforce our policies in a variety of ways—from working with developers to fix the problem, to suspending developers from our platform, to pursuing litigation."⁶⁵²

654. The above statement was materially misleading because it was designed to cast doubt on *The New York Times* and *Guardian* articles reporting on Facebook's failure to address the Cambridge Analytica data breach in a manner consistent with defendants' past public statements. In reality, Facebook was not remotely "enforcing

⁶⁵² Paul Grewal, *Suspending Cambridge Analytica and SCL Group From Facebook*, Facebook Newsroom (Mar. 16, 2018) (The MTD Order identified this statement as Statement 28.).

[its] policies in a variety of ways.” On the contrary, Facebook: (i) had authorized Kogan and his affiliated companies to sell user data to third parties in direct violation of the terms of service posted on Facebook’s website; (ii) had taken no action against Kogan or other malicious actors upon learning that user data had been compromised in violation of the terms of service; (iii) had waited six months before asking Cambridge Analytica and other entities to certify that all user data had been destroyed; and (iv) had made no effort—either themselves, or in concert with government bodies—to identify what data had been compromised from what users, or to notify users who had been, or were at risk of being, targeted.

655. Further, the statements set forth above were materially false and misleading because they omitted the following material facts necessary in order to make those statements, in light of the circumstances under which they were made, not misleading: (i) the Company had knowingly or recklessly allowed third parties other than Cambridge Analytica and its affiliates to harvest and misuse users’ data without their knowledge or consent; (ii) Facebook had taken no action against those other malicious actors upon learning that user data had been compromised in violation of Facebook’s terms of service; (iii) Facebook had waited six months before asking Cambridge Analytica and other entities to certify that all user data had been destroyed and then failed to take any steps to confirm destruction; (iv) Facebook had made no effort to identify what data had been compromised from what users; (v) Facebook had violated the FTC Consent Decree; (vi) Facebook had made no effort to notify users that Cambridge Analytica or the other app developers had, without users’ knowledge or consent, collected and still possessed vast amounts of Facebook users’ friends’ personal data; and

(vii) a major risk to Facebook's business model, finances and reputation existed.

4. Statements on Facebook's April 4, 2018 Telephonic Press Conference

656. On April 4, 2018, Zuckerberg conducted a telephonic press conference, which was transcribed and posted on Facebook's website under the title "Hard Questions: Q&A With Mark Zuckerberg on Protecting People's Information." During this press conference, he stated in part:⁶⁵³

For Facebook specifically, one of the things we need to do and that I hope that more people look at are just the privacy controls that you have. I think, especially leading up to the GDPR event, a lot of people are asking us, "Okay, are you going to implement all those things?" *And my answer is that we've had almost all of what's in there implemented for years, around the world, not just in Europe. So, to me, the fact that a lot of people might not be aware of that is an issue, and I think we could do a better job of putting these tools in front of people and not just offering them*, and I would encourage people to use them and make sure that they're comfortable with how their information is used on our services and others.

657. The above statement was materially false and misleading because it sought to assure investors that data breaches like the Cambridge Analytica scandal were behind the Company and the consequences of that breach would be minimal because Facebook had been protecting

⁶⁵³ *Hard Questions: Q&A With Mark Zuckerberg on Protecting People's Information*, Facebook Newsroom (Apr. 4, 2018) (The MTD Order identified this statement as Statement 32.).

privacy for years—when, in reality, Facebook had not been protecting privacy and the consequences of Facebook’s data protection misconduct would not be fully revealed until July 25, 2018, when Facebook disclosed, *inter alia*, heightened privacy-related expenses and declining active user figures. Further, Zuckerberg’s statement that “we’ve had almost all of what’s in [the GDPR] implemented for years, around the world,” misleadingly sought to assure investors that Facebook was already adhering to or prepared to meet the requirements of the GDPR, when in reality the Company was not meeting those requirements, which was not fully revealed until July 25, 2018. Defendants’ knowledge or reckless disregard that these statements would be, and were, misleading to investors may be inferred from the same facts that support a strong inference of scienter with respect to the assurances about Facebook’s purported commitment to enforcement of its privacy policies.

658. The foregoing statements were also materially false and misleading because they omitted the following material facts necessary in order to make those statements, in light of the circumstances under which they were made, not misleading: (i) Facebook had violated the FTC Consent Decree; (ii) Facebook’s misconduct with respect to user privacy would impact the Company’s bottom line by destroying its reputation as a company that protected privacy and by requiring the Company to incur billions in expenses to become privacy compliant, including with respect to the GDPR; and (iii) as a result, Facebook’s user numbers, revenue growth, operating margins and business prospects would materially decline.

VII. Additional Scierer Allegations

659. The facts detailed above, when viewed collectively and holistically and together with the other allegations in this Complaint, establish a strong inference that each of the defendants knew or were deliberately reckless that each of the misrepresentations and omissions set forth above would be, and were, misleading to investors at the time they were made.

660. Each of the defendants knew or recklessly disregarded that their statements concerning privacy risks and the Cambridge Analytica breach were or would be misleading to investors at the time they were made because, as previously alleged, at the time the foregoing statements were made, each of the defendants knew or recklessly disregarded, *inter alia*, that: (a) Facebook user data had been provided to Cambridge Analytica in violation of Facebook's terms of use; (b) Facebook had done nothing to investigate the scope of the breach or require destruction of the user data at the time it learned of the breach; (c) Facebook acted only after the risks of exposure had increased as a result of Cambridge Analytica's participation in events leading to the Brexit vote; (d) defendants had deliberately decided **not** to notify affected users that their data had been compromised; (e) the certification obtained from SCL was unreliable to reasonably assure that user data had in fact been deleted; (f) Facebook's lax historic privacy practices had given rise to numerous other risks of user data being compromised, such that the Cambridge Analytica data breach was not an isolated event; and (g) Facebook was continuing to share user data without authorization and in violation of its stated policies.

661. Defendants' scierer may be further inferred from other facts alleged herein, including that: (a) GSR

Founder Chancellor, who had detailed knowledge about Cambridge Analytica's access to and use of the user data had been hired by Facebook around the time it learned of the data breach, and was still working in its headquarters at the time the foregoing statements were made; (b) defendants had been repeatedly warned of the concealed risks to the Company arising from its lax privacy practices, including by McNamee, Parakilas and others; (c) defendants knew that providing truthful, accurate and complete disclosures would threaten their business model, as it would expose users to information that was likely to dissuade them from actively engaging on Facebook's social media platforms; (d) defendants' close attention to user engagement metrics, and the critical importance of those metrics to Facebook's business model and financial success; (e) the Company had a long history of internally disregarding privacy rights of users, and acting in ways that contradicted its public assurances to users; and (f) Facebook was subject to an FTC Consent Decree at the time the statements were made, providing defendants with heightened awareness of the risks of and their responsibilities with respect to violating user privacy rights.

662. In addition, defendants' scienter can be inferred from the stark contrast between their disinterest in protecting users' privacy and the aggressive tack they took and take in protecting their own, in particular when it came to negotiating and enforcing the Company's confidentiality and non-disclosure agreements. Kogan, who refused to respond to a number of questions asked of him by members of the U.K. parliament for fear that doing so would violate the agreement he signed with Facebook, was typical. ¶¶212-214, *supra*. As reported by *Bloomberg*, Facebook has a well-earned reputation for "searching for leakers" and negatively influencing their ability to find

employment elsewhere in Silicon Valley.⁶⁵⁴ Indeed, Zuckerberg has reportedly announced at all-hands meetings the firing of employees for leaking, often to applause from other employees.⁶⁵⁵ Consistent with these Facebook practices, counsel for plaintiffs, in investigating the allegations contained in this complaint, have contacted dozens of witnesses otherwise inclined to be interviewed who declined to provide information based on their fear either that they would be prosecuted by Facebook for violating the terms of a non-disclosure agreement with the Company, or subject to retaliation from Facebook in seeking employment, or both.

663. Defendants' massive stock sales during the Class Period provide additional strong evidence in support of an inference of scienter, in that they further demonstrate how each of the defendants had a direct, substantial pecuniary motive to conceal the true facts from investors and users, so as to enable defendants to sell their personal shares of Facebook stock at prices that were inflated by fraud.

664. In 2015, defendant Zuckerberg learned that Cambridge Analytica was misusing Facebook users' personal data. Defendant Zuckerberg has admitted to possessing knowledge of this nonpublic information. In a recent March 21, 2018 Facebook post, he admitted that "[i]n 2015, we learned from journalists at *The Guardian* that Kogan had shared data from his app with Cambridge Analytica."⁶⁵⁶ Likewise, in a March 21, 2018 interview with

⁶⁵⁴ Bloomberg, Decrypted podcast, *Facebook's Former Employees Open Up About the Data Scandal* (Mar. 29, 2018) (starting at minute 2).

⁶⁵⁵ *Id.*

⁶⁵⁶ Mark Zuckerberg, Facebook (Mar. 21, 2018).

Wired, he admitted that “in 2015, . . . we heard from journalists at *The Guardian* that Aleksandr Kogan seemed to have shared data with Cambridge Analytica and a few other parties.”⁶⁵⁷ Sandberg similarly admitted in a recent April 6, 2018 interview with the Today show that Facebook was aware as early as November 2015 that Kogan shared users’ data with Cambridge Analytica, stating: “You are right that we could have done these two and a half years ago. . . . [W]e thought that the data had been deleted and we should have checked.”⁶⁵⁸

665. At the same time in December 2015 that *The Guardian* told Facebook that Cambridge Analytica had illegally provided Facebook user data to third parties, defendant Zuckerberg began the process of disposing of billions of dollars of his Facebook shares through a limited liability company that he controls and created in December 2015 called Chan Zuckerberg Initiative, LLC (“CZI”). On December 22, 2015, eleven days after *The Guardian* published its article, defendant Zuckerberg transferred over 414 million of his Facebook shares-valued at about \$45 billion at the time of the transfer-to CZI. Defendant Zuckerberg retained complete control over CZI’s ability to dispose of the transferred shares.

666. Over the ensuing months, defendant Zuckerberg proceeded to unload over 29.4 million Facebook shares for nearly \$5.3 billion dollars. During the year that preceded the eventual revelation that Facebook failed to safeguard its users’ data, defendant Zuckerberg sold over 10.1 mil-

⁶⁵⁷ Nicholas Thompson, *Mark Zuckerberg Talks to Wired about Facebook’s Privacy Problem*, *Wired* (Mar. 21, 2018).

⁶⁵⁸ Eun Kyung Kim, *Sheryl Sandberg on TODAY: Other Facebook data breaches ‘possible’*, *Today* (Apr. 6, 2018).

lion of his personal Facebook shares, collecting \$1.74 billion in profits. As the financial press has since noted, defendant Zuckerberg unloaded more shares “than any insider at any other company”⁶⁵⁹ in the months preceding the revelations of Facebook’s misconduct. Indeed, within the one month preceding the March 17, 2018 revelations, defendant Zuckerberg sold over \$780 million in Facebook stock.

667. Defendant Sandberg also sold large amounts of her personally-held Facebook shares during the Class Period prior to the revelation of Facebook’s data security breach. In total, defendant Sandberg sold over **2.2 million** shares of Facebook stock between February 3, 2017 and March 23, 2018, collecting **over \$318 million** for these sales.

668. As the financial press has observed, during the months preceding Facebook’s disclosure of its data security breach, “[Facebook] executives [were] selling shares like crazy.”⁶⁶⁰ During the three-month window prior to the disclosure of the data security breach alone, Zuckerberg sold more stock “than any insider at any other company.”⁶⁶¹ In fact, Zuckerberg **sold twice as much stock** during the Class Period as compared to the same amount of time preceding the Class Period. Meanwhile, Zuckerberg did not buy **any** shares during the Class Period. As noted in news reports, Sandberg’s sales of her personal

⁶⁵⁹ Evelyn Cheng, *Zuckerberg has sold more Facebook stock in the last 3 months than any insider at any other Company*, CNBC (Mar. 20, 2018).

⁶⁶⁰ Matt Rosoff, *Facebook is facing its biggest test ever—and its lack of leadership could sink the company*, CNBC (Mar. 18, 2018).

⁶⁶¹ Evelyn Cheng, *Zuckerberg has sold more Facebook stock in the last 3 months than any insider at any other Company*, CNBC (Mar. 20, 2018).

stock, while less than defendant Zuckerberg, “is still unusually large among officers of top tech companies.”⁶⁶²

669. *CNBC* reported that in the first quarter of 2018, “as Facebook struggled with data leaks and fake news scandals, insiders at the company were selling more stock than they typically do,” and that in the “second quarter, top executives sold 13.6 million shares, up from 8.3 million in the first quarter, and roughly *triple the amount* they sold in the last quarter of 2017.”⁶⁶³ Facebook’s SEC filings corroborate these reports and reveal suspicious trading by each of the Executive Defendants.

A. Zuckerberg’s \$5.3 Billion Aggregate Sales

670. During the February 27, 2017 to July 25, 2018 period, Zuckerberg sold over **\$5.3 billion** worth of Facebook stock. Zuckerberg sold this stock out of an investment vehicle that he controls and created in December 2015, when he transferred 99% of his Facebook stock to the vehicle. He publicly proclaimed that the purpose of the vehicle was charitable but the limited liability company structure does not require the vehicle to spend “a minimum of 5 percent of the value of their endowment every year for charitable purposes”⁶⁶⁴ as typical nonprofits require. When Facebook reported to investors information about this new private investment vehicle in December 2015, the Company confirmed that Zuckerberg would “control the voting and disposition of any shares held by such entity.”⁶⁶⁵ Thus,

⁶⁶² Matt Rosoff, *Facebook is facing its biggest test ever—and its lack of leadership could sink the company*, *CNBC* (Mar. 18, 2018).

⁶⁶³ Kate Rooney, *Facebook insiders sold more stock than usual in the second quarter*, *CNBC* (July 26, 2018).

⁶⁶⁴ Natasha Singer and Mike Isaac, *Mark Zuckerberg’s Philanthropy Uses L.L.C. for More Control*, *N.Y. Times* (Dec. 2, 2015).

⁶⁶⁵ Facebook, Inc. Form 8-K (Dec. 1, 2015).

Zuckerberg “remains completely free to do as he wishes”⁶⁶⁶ with the proceeds from his Class Period stock sales as a result.

671. When Zuckerberg created his investment vehicle in December 2015, Facebook reported that he told the Company the amount of stock he planned to sell into the open market. In particular, Facebook reported that Zuckerberg told the Company that “he *plan[ned]* to sell or gift *no more* than \$1 billion of Facebook stock each year for the next three years and that he intends to retain his majority voting position in our stock for the foreseeable future.”⁶⁶⁷ Zuckerberg had already created the investment vehicle on or about December 1, 2015, when Facebook reported the news to investors. The first reports of the Cambridge Analytica scandal surfaced in late December 2015 and, after that time but before the scandal surfaced, Zuckerberg changed his original plan to sell \$3 billion.⁶⁶⁸

672. In fact, Zuckerberg’s Class Period sales of **\$5.3 billion** are **55% higher** than the \$3 billion plan that the Company reported on December 1, 2015 when Zuckerberg created his first plan. He sold **\$2 billion** in stock (or 11.9 million shares) during the February 27, 2017 to March 23, 2018 period that preceded *The Guardian* and *The New York Times* reports regarding the Cambridge Analytica scandal and Facebook’s attendant inability to

⁶⁶⁶ Jesse Eisinger, Pro Publica, *How Mark Zuckerberg’s Altruism Helps Himself*, N.Y. Times (Dec. 3, 2015).

⁶⁶⁷ Facebook, Inc. Form 8-K (Dec. 1, 2015).

⁶⁶⁸ Zuckerberg publicly reported a change in his plan on or about September 22, 2017. See Facebook, Inc. Form 8-K (Sept. 27, 2017). (“On September 22, 2017, Mr. Zuckerberg announced that he anticipates selling 35 million to 75 million shares of Facebook stock over approximately 18 months from the date of this report . . .”).

safeguard its users' personal information. Once that news surfaced, Zuckerberg and his team minimized the problem, "pumping" Facebook's stock price higher during the March—July 2018 period. During that time Zuckerberg "dumped" over 7.7 million shares for proceeds of more than **\$3.3 billion** before the July 25, 2018 investor call when he and others at Facebook shocked the markets with the news that Facebook had essentially ended its ability to grow in light of the business changes that the Cambridge Analytica scandal precipitated.

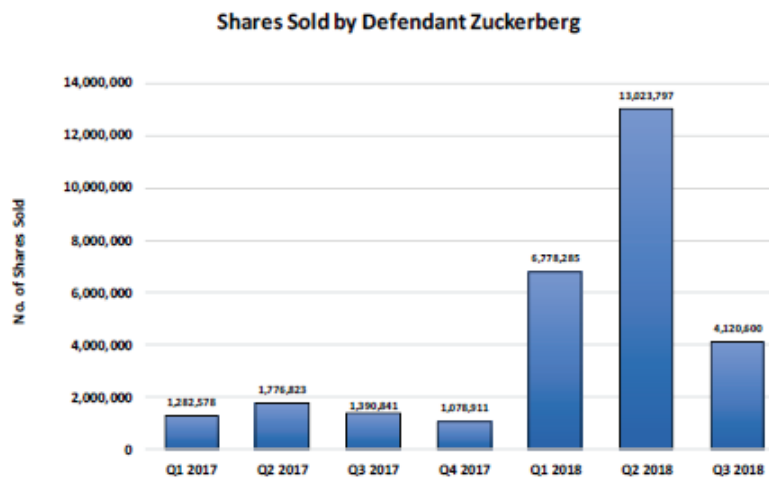
673. Zuckerberg's suspicious sales immediately preceding the March 2018 revelations, along with the financial benefits that he garnered in minimizing that news before the Company's July 2018 investor are clear. After the March 18, 2018 disclosure, defendant Zuckerberg assured investors that Facebook was taking appropriate steps to ensure that users' privacy was being protected and that the breach would have only a negligible impact on users' engagement on the Facebook platform. During that same time, defendant Zuckerberg continued to unload his Facebook shares. Specifically, between March 18, 2018 and the July 25, 2018 investor call, defendant Zuckerberg sold \$3.45 billion of Facebook stock (18.5 million shares). As the financial press has since reported, defendant Zuckerberg again continued to "sell[] more stock than [he] typically d[id]" during this period, selling in the second quarter of 2018 "double what he sold in the first quarter" of 2018 and "10 times what he sold in the fourth quarter" of 2017.⁶⁶⁹

674. Defendant Zuckerberg's trading during the Class Period dramatically departed from his prior trading

⁶⁶⁹ Kate Rooney, *Facebook insiders sold more stock than usual in the second quarter*, CNBC (July 26, 2018).

activity, as he sold three times more stock during the Class Period than he did for the same period preceding the Class Period. Strikingly, during the Class Period while he was in possession of material nonpublic information, defendant Zuckerberg did not buy a single Facebook share.

675. As the following charts show, Zuckerberg's quarterly insider sales during the Class Period dwarf his prior sales,



both in the dollar amount of the sales and in the number of shares sold:

676. Further, Zuckerberg engaged in random patterns of selling during the first part of the Class Period in 2017—selling only twice in February, six times in March, twice in April, four times in May, six times in June, twice in July, four times in August, five times in September, three times in October, four times in November and twice in December. Then, in March 2018, he rapidly accelerated

his trading to sell shares *every single trading day possible* until July 25, 2018—when the bottom dropped out on the stock price.

677. Finally, in the fourth quarter of 2018, Zuckerberg did not sell a single share. As noted by Bloomberg reporters, this was “the first quarter in more than two years [that Zuckerberg has] refrained from doing so.”⁶⁷⁰ The reasons are obvious, he capitalized on the artificially inflated price of Facebook’s stock prior to the July 25, 2018 corrective disclosure—and then stopped selling when the price was low.

B. Sandberg’s \$389 Million Insider Sales

678. Defendant Sandberg also dumped massive amounts Facebook stock during the Class Period. She sold **\$389 million** worth of Facebook stock throughout this time, and, like Zuckerberg, was in a position to control the timing of the true extent of Facebook’s underlying business problems with regard to the way that it treated users’ information. During the nearly one-year period from February 16, 2017 to March 15, 2018, Sandberg sold over 1.5 million shares more than \$270 million in proceeds. Similar to Zuckerberg’s rosy statements to the market after *The Guardian* and *The New York Times* stories surfaced in late March 2018, Sandberg also issued favorable statements that increased the stock’s price before the July 2018 earnings call. During the three and a half-month period from March 30, 2017 to July 19, 2018, Sandberg sold over 411 thousand shares for \$75 million in proceeds. In all, she unloaded over 2.5 million shares for more than \$389 million:

⁶⁷⁰ Anders Melin and Brandon Kochkodin, *Mark Zuckerberg Halts Stock Sales as Facebook Shares Tumble*, Bloomberg (Jan. 3, 2019).

Sale Date	Price	Shares Sold	Proceeds
2/16/2017	\$133.39	327,000	\$43,618,530
2/28/2017	\$135.58	158,534	\$21,494,040
2/28/2017	\$136.15	88,190	\$12,007,069
2/28/2017	\$136.16	80,276	\$10,930,380
3/15/2017	\$139.02	115,258	\$16,023,167
3/15/2017	\$139.03	108,469	\$15,080,445
3/15/2017	\$139.77	54,530	\$7,621,658
3/15/2017	\$139.78	48,743	\$6,813,297
3/30/2017	\$140.37	141,490	\$19,860,951
3/30/2017	\$142.41	130,910	\$18,642,893
3/30/2017	\$142.90	100	\$14,290
4/18/2017	\$141.20	66,306	\$9,362,407
4/18/2017	\$141.22	77,194	\$10,901,337
4/18/2017	\$141.73	12,300	\$1,743,279
4/18/2017	\$141.77	7,700	\$1,091,629
5/11/2017	\$149.92	159,470	\$23,907,742
5/11/2017	\$150.51	2,200	\$331,122
5/11/2017	\$150.53	1,830	\$275,470
5/24/2017	\$149.22	39,232	\$5,854,199
5/24/2017	\$149.23	37,675	\$5,622,240
5/24/2017	\$149.83	45,662	\$6,841,537
5/24/2017	\$149.84	40,931	\$6,133,101
6/6/2017	\$152.99	19,006	\$2,907,728

Sale Date	Price	Shares Sold	Proceeds
6/6/2017	\$153.00	20,894	\$3,196,782
6/6/2017	\$153.98	123,600	\$19,031,928
6/19/2017	\$152.47	41,899	\$6,388,341
6/19/2017	\$152.50	48,564	\$7,406,010
6/19/2017	\$153.01	21,315	\$3,261,408
6/19/2017	\$153.04	19,722	\$3,018,255
2/14/2018	\$173.46	1,900	\$329,574
2/14/2018	\$174.97	10,900	\$1,907,173
2/14/2018	\$176.54	6,300	\$1,112,202
2/14/2018	\$177.14	12,525	\$2,218,679
2/14/2018	\$178.32	10,500	\$1,872,360
2/14/2018	\$179.32	12,875	\$2,308,745
3/2/2018	\$173.62	18,200	\$3,159,884
3/2/2018	\$174.51	11,080	\$1,933,571
3/2/2018	\$175.49	22,236	\$3,902,196
3/2/2018	\$176.48	3,484	\$614,856
3/15/2018	\$182.79	28,866	\$5,276,416
3/15/2018	\$183.51	26,134	\$4,795,850
4/2/2018	\$154.95	16,870	\$2,614,007
4/2/2018	\$155.60	20,620	\$3,208,472
4/2/2018	\$156.67	11,610	\$1,818,939
4/2/2018	\$157.65	3,500	\$551,775
4/2/2018	\$158.54	2,400	\$380,496

Sale Date	Price	Shares Sold	Proceeds
4/18/2018	\$166.66	40,261	\$6,709,898
4/18/2018	\$167.32	14,739	\$2,466,129
5/14/2018	\$186.84	43,789	\$8,181,537
5/14/2018	\$187.51	11,211	\$2,102,175
5/30/2018	\$185.88	12,492	\$2,322,013
5/30/2018	\$186.80	5,200	\$971,360
5/30/2018	\$187.72	37,308	\$7,003,458
6/12/2018	\$192.20	46,206	\$8,880,793
6/12/2018	\$192.92	8,794	\$1,696,538
6/28/2018	\$193.94	4,424	\$857,991
6/28/2018	\$194.94	17,172	\$3,347,510
6/28/2018	\$195.79	24,444	\$4,785,891
6/28/2018	\$196.71	8,960	\$1,762,522
7/19/2018	\$208.32	41,078	\$8,557,369
7/19/2018	\$209.16	13,922	\$2,911,926
Totals		2,589,000	\$389,943,538

C. Wehner's \$21 Million Insider Sales

679. Defendant Wehner also unloaded large amounts of Facebook stock during the Class Period, as the following chart demonstrates:

Sale Date	Price	Shares Sold	Proceeds
2/21/2017	\$133.50	6,584	\$878,964
3/1/2017	\$136.50	1,209	\$165,029
3/1/2017	\$136.90	806	\$110,341
4/24/2017	\$144.96	16,008	\$2,320,520
4/28/2017	\$149.90	20,000	\$2,998,000
5/19/2017	\$148.47	15,470	\$2,296,831
8/21/2017	\$167.16	15,470	\$2,585,965
11/21/2017	\$179.05	15,470	\$2,769,904
2/22/2018	\$178.79	14,901	\$2,664,150
5/16/2018	\$183.61	9,522	\$1,748,334
5/21/2018	\$184.90	4,761	\$880,309
6/20/2018	\$199.90	10,000	\$1,999,000
Totals		130,201	\$21,417,346

VIII. Additional Allegations of Reliance, Materiality, Loss Causation and Damages

680. Lead Plaintiffs and other members of the Class suffered damages as a result of the misrepresentations and omissions alleged herein when the circumstances, events and conditions concealed from investors became known to the market, or the risks arising from those circumstances, conditions and events manifested, causing declines in the market price of Facebook common stock, which trades in an efficient market.

A. Market Efficiency

681. Through the efficient operation of the markets in which Facebook common stock was publicly traded, Lead Plaintiffs and the other members of the proposed Class may be presumed to have relied upon each of the false and misleading statements alleged herein.

682. At all relevant times, the market for Facebook's common stock was an efficient market for the following reasons, among others:

(a) Facebook's stock met the requirements for listing, and was listed and actively traded on the NASDAQ Global Select Market, a highly efficient and automated market;

(b) As a regulated issuer, Facebook filed periodic public reports with the SEC and the NASDAQ and was, at all times alleged herein, eligible to file a Form S-3 with the SEC;

(c) Facebook regularly communicated with public investors via established market communication mechanisms, including through regular disseminations of press releases on the national circuits of major newswire services, publications on its website and other Internet sites, and through other wide-ranging public disclosures, such as through conference calls, communications with the financial press and other similar reporting services;

(d) During the Class Period, Facebook was followed by securities analysts employed by major brokerage firms. Analysts employed by each of these firms regularly wrote reports based upon the publicly available information disseminated by defendants about Facebook. These reports were distributed to

the sales force and certain customers of their respective brokerage firms;

(e) Institutions collectively owned more than two-thirds of Facebook's outstanding shares during the Class Period. Each of these institutions regularly analyzed and reported on the publicly available information about Facebook and its operations; and

(f) During the Class Period, the average daily trading volume of Facebook common stock was greater than 20 million shares.

683. Through the foregoing mechanisms, the information publicly disseminated by defendants about the Company and its operations, and the import thereof, became widely available to and was acted upon by investors in the marketplace such that, as a result of their transactions in Facebook stock, the information disseminated by defendants, including the false and misleading statements described above, became incorporated into and were reflected by the market price of Facebook's common stock.

684. Under these circumstances, all purchasers of Facebook's common stock during the Class Period are presumed to have relied upon the false and misleading statements and material omissions alleged herein.

B. Loss Causation and Damages

685. Each member of the proposed Class suffered economic losses as a direct and proximate result of the fraud alleged herein. Each Class member suffered similar injury as a result of: (i) their purchase of Facebook's common stock at prices that were higher than they would have been had defendants made truthful and complete disclosures of information about the Company as necessary to prevent the statements, omissions and course of

business alleged herein from being materially false or misleading to investors; and (ii) their retention of those shares through the date of one or more declines in the market price of those shares that was caused by the revelation of defendants' misrepresentations and omissions and the risks concealed from investors by defendants' scheme to defraud, or the financial consequences of their concealed actions.

686. The misrepresentations and omissions alleged herein impacted the public trading price for Facebook's common stock by causing it to trade at a price higher than it would have had the facts, risks and conditions concealed by defendants' fraud become known sooner than it did. The impact on Facebook's stock price occurred by increasing the trading price of Facebook stock at the time of the misrepresentation or by preventing a price decline that would have occurred at that time with the full disclosure of the truth, or both.

687. The facts, risks and conditions concealed from investors by defendants' scheme to defraud reached the market through a series of partial disclosures. Though each of the disclosures was incomplete, each revealed some of the falsity of defendants' statements regarding user control over data, the Cambridge Analytica matter, and other elements of defendants' fraud alleged herein, including the concealed materialization of risks to its operations, leading to price declines that partially corrected Facebook's stock price by reducing the extent to which it had been inflated by defendants' fraud scheme, thereby injuring Lead Plaintiffs and other members of the Class who had purchased Facebook securities during the Class Period at prices that had been artificially inflated by the fraudulent course of business and misleading statements and omissions alleged herein.

688. The disclosures that impacted the price of Facebook’s common stock include those identified in the chart below, which identifies each event, the change in Facebook’s stock price on the day of the event, and, for purposes of comparison, the percentage change during the same time period in the Standard & Poor’s 500 Stock Index (“S&P 500”), one of the market indices to which Facebook compares its stock performance in its annual reports to the SEC:

Date	Event ⁶⁷¹	Facebook		S&P 500 ⁶⁷²
		\$ Δ	% Δ	% Δ
3/19/18	<i>NYT & Guardian</i> reports	(\$12.53)	(6.8%)	(1.4%)
3/20/18		(\$4.41)	(2.6%)	0.15%

⁶⁷¹ In some cases, the identified event occurred after the market closed on the preceding trading day but prior to the date indicated in the chart, which is the date of the relevant price decline. The list of events identified herein is necessarily preliminary, and based upon Lead Plaintiffs’ analysis and investigation to date. Upon further investigation and discovery and additional analysis, Lead Plaintiffs may change, alter or amend their theory of damages, including by identifying different or additional inflationary and corrective events that caused or contributed to the damages claimed in this action, or by using other industry indices or competitor stock price data to more precisely establish the magnitude of the Company-specific change arising from those events.

⁶⁷² The chart indicates the percentage change in the S&P 500 Index as a whole. Part of the change in the index price therefore reflects the change in the price of Facebook stock, which represents a significant portion of the index. As a result, the company-specific portion of the price changes reflected in the chart is actually greater than indicated by a simple comparison of Facebook’s price change to the change in the market index.

3/22/18	Continuing revelations of extent of data breach and lax enforcement, and of regulatory and user backlash	(\$4.50)	(2.7%)	(2.5%)
3/23/18		(\$5.50)	(3.3%)	(2.1%)
3/27/18		(\$7.84)	(4.9%)	(1.7%)
4/26/18	1Q18 Earnings Release	\$14.47	9.1%	1.0%
7/26/18	2Q18 Earnings Release	(\$41.24)	(19.0%)	(0.3%)

689. On Monday, March 19, 2018, following the numerous disclosures over the preceding weekend regarding the misuse of Facebook user data and lack of user control—including the press release issued by Facebook after the market closed on Friday, March 16, 2018 and the articles published by *The New York Times* and *The Guardian* on Saturday, March 17, 2018—caused the price of Facebook common stock to decline. See ¶[[373]]. The shares opened at \$177.01—a 4.4% decline from the previous Friday’s closing price. Over the course of the day, as additional news regarding the extent of the data breach emerged, Facebook’s stock continued to decline. Facebook closed at \$172.56, a 6.8% decline from the prior Friday’s closing price on volume of 88 million shares, more than four times the average trading volume during the Class Period.

690. The news regarding Cambridge Analytica’s continued possession and misuse of the personal data of tens of millions of Facebook users that emerged over the

March 16-17, 2018 weekend partially revealed Defendants' Class Period representations set forth above to be materially false and misleading.

691. For example, contrary to Defendants' Class Period representations concerning control over user data and Facebook respecting user privacy, this news revealed that Facebook could not ensure that users controlled their data or had privacy with respect to data accessed by third parties on the Facebook platform. Indeed, the March 17, 2018 article in *The New York Times* expressly linked the news to issues of data control, stating, for example, that "copies of the data still remain beyond Facebook's control" and noting that *The Times* even "viewed a set of raw data from the profiles Cambridge Analytica obtained."⁶⁷³

692. Likewise, Facebook's *own* March 16, 2018 website statements announcing the suspension of Cambridge Analytica and SCL Group drew a direct link to issues of user control. For example, Facebook assured the public that a massive loss of data control like what happened with Cambridge Analytica could not happen again, stating, "[i]n 2014 . . . we made an update to ensure that each person decides what information they want to share about themselves, including their friend list," which "is just one of the many ways we give people the tools to **control their experience**" (emphasis in Facebook's original).⁶⁷⁴

693. The press also expressly linked the March 2018 news concerning Cambridge Analytica to the revelation of a lack of control over Facebook user data. For example,

⁶⁷³ Matthew Rosenberg, Nicholas Confessore & Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. Times (Mar. 17, 2018).

⁶⁷⁴ Paul Grewal, *Suspending Cambridge Analytica and SCL Group From Facebook*, Facebook Newsroom (Mar. 16, 2018).

a March 19, 2018 article in the *Los Angeles Times* noted that Facebook “bushwhacked” the public by promising that users “own all of the content and information [that they] post on Facebook, and [users] can control how it is shared”—when “[t]he reality is: [user] data belong[s] to Facebook, and the company will enrich itself by doing with it whatever it pleases.”⁶⁷⁵

694. The March 16-17, 2018 news also exposed several other categories of Defendants’ Class Period statements as false and misleading. Indeed, this news revealed that, *inter alia*, Defendants’ risk statements were misleading because, in reality and contrary to these statements, improper access, disclosure and misuse of user data were not merely hypothetical investment risks. In fact, Facebook had suffered a significant episode of misuse of user data by an app developer. The news also revealed the following statements to be materially misleading:⁶⁷⁶

(a) Defendants’ statements about not “uncovering anything that suggests wrongdoing with respect to Cambridge Analytica’s work on the . . . Trump campaign[]”;

(b) Defendants’ statements about “requiring” data misusers to “destroy all improperly collected data”;

(c) Defendants’ statements about complying with the 2012 FTC Consent Decree; and

⁶⁷⁵ David Lazarus, *Column: Facebook says you ‘own’ all the data you post. Not even close, say privacy experts*, *Los Angeles Times* (Mar. 19, 2018).

⁶⁷⁶ See Mark DeCambre & Emily Bary, *Facebook sheds nearly \$40 billion of market cap as investors flee stock*, *MarketWatch* (Mar. 19, 2018).

(d) Defendants' statements about notifying Facebook users whose accounts were compromised or at risk of being compromised.

695. Further, market commentators also noted the "current unknowns around FB shares," which were identified as: "1) negative impact to user growth and engagement, and 2) the potential for regulatory activity and/or scrutiny."

696. The price of Facebook common stock continued to decline thereafter as a result of additional disclosures of material information regarding the lack of user control over their data on the Facebook platform, the extent of the Cambridge Analytica data misuse, Facebook's misrepresentations about its response to the Cambridge Analytica data misuse, and the magnitude of the risks facing the Company. By the close of the market on March 27, 2018, the price of Facebook common stock had declined to \$152.22 as a result of such disclosures, completing a stunning 17.8% (\$32.87) decline in the price of its shares immediately before Facebook's failure to retrieve user data from Cambridge Analytica and other third parties was disclosed. Following are just some of the disclosures that caused Facebook's stock price to decline.⁶⁷⁷

On March 18, 2018, Wylie tweeted that he had been "Suspended by @facebook. For blowing the whistle. ***On something they have known privately for 2 years***";⁶⁷⁸

On March 19, 2018, The New York Times reported that Facebook's Chief Information Security Officer,

⁶⁷⁷ Paul Lewis, *'Utterly Horrifying': ex-Facebook insider says covert data harvesting was routine*, Guardian (Mar. 20, 2018).

⁶⁷⁸ Christopher Wylie (@chrisinsilico), TWITTER (Mar. 18, 2018).

had been forced to resign from the Company in December 2017 as a result of the growing investigations into Facebook’s role in allowing Russian hacking to occur on its platform during the 2016 U.S. presidential election;⁶⁷⁹

On March 20, 2018, The Guardian reported that app developers routinely practiced data harvesting using the Facebook platform, and, as a result, data from hundreds of millions of users was at risk of being exploited through tactics similar to Cambridge Analytica’s. This news, and additional disclosures regarding the widening scope of the data privacy risks, including calls for users to “#deleteFacebook” and unconfirmed reports of government investigations into the matter, caused the Company’s stock price to fall further, closing at \$168.15, a further 2.6% decline in the value of Facebook shares; and

Also on March 20, 2018, The Guardian reported that Parakilas—the platform operations manager responsible for policing access to Facebook data in 2011 and 2012—had stated that Facebook’s lax data use policies had likely been exploited by numerous other app developers, putting the data of hundreds of millions more Facebook users at risk.

697. On March 21, 2018, Zuckerberg and Sandberg began conducting media interviews designed to assure investors, users and the public that defendants were taking responsibility for their actions, were doing everything they could to correct the problem, and that Cambridge

⁶⁷⁹ Nicole Perlroth, Sheera Frenkel & Scott Shane, *Facebook Exit Hint at Dissent on Handling of Russian Trolls*, N.Y. Times (Mar. 19, 2018).

Analytica had deceived them into believing that it had destroyed the purloined user data in 2015. As a result of defendants' public relations campaign, the decline in Facebook's share price was temporarily halted, and Facebook's stock closed at \$169.39, less than a percentage point higher than its closing price on March 20.

698. However, as additional details emerged concerning the scope of the data breach, the risks facing the Company, and increased calls for government investigations, Facebook's stock price resumed its decline, closing at \$159.39 on Friday, March 23, 2018, completing an overall decline of \$25.70/share (14%) from the closing price the prior Friday before the scandal broke.

699. On March 27, 2018, the price of Facebook common stock fell by \$7.84/share, a 4.9% decline from the prior day's close. This decline was the result of continuing revelations of the lack of user control, the Cambridge Analytica data misuse and the risks to the Company, including the FTC's confirmation that it had opened an investigation into Facebook's compliance with the 2012 FTC Consent Decree.

700. During the period from March 20, 2018 through March 27, 2018, reporters continued to link the news about Cambridge Analytica's continued control and misuse of millions of Facebook users' data directly to the notion that users and even Facebook lacked control over user data. For example:

(a) A March 20, 2018 article published in *The Guardian* quoted Parakilas, Facebook's former platform operations manager: "Asked what kind of control Facebook had over the data given to 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.”⁶⁸⁰

(b) A March 20, 2018 article published by BBC News about the Cambridge Analytica scandal asked: “The bigger question becomes—what does [Facebook] share with others and what can users do to regain control of their information?” According to the article, Dr. Paul Bernal, a lecturer in Information Technology, Intellectual Property and Media Law at the University of East Anglia School of Law, indicated: “There really is only one way to make sure data we create on a daily basis remains entirely private ‘Leave Facebook.’” The article further noted that “the hashtag #DeleteFacebook is now trending on Twitter in the wake of the Cambridge Analytica scandal.”⁶⁸¹

(c) A March 21, 2018 article published by CBS News quoted one academic from the University of Munich, Professor Jens Grossklags, as stating: “Consumers don’t often understand what they are sharing and what controls they are giving up.”⁶⁸²

(d) A March 28, 2018 article published by Reuters titled: “Facebook to change privacy controls in wake of data scandal” stated: “Facebook announced a series of changes on Wednesday [March 28, 2018] to give users more control over their data, after a huge data scandal which has wiped more than \$100 billion

⁶⁸⁰ Paul Lewis, *‘Utterly horrifying’: ex-Facebook insider says covert data harvesting was routine*, Guardian (Mar. 20, 2018).

⁶⁸¹ Jane Wakefield, *Is leaving Facebook the only way to protect your data?*, BBC News (Mar. 20, 2018).

⁶⁸² Aimee Picchi, *Facebook: Your personal info for sale*, CBS News (Mar. 21, 2018).

from its stock market value.”⁶⁸³ This article quoted a blog post from Erin Egan, Facebook’s Vice President and Deputy General Counsel, as stating that Facebook was now “taking additional steps in the coming weeks to put people in more control over their privacy.” The article further noted that “Facebook shares have fallen almost 18 per cent since March 17 [2018]. Users’ data was improperly accessed by British political consultancy Cambridge Analytica, which was hired by Donald Trump’s 2016 presidential campaign.”⁶⁸⁴

(e) A March 28, 2018 article by NPR also commented on the Facebook platform changes in the wake of the news regarding Cambridge Analytica, stating that, “Facebook responded to intensifying criticism over its mishandling of user data Wednesday [March 28, 2018] by announcing new features to its site that will give users more visibility and control over how their information is shared.” This article also noted that angry users have “called for a #DeleteFacebook boycott.”⁶⁸⁵

701. As noted above, Facebook itself conceded by its actions that the Cambridge Analytica scandal concerned user control over data because it responded to the news by announcing new platform features designed to “put people more in *control* of their privacy.”⁶⁸⁶

⁶⁸³ Joseph Menn, *UPDATE 1-Facebook’s security chief to depart, source says*, Reuters (Mar. 19, 2018).

⁶⁸⁴ *Id.*

⁶⁸⁵ Yuki Noguchi, *Facebook Changing Privacy Controls As Criticism Escalates*, NPR (Mar. 28, 2018).

⁶⁸⁶ *It’s Time to Make Our Privacy Tools Easier to Find*, Facebook (Mar. 28, 2018).

702. On April 26, 2018, Facebook’s stock price rocketed upwards by 9% as the Company reported 1Q18 earnings which, together with the statements made by defendants on the earnings call that day, led many analysts and investors to believe that the data breach had only had a negligible impact on user engagement with Facebook’s platform.

703. On June 3, 2018, *The New York Times* published the article discussed above concerning Facebook’s improper whitelisting practices. While there were certain new details in the article, it was not sufficiently distinct from the March 2018 disclosures to trigger a significant sell-off in Facebook stock. At this point in time, Facebook’s stock price already incorporated the March 2018 news relating to Cambridge Analytica, which had revealed the essential facts disclosed in the June 3 article: that users did not have control over their Facebook data or their privacy on the Facebook platform because users did not know that their data was being shared with numerous third parties. For instance, as noted above, on March 20, 2018 the *Guardian* already had reported the account of Facebook insider Parakilas that the Cambridge Analytica scandal was not confined to Cambridge Analytica and “numerous companies” had likely gained control of “hundreds of millions” of Facebook users’ data such that “Parakilas estimates that a ‘majority of Facebook users’ could have had their data harvested by app developers without their knowledge.’”⁶⁸⁷

704. Multiple news reports placed the June 3 article in context as a follow-on to the March 2018 revelations around Cambridge Analytica. For instance, on June 4, 2018, an AP article stated that the June 3 “report taps into

⁶⁸⁷ See also Ex. C at 10.

continuing anxiety about the information users give up—and to whom—when they use Facebook.”⁶⁸⁸ Indeed, the June 4 AP article referenced an April 24, 2018 disclosure by Facebook and noted that: “the company recently said it will end these data-sharing agreements as part of a broader review of its privacy practices *sparked by the Cambridge Analytica* scandal.”⁶⁸⁹ The article further stated that: “These device-maker deals could raise concerns *similar to those in Facebook’s recent Cambridge Analytica* scandal.”

705. A CNN Business report on June 4, 2018 noted that the whitelisting issues “may only add fuel to the fire of existing investigations into Facebook at the state and federal level, including a Federal Trade Commission probe into the company’s data practices.”⁶⁹⁰ Another article that day discussed the June 3 disclosure as one that should have come as no surprise to Facebook users and investors, saying: “Facebook’s attempts to justify its mishandling of user data have become a broken record . . . the company has proven *time and time again* it cannot be trusted to take user privacy seriously . . . the fact remains that its user information has spread far beyond any boundaries the company can control.”⁶⁹¹ A report in *USA Today* noted that “this [June 3] development is the latest in a *series of revelations* on Facebook’s data sharing practices . . . Zuckerberg has apologized for not doing

⁶⁸⁸ Barbara Ortutay, *New Facebook privacy furor: What’s at stake?*, AP News (June 4, 2018).

⁶⁸⁹ *Id.*

⁶⁹⁰ Seth Fiegerman, *Facebook faces new regulatory backlash over data privacy*, CNN Business (June 4, 2018).

⁶⁹¹ Amy Gesenhues, *Facebook faces more scrutiny, this time for sharing user data with device makers*, Marketing Land (June 4, 2018).

enough to protect user data.”⁶⁹² An Axios story similarly noted that the story closely followed the Cambridge Analytica scandal and “*reinforces* the picture of a company that’s been less than forthcoming at key moments.”⁶⁹³

706. Finally, Facebook was successful in downplaying to the market the significance of its whitelisting arrangements, which also prevented a significant sell-off of Facebook stock. On June 4, Facebook published a blog post entitled: “Why We Disagree With *The New York Times*,” in which Facebook reassured the market that its whitelisting arrangements were harmless and falsely insisted that data was not shared without user consent. Facebook claimed in the blog post that it “controlled [the whitelisting arrangements] tightly from the get-go” and that whitelisted entities “signed agreements that prevented people’s Facebook information from being used for any other purpose than to recreate Facebook-like experiences.”⁶⁹⁴ Facebook was also quoted by CNN as saying that *The New York Times* “is wrong about user controls.” The press picked up on these denials by Facebook and reported, for instance, that “it is not clear how the device makers could have abused Facebook even if they wanted to [and] so far there’s no evidence that phone and tablet makers used Facebook data improperly.”⁶⁹⁵

⁶⁹² Ashley Wong, *Facebook gave some developers access to users’ friends after policy changed*, USA Today (June 8, 2018).

⁶⁹³ David McCabe, *Facebook shared friends’ data with third parties beyond cutoff date*, Axios (June 8, 2018).

⁶⁹⁴ Ben Lovejoy, *Apple, Samsung, Microsoft and others given ‘deep access’ to Facebook user data*, 9TO5Mac (June 4, 2018).

⁶⁹⁵ Barbara Ortutay, *New Facebook privacy furor: What’s at stake?*, AP News (June 4, 2018).

707. On July 25, 2018, Facebook announced its earnings for the second quarter of 2018. This was the first full quarter of Facebook results since the Cambridge Analytica data scandal news had surfaced in March 2018. This announcement revealed the true extent of the damage that the revelations about Cambridge Analytica had on Facebook's business and caused Facebook's stock to plummet by nearly 19%—from \$217.50 per share at the close on July 25, 2018 to \$176.26 per share at the close on July 26, 2018. This staggering single-day loss wiped out approximately \$100 billion in shareholder value and, at the time, was the largest such one-day drop in U.S. history. Defendants revealed that the data privacy scandal had caused a far greater impact on the Company than they had previously represented, resulting in dramatically lowered user engagement, substantially decreased advertising revenue and earnings, and reduced growth expectations going forward.

708. For example, on Facebook's July 25, 2018 earnings call, Wehner stated: "we expect our revenue growth rates to decline by high single digit percentages from prior quarters" due to, *inter alia*, Facebook "... giving people who use our services more choices around data privacy, which may have an impact on our revenue growth." This caused significant concern among securities analysts. Indeed, Defendants engaged in the following exchange with a securities analyst from Citigroup:

Mark May: Just following up on the comments. Sheryl [Sandberg] mentioned that there's really no meaningful impact on GDPR to the ad business, at least as of now. But then, Dave, I think you mentioned that because you're giving people more control over their privacy and data, that this is one of the reasons

why you're expecting the meaningful decel [*i.e.*, deceleration] in the second half. Just trying to reconcile those two things. Maybe the questions are—have been too specific around the impact of GDPR and should be more broad around data and privacy. And I guess, ultimately, the question is what impact, if any, is these greater controls that you're giving users having on ad revenue growth and monetization?

David Wehner: Sure, Mark. Let me take that. So GDPR didn't have a significant impact in Q2 partially because of its implementation date. So you're just seeing effectively 1 month of it. In terms of revenue, we do think that there will be some modest impact. And I don't want to overplay these factors, but you've got a couple things going on. You've got the impact of the opt-outs. And while we're very pleased with the vast majority of people opting into the third-party data use, some did not. So that'll have a small impact on revenue growth. And then we're also seeing some impact from how advertisers are using their own data for targeting, so again, that'll have a modest impact on growth. And then in addition, we're continuing to focus our product development around putting privacy first, and that's going to, we believe, have some impact on revenue growth. So it's really a combination of kind of how we're approaching privacy as well as GDPR and the like. So I think all of those factors together are one of the factors that we're talking about

709. As for user engagement declining, Zuckerberg stated: "I also want to talk about privacy. GDPR was an important moment for our industry. We did see a decline in monthly actives [*i.e.*, users] in Europe—down by about 1 million people as a result." This decline was also directly linked to control issues because the GDPR is designed to

provide people with privacy and control over their data. Indeed, Facebook's practice of sharing data with white-listed third parties without knowledge or consent and by overriding privacy controls is a plain violation of the GDPR. So Zuckerberg's admission that GDPR resulted in a decline in active users in Europe is an acknowledgment that providing users with the ability to control their data caused this decline in user engagement.

710. The decline in user engagement, advertising revenues, and guidance for the remainder of the year—alongside the increased spending that Facebook was required to undertake to protect user data from being exploited—were the result of defendants' concealment of the risks arising from the Cambridge Analytica data breach; defendants' false assurances about the adequacy of the Company's prior response to that incident; and the adequacy of the measures that defendants imposed to prevent similar events from occurring in the future or to curtail the harm if they did.

711. Facebook's quarterly results were a direct and proximate result of the concealed problems with the Company's decision to grow at the expense of protecting user privacy. The Company's costs ballooned to \$7.4 billion, a 50% increase from the prior year. Much of the increase resulted from measures imposed to protect user data from exploitation, including to provide the level of protection that the Company had previously, and falsely, asserted it was already providing. Capital expenditures similarly rose 133% from the prior year, reflecting spending on infrastructure necessary to render Facebook's services safe for users.

712. Investors and analysts explicitly connected the historic decline in Facebook's market capitalization to the Cambridge Analytica scandal—and Facebook's response

to the scandal by giving users more control, as well as related privacy concerns, including the recent implementation of GDPR in Europe, that had shaken the Company over the previous months.

713. For instance, on July 26, 2018, CFRA issued a report noting, “[w]e lower our EPS estimates for 2018 to \$7.29 from \$7.42 and 2019 to \$8.24 from \$8.63, given what we see as FB’s *efforts to invest significantly to respond to the Cambridge Analytica revelations*.”⁶⁹⁶ Cowen similarly noted that the decline in advertising revenue that Facebook was bringing in was driven in part by “*privacy via features that could reduce ad targeting capabilities* (like clearing user history) and GDPR impact on users in Europe (as some users don’t opt in for tracking usage).”⁶⁹⁷ Wells Fargo noted its concern over the negative impact “*of the continued efforts around security and privacy*, both from the standpoint of GDPR implementation as well as new services and controls that offer more ways for users to opt out of ads,” and its report also mentioned the magnitude of the “*Security & Privacy efforts*” that Facebook was now being forced to impose.⁶⁹⁸

714. Additionally, J.P. Morgan’s report on July 26, 2018, stated: “FB is seeing some headwinds from data & privacy related issues. On the user front, FB MAUs in Europe declined 1M Q/Q and DAUs dropped 3M from 282M in 1Q18 to 279M in 2Q18 as DAU/MAU fell 60bps

⁶⁹⁶ Scott Kessler, *CFRA Reiterates Hold Opinion on Shares of Facebook, Inc.*, CFRA (July 26, 2018).

⁶⁹⁷ John Blackledge, Nick Yako, et al., *2Q18 Results: 2H18 Ad Rev Decel and L-T Margin Forecast Worse Than Expected*, Cowen (July 26, 2018).

⁶⁹⁸ Ken Sena, Peter Stabler, et al., *FB: Coming Up Against Scale*, Wells Fargo Securities (July 25, 2018).

Q/Q. Europe also saw more significant revenue deceleration than other geos. ***While part of the revenue impact was due to FX, we believe FB likely felt data & privacy issues more in Europe, with some early impact from GDPR in terms of both users & monetization.*** For 2H18, FB also called out privacy as likely to drag on revenue growth. FB is giving users more choices around privacy & how their data is used, & we believe advertisers are also being more cautious around targeting consumers.”⁶⁹⁹

715. Macquarie’s analysts similarly described their “concerns re LT trends/headlines are forcing significant changes to user privacy/data concerns. In 3Q, we expect that users globally may be offered options that go well beyond GDPR changes. Such changes are likely a key driver of the 4Q revenue guidance.”⁷⁰⁰

716. Barclays issued a research report titled “FB Throws Some Napalm on the Fire” that described:⁷⁰¹

⁶⁹⁹ Doug Anmuth, Ashwin Kesireddy, et al., *Major Reset Stories & Data/Privacy Drag on N-T Revs Heavy Investments Continue; Remain OW, PT to \$205 Dropping from AFL*, J.P. Morgan (July 26, 2018).

⁷⁰⁰ Benjamin Schachter, Ed Alter & Angela Newell, *2Q’18 Bombshell Guidance; Structural Shifts*, Macquarie Research (July 26, 2018); see also Shelby Seyrafi, CFA, *FB: Major Guidance Reset, but we Suspect the Company is Conservatively Creating a Lower Bar*, FBN Securities (July 26, 2018) (“Drivers of the deceleration On privacy/GDPR, the data we came across was a bit mixed, but it appears that the negative impact was worse than we had modeled. . . . Moreover, this was with basically a half-quarter’s impact from GDPR, as this was instituted in May.”).

⁷⁰¹ Ross Sandler, Deepak Mathivanan, et al., *FB Throws Some Napalm On The Fire*, Barclays Equity Research (July 26, 2018).

Key Take-Away: Either Core Is Imploding or FB Wants Self-Inflicted Pain

We haven't seen this disastrous a print since the 1Q16 LNKD-massacre that brought the entire NASDAQ down. The two theories we could come up with as to why FB is guiding revenue down severely with 3Q and 4Q now expected to both decelerate high single digits sequentially are: 1) they don't want to create the perception of getting rich while their product presents issues for society (but why didn't this happen on the Jan/April calls?), or 2) ***there are more serious engagement problems with core Facebook that have materialized recently that they are trying to fix.***

717. Journalists and commentators also connected Facebook's earnings report for the second quarter of 2018 to the privacy scandals that had ensnared the Company earlier in the year. For example, CNBC headlined its July 25, 2018 video report on Facebook's earnings miss, "Facebook shares collapse ***as a result of Cambridge Analytica.***"⁷⁰² Bloomberg noted on July 25, 2018, "Facebook Takes Historic Plunge as ***Scandals Finally Take a Toll.***"⁷⁰³ The New York Times similarly headlined its story, "Facebook starts paying a price for scandals."⁷⁰⁴ CNET.com's reporting suggested that the July 2018 stock collapse was the inevitable end-point of the Company's continuing response to the Cambridge Analytica privacy scandal, noting, "Until now . . . there was a sense that the

⁷⁰² Julia Boorstin, *Facebook shares collapse as a result of Cambridge Analytica election scandal*, CNBC (July 25, 2018).

⁷⁰³ Sarah Frier, *Facebook Takes Historic Plunge as Scandals Finally Take a Toll*, Bloomberg (July 25, 2018).

⁷⁰⁴ Sheera Frankel, *Facebook Starts Paying a Price for Scandals*, N.Y. Times (July 25, 2018).

vast majority of users didn't fully understand Facebook's business. But the ongoing scandals have caused many people to take another look."⁷⁰⁵

718. Reporting for *Forbes* in a July 29, 2018 article titled "Profit Versus Privacy: Facebook's Stock Collapse and its Empty 'Privacy First' Policy," Kalev Leetaru described, "At the center of [Facebook's] pessimistic outlook? The *increasing impact of the profit versus privacy battle at the center of the Cambridge Analytica story* and the growing inability of Facebook to control its platform and protect it from harmful misuse."⁷⁰⁶ In *Tech Republic*, James Sanders published a report on that described the "fallout from a confluence of factors in the *Facebook data privacy scandal* has come to bear in the last week of July 2018."⁷⁰⁷ *USA Today* noted that the "Cambridge Analytica scandal [was] one of many reasons for [Facebook's] stock plunge."⁷⁰⁸ And The Washington Post explained, "The cost of years of privacy missteps finally caught up with Facebook this week. . . . Worries about the rising costs of privacy regulations and controversies, along with declining growth in users and revenue played a key role in a major Wall Street sell-off"⁷⁰⁹

⁷⁰⁵ Richard Hieva, *Facebook's bad year just got worse*, CNet.com (July 26, 2018).

⁷⁰⁶ Kalev Leetaru, *Profit Versus Privacy: Facebook's Stock Collapse and its Empty 'Privacy First' Policy*, *Forbes* (July 29, 2018).

⁷⁰⁷ James Sanders, *Facebook data privacy: A cheat sheet*, *Tech Republic* (Sept. 12, 2018).

⁷⁰⁸ Jessica Guynn, *Why Facebook had its worst day is complicated*, *USA Today* (July 28, 2018).

⁷⁰⁹ Craig Timberg and Elizabeth Dwoskin, *How years of privacy controversies finally caught up with Facebook*, *Wash. Post* (July 26, 2018).

719. Overseas, the news reports were comparable. *The Guardian* reported on July 26, 2018, “More than \$119bn (£90.8bn) has been wiped off Facebook’s market value, which includes a \$17bn hit to the fortune of its founder, Mark Zuckerberg, **after the company told investors that user growth had slowed in the wake of the Cambridge Analytica scandal.**”⁷¹⁰ The Independent (U.K.) also headlined an article, “Facebook shares **plummet over privacy scandal** and slow growth in new users.”⁷¹¹

720. Additional analysts, press outlets and other market commentators also linked Facebook’s 2Q18 results and the resulting stock price decline directly to the Cambridge Analytica scandal, the privacy initiatives that Facebook was implementing in order to provide users control over their data in the wake of the Cambridge Analytica scandal, as well as Facebook’s efforts to comply with GDPR, including its imposition of user data control requirements. For example:

(a) On July 25, 2018, an analyst from UBS wrote: “Regulation & Data Privacy—Management expects modest revenue impact from MAU decline (‘opt-outs’) due to regulation & privacy concerns, mainly in Europe (Q2 saw a 3m DAU decline in Europe).”

(b) On July 25, 2018, a Wells Fargo analyst wrote: “The pressures cited [by Facebook on the 2Q18 Earnings Call] were . . . the effects of the continued efforts around security and privacy, both from the standpoint of GDPR implementation as well as new

⁷¹⁰ Rupert Neate, *Over \$119bn wiped off Facebook’s market cap after growth shock*, *Guardian* (July 26, 2018).

⁷¹¹ Tom Embury-Dennis, *Facebook shares plummet over privacy scandal and slow growth in new users*, *Independent* (July 25, 2018).

services and controls that offer more ways for users to opt out of ads. Additionally, on the cost side, the factors cited by magnitude were Security & Privacy efforts (now in the billions per annum)”

(c) On July 25, 2018, a William Blair analyst wrote: “Facebook shares are down about 20% in the after-market, due to a lowered growth and profitability outlook versus Street expectations. On growth, management noted a few factors that will negatively affect growth, including . . . GDPR, privacy changes, and any potential future regulation changes.” William Blair further stated: “Revenue to decelerate meaningfully in the second half of 2018. Management called out three reasons why it expects the company’s year-over-year revenue growth rate to decline sequentially by high single digits in each of the next two quarters . . . [including] New data privacy tools could limit targeting capabilities. This includes the potential impact from GDPR in addition to new tools Facebook has developed that give users more choice around the data that can be shared with advertisers for ad targeting.”

(d) On July 25, 2018, *Investor’s Business Daily* wrote: “Facebook (FB) stock plunged 10% after the company released earnings. But then shares plummeted as much as 23% to 167 during its earnings call commentary. [. . .] Bears pounced on how Europe’s new General Data Protection Regulations, or GDPR, and other consumer data privacy initiatives will impact Facebook’s revenue growth.”⁷¹²

⁷¹² Reinhardt Krause and Brian Deagon, *Facebook Stock Crashes On Earnings Call Warning After Revenue Misses*, *Investor’s Business Daily* (July 25, 2018).

(e) On July 25, 2018, the Australian Broadcasting Corporation wrote: “Facebook stocks have plunged by as much as 24 per cent in after-hours trading due to concerns about the impact of privacy issues on the social media company’s business,” and “[t]he plummeting stock price wiped out about \$US150 billion in the company’s market value in less than two hours.” This report also quoted Morningstar analyst Ali Mogharabi as stating: “[w]hen it comes to much slower revenue growth . . . we think it’s due to slower user growth given GDPR and more focus on privacy.”

(f) On July 25, 2018, *The Verge* wrote: “[o]n an earnings call with investors, Facebook leadership did say that giving users more privacy controls would in the future cut into its advertising revenues . . . it seems as if Facebook is not the untouchable behemoth investors seem to think it is.”⁷¹³

(g) On July 25, 2018, *U.S. News & World Report* noted that Facebook missed analyst expectations concerning monthly active users and daily active users metrics and quoted the COO of FileCloud as stating: “It turns out there is indeed a direct correlation between data privacy scandals and daily active users on Facebook.”⁷¹⁴

(h) On July 26, 2018, *The Guardian* wrote: “Facebook’s shares plunged 19% . . . after the Silicon Valley company revealed that 3 million users in Europe had abandoned the social network since the Observer revealed the Cambridge Analytica breach of

⁷¹³ Nick Statt, *Facebook growth slows in aftermath of privacy scandals*, *The Verge* (July 25, 2018).

⁷¹⁴ John Divine, *Facebook Stock Plunges on Earnings*, *U.S. News & World Report* (July 25, 2018).

87m Facebook profiles and the introduction of strict European Union data protection legislation.” It further stated: “David Wehner, Facebook’s chief financial officer, said on Wednesday [July 25, 2018] that the company’s decision to give its users ‘more choices around data privacy’ following the Cambridge Analytica scandal ‘may have an impact on our revenue growth.’”⁷¹⁵

(i) On July 26, 2018, *Investor’s Business Daily* wrote that Facebook’s 2Q18 earnings results were “the first full quarter of Facebook (FB) results since the Cambridge Analytica data scandal surfaced earlier this year. Analysts raised concerns as to whether the scandal would cause advertisers to slink away or user growth to slow. That appears to be the case to a degree.”⁷¹⁶

(j) On July 28, 2018, *USA Today* wrote that Facebook’s 2Q18 earnings results “left no doubt that Cambridge Analytica and a barrage of other scandals have taken a serious toll”⁷¹⁷

(k) On July 26, 2018, *Forbes* wrote: “Following months of negative press, including the Cambridge Analytica data breach, Facebook missed second-quarter projections for both growth in revenue and growth in the number of daily active users across North America and Europe. Investors were further rattled by a comment from Facebook CFO David Wehner,

⁷¹⁵ Rupert Neate, *Over \$119bn wiped off Facebook’s market cap after growth shock*, *Guardian* (July 26 2018).

⁷¹⁶ Brian Deagon, *IBD 50 Stocks To Watch: Facebook Stock Plunges On Weak Results*, *Investor’s Business Daily* (July 26, 2018).

⁷¹⁷ Jessica Guynn, *Why Facebook had its worst day is complicated*, *USA Today* (July 28, 2018).

who said Facebook’s revenue growth would continue to slow down for the rest of 2018.”⁷¹⁸

(l) On July 26, 2018, *Yahoo Finance* wrote: “Facebook CFO Dave Wehner warned that revenue growth for the third- and fourth-quarters would decelerate in the high-single digits because of factors that include more data privacy options”⁷¹⁹

(m) On July 26, 2018, *CRN Australia* wrote: “Facebook’s stock fell as much as 24 percent on . . . Wednesday [July 25, 2018] over concerns about the impact of privacy issues on the social media company’s business, with executives warning that revenue growth would slow and expenses would rise. The plummeting stock price wiped out about US\$150 billion in market capitalisation in under two hours.”⁷²⁰

(n) On July 26, 2018, *Variety* wrote: “the introduction of new controls for users to limit their data-sharing with Facebook ‘may have an impact on our revenue growth.’”⁷²¹

(o) On July 26, 2018, Aegis Capital Corp. wrote: “The deceleration per FB is due to . . . data privacy controls, including GDPR impacts.”

⁷¹⁸ Madeline Berg, *On A Bad Day For Facebook Stock, Mark Zuckerberg’s Net Worth Plunges \$15.4 Billion*, *Forbes* (July 26, 2018).

⁷¹⁹ JP Mangalindan, *Facebook user numbers and revenue guidance disappoint, stock collapses*, *Yahoo Finance* (July 26, 2018).

⁷²⁰ Munsif Vengattil & Paresh Dave, *Facebook loses US\$150 billion in market value over privacy concerns*, *CRN Australia* (July 26, 2018).

⁷²¹ Todd Spangler, *Facebook Loses \$120 Billion in Market Value, as Stock Slides on Fears Growth Is Hitting a Wall*, *Variety* (July 26, 2018).

(p) On July 26, 2018, Evercore ISI wrote: “Why is the outlook calling for revenue deceleration? While bears may suspect core Facebook engagement challenges may be to blame, management’s stated drivers are . . . 3) the company providing users more choices around data privacy”

(q) On July 26, 2018, MKM Partners wrote: “The stock traded off by 10% into the call. The CFO [Wehner] then warned that revenue growth would decelerate by high single-digits sequentially Management highlights three areas for its revenue outlook . . . (iii) product focus on choice around user privacy, which could have an impact on monetization.”

C. Dr. Cain’s Expert Analysis Confirms Lead Plaintiffs’ Loss Causation Allegations

721. In addition, Lead Counsel retained an expert economist, Matthew D. Cain, Ph.D., to opine on loss causation issues for pleading purposes. Dr. Cain is a Senior Fellow at the Berkeley Center for Law and Business and a Senior Visiting Scholar at Berkeley Law School, University of California. He has a Ph.D. in Finance from Purdue University and has published research in leading finance, accounting, law, and economics journals, including the *Journal of Financial Economics*, the *Journal of Law and Economics*, the *Journal of Accounting and Economics*, the *Journal of Empirical Studies*, and the *Journal of Financial and Quantitative Analysis*. From 2014 to 2018, Dr. Cain worked at the SEC, where he provided economic analysis and expert witness testimony on behalf of the SEC in a wide variety of enforcement investigations, settlement negotiations and litigation. He also served as an advisor to SEC Commissioner Robert J. Jackson, Jr. and was awarded the Chairman’s Award for Economic Re-

search. Prior to working at the SEC, Dr. Cain was an Assistant Professor of Finance at the University of Notre Dame.⁷²²

722. In particular, Lead Counsel retained Dr. Cain to provide opinions on: (1) whether the alleged misstatements and/or omissions would be expected to impact the investing decisions of a reasonable investor; and (2) whether price declines in Facebook's common stock in March 2018 and on July 26, 2018 following corrective disclosures were statistically significant and were, from an economic perspective, proximately caused by the revelation of the truth concerning Defendants' alleged prior misstatements and/or omissions (*i.e.*, loss causation) and whether the price increase on April 26, 2018 was due to artificial inflation created by Defendants' alleged misrepresentations and/or omissions.⁷²³

723. Based on his analysis, Dr. Cain opined that, on each of the alleged corrective disclosures discussed in his declaration, "new information was revealed to the market concerning the continued misuse of user data by Cambridge Analytica, the extent and scope of Facebook's data privacy issues, and the lack of user control over data provided to Facebook. This information would be expected to carry importance in the investing decisions of a reasonable investor."⁷²⁴ Dr. Cain further opined that these alleged corrective disclosures "significantly altered the information environment available to investors in Facebook

⁷²² See Ex. C at 1-2.

⁷²³ *Id.* at 2-3.

⁷²⁴ *Id.* at 4; see also *id.* at 26.

securities” and “would be expected to have an impact on the investing decisions of a reasonable investor.”⁷²⁵

724. Dr. Cain also opined that: “the price declines in Facebook’s common stock on March 19, 2018, March 20, 2018, March 27, 2018 and July 25, 2018 were statistically significant” and were “economically sizeable, representing many billions of dollars of shareholder losses.”⁷²⁶ Dr. Cain further opined that: “from an economic perspective, these declines were *proximately caused* by the revelation of the truth concerning Defendants’ alleged misrepresentations and/or omissions.”⁷²⁷

725. In addition to the facts set forth above, Dr. Cain’s loss causation opinions further support Lead Plaintiffs’ allegations that the alleged corrective disclosures caused declines in the price of Facebook’s common stock price—and that members of the proposed Class suffered economic losses as a direct and proximate result of Defendants’ violations of the federal securities laws as alleged herein.

IX. Class Action Allegations

726. Lead Plaintiffs bring this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of all persons who purchased or otherwise acquired Facebook common stock during the Class Period (the “Class”). Excluded from the Class are defendants and their immediate families, directors and officers of Facebook and their immediate families, and each of the

⁷²⁵ *Id.* at 5; *see also id.* at 25-26.

⁷²⁶ *Id.* at 5; *see also id.* at 26.

⁷²⁷ *Id.* at 5; *see also id.* at 26.

foregoing persons' legal representatives, heirs, successors or assigns, and any entity in which defendants have or had a controlling interest.

727. The members of the Class are so numerous that joinder of all members is impracticable. The disposition of their claims in a class action will provide substantial benefits to the parties and the Court. During the Class Period, Facebook had more than 2.395 billion shares of common stock outstanding, owned by hundreds or thousands of persons.

728. There is a well-defined community of interest in the questions of law and fact involved in this case. Questions of law and fact common to the members of the Class that predominate over questions that may affect individual Class members include:

- (a) Whether the 1934 Act was violated by defendants;
- (b) Whether defendants omitted and/or misrepresented material facts;
- (c) Whether defendants' statements omitted material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading;
- (d) Whether defendants knew or recklessly disregarded that their statements were false and misleading;
- (e) Whether the price of Facebook common stock was artificially inflated; and
- (f) The extent of damage sustained by Class members and the appropriate measure of damages.

729. Lead Plaintiffs' claims are typical of those of the Class because Lead Plaintiffs and the Class sustained damages from defendants' wrongful conduct.

730. There is a presumption that each of the members of the Class relied on the misrepresentations and omissions alleged herein, pursuant to the fraud on the market theory as well as under *Affiliated Ute Citizens of Utah v. United States*, 406 U.S. 128 (1972) where the acts complained of are predicated upon omissions of material facts.

731. The misconduct alleged herein operated as a fraud on the market as it impacted the market price of Facebook common stock, including because:

(a) Defendants made public misrepresentations or failed to disclose material facts during the Class Period;

(b) the omissions and misrepresentations were material;

(c) the Company's stock traded in an efficient market;

(d) the misrepresentations alleged would tend to induce a reasonable investor to misjudge the value of the Company's stock; and

(e) Lead Plaintiffs and other members of the Class purchased Facebook common stock between the time defendants misrepresented or failed to disclose material facts and the time the true facts were disclosed, without knowledge of the misrepresented or omitted facts.

732. Lead Plaintiffs will adequately protect the interests of the Class and have retained counsel who are experienced in class action securities litigation. Lead Plaintiffs have no interest that conflicts with those of the Class.

733. A class action is superior to other available methods for the fair and efficient adjudication of this controversy.

X. Claims for Relief

COUNT I

For Violation of §10(b) of the 1934 Act and Rule 10b-5 Against All Defendants

734. Lead Plaintiffs incorporate all prior allegations by reference.

735. During the Class Period, defendants disseminated or approved the false statements specified above, which they knew or recklessly disregarded were misleading in that they contained misrepresentations and failed to disclose material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading.

736. Defendants violated §10(b) of the 1934 Act and Rule 10b-5 in that they:

(a) Employed devices, schemes and artifices to defraud;

(b) Made untrue statements of material fact or omitted to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading;
or

(c) Engaged in acts, practices and a course of business that operated as a fraud or deceit upon plaintiff and others similarly situated in connection with their purchases of Facebook common stock during the Class Period.

737. Lead Plaintiffs and the Class have suffered damages in that, in reliance on the integrity of the market, they paid artificially inflated prices for Facebook common stock. Lead Plaintiffs and the Class would not have purchased Facebook common stock at the prices they paid, or at all, if they had been aware that the market prices had been artificially and falsely inflated by defendants' misleading statements.

738. As a direct and proximate result of these defendants' wrongful conduct, Lead Plaintiffs and the other members of the Class suffered damages in connection with their purchases of Facebook common stock during the Class Period.

COUNT II

For Violation of §20(a) of the 1934 Act Against All Defendants

739. Lead Plaintiffs incorporate all prior allegations by reference.

740. During the Class Period, defendants acted as controlling persons of Facebook within the meaning of §20(a) of the 1934 Act. By virtue of their positions and their power to control public statements about Facebook, the Executive Defendants had the power and ability to control the actions of Facebook and its employees. Facebook controlled the Executive Defendants and its other officers and employees. By reason of such conduct, defendants are liable pursuant to §20(a) of the 1934 Act.

COUNT III

For Violations of §20A of the 1934 Act Against Defendant Mark Zuckerberg

741. Lead Plaintiffs repeat, incorporate, and reallege each and every allegation set forth above as if fully set

forth herein. As set forth in the paragraphs above and below, defendant Zuckerberg committed underlying violations of §10(b) and Rule 10b-5 thereunder by selling Facebook common stock while in possession of material nonpublic information about the Company’s deficient privacy protections and material risks to the Company and, consequently, is liable to contemporaneous purchasers of that stock under §20A of the 1934 Act.

742. Under §20A of the 1934 Act, “[a]ny person who violates any provision of this title or the rules or regulations thereunder by purchasing or selling a security while in possession of material, nonpublic information shall be liable in an action . . . to any person who, contemporaneously with the purchase or sale of securities that is the subject of such violation, has purchased (where such violation is based on a sale of securities) or sold (where such violation is based on a purchase of securities) securities of the same class.” 15 U.S.C. §78t-1(a).

743. Throughout the Class Period, defendant Zuckerberg was in possession of material nonpublic information regarding Facebook’s deficient privacy protections and material risks to the Company.

744. Defendant Zuckerberg’s aggregated daily insider sales of his Facebook Class A common stock during the Class Period are shown in the table below:

Trade Date	Shares	Insider Sale Proceeds
2/27/2017	192,874	\$26,249,516
2/28/2017	193,242	\$26,249,687
3/8/2017	190,638	\$26,249,493
3/9/2017	189,998	\$26,249,525

Trade Date	Shares	Insider Sale Proceeds
3/17/2017	187,604	\$26,249,636
3/20/2017	187,728	\$26,249,745
3/30/2017	70,219	\$9,999,858
3/31/2017	70,275	\$9,999,797
4/11/2017	187,767	\$26,249,778
4/12/2017	187,687	\$26,249,593
5/16/2017	141,950	\$21,249,850
5/17/2017	144,437	\$21,249,779
5/26/2017	140,064	\$21,249,886
5/30/2017	139,469	\$21,249,655
6/8/2017	138,149	\$21,249,717
6/9/2017	138,846	\$21,249,129
6/21/2017	138,813	\$21,249,578
6/22/2017	138,205	\$21,249,941
6/29/2017	140,841	\$21,249,271
6/30/2017	140,595	\$21,249,035
7/12/2017	134,599	\$21,249,617
7/13/2017	133,501	\$21,249,680
8/14/2017	124,625	\$21,249,796
8/15/2017	124,359	\$21,249,595
8/25/2017	127,342	\$21,249,709
8/28/2017	127,183	\$21,249,553

Trade Date	Shares	Insider Sale Proceeds
9/7/2017	123,644	\$21,249,717
9/8/2017	123,503	\$21,249,854
9/19/2017	123,815	\$21,249,679
9/20/2017	123,637	\$21,249,477
9/29/2017	124,633	\$21,249,547
10/2/2017	124,894	\$21,249,517
10/11/2017	123,485	\$21,249,788
10/12/2017	122,752	\$21,249,620
11/14/2017	119,230	\$21,249,761
11/15/2017	119,485	\$21,249,412
11/27/2017	116,141	\$21,249,533
11/28/2017	115,997	\$21,249,612
12/7/2017	119,098	\$21,249,707
12/8/2017	117,829	\$21,249,838
2/12/2018	220,000	\$38,635,723
2/13/2018	177,200	\$30,929,013
2/14/2018	220,000	\$39,026,000
2/15/2018	245,400	\$43,901,109
2/16/2018	245,400	\$43,719,265
2/20/2018	220,000	\$38,835,127
2/21/2018	228,400	\$40,904,384
2/22/2018	228,400	\$40,881,223

Trade Date	Shares	Insider Sale Proceeds
2/23/2018	220,000	\$40,014,898
2/26/2018	220,000	\$40,618,821
2/27/2018	220,000	\$40,253,285
2/28/2018	245,400	\$44,529,455
3/1/2018	245,400	\$43,423,597
3/2/2018	220,000	\$38,500,131
3/5/2018	220,000	\$39,410,874
3/6/2018	220,000	\$39,720,907
3/7/2018	220,000	\$39,907,908
3/8/2018	228,400	\$41,692,621
3/9/2018	228,400	\$42,162,003
3/12/2018	220,000	\$40,732,522
3/13/2018	220,000	\$40,225,112
3/14/2018	245,400	\$44,942,497
3/15/2018	245,400	\$44,939,108
3/16/2018	220,000	\$40,594,574
3/19/2018	175,246	\$30,504,876
3/20/2018	145,000	\$24,158,892
3/21/2018	153,400	\$25,808,227
3/22/2018	152,700	\$25,441,367
3/23/2018	145,000	\$23,674,979
3/26/2018	145,000	\$22,555,546

Trade Date	Shares	Insider Sale Proceeds
3/27/2018	153,539	\$24,175,526
3/28/2018	140,200	\$21,527,971
3/29/2018	145,000	\$22,978,944
4/2/2018	145,000	\$22,610,877
4/3/2018	145,000	\$22,462,916
4/4/2018	145,000	\$22,237,405
4/5/2018	145,000	\$23,081,281
4/6/2018	145,000	\$23,049,687
4/9/2018	162,000	\$25,765,797
4/10/2018	162,000	\$26,077,639
4/11/2018	145,000	\$24,059,149
4/12/2018	145,000	\$23,853,082
4/13/2018	145,000	\$23,885,937
4/16/2018	145,000	\$23,893,540
4/17/2018	145,000	\$24,348,750
4/18/2018	145,000	\$24,190,673
4/19/2018	162,000	\$27,014,864
4/20/2018	162,000	\$27,052,706
4/23/2018	145,000	\$24,161,233
4/24/2018	145,000	\$23,426,871
4/25/2018	145,000	\$23,087,982
4/26/2018	212,557	\$37,088,554

Trade Date	Shares	Insider Sale Proceeds
4/27/2018	177,028	\$30,883,270
4/30/2018	156,967	\$27,260,171
5/1/2018	145,000	\$24,908,295
5/2/2018	220,000	\$38,862,071
5/3/2018	199,530	\$34,808,784
5/4/2018	237,000	\$41,697,212
5/7/2018	237,000	\$42,287,824
5/8/2018	220,000	\$39,186,693
5/9/2018	220,000	\$39,885,285
5/10/2018	220,000	\$40,669,369
5/11/2018	220,000	\$40,987,320
5/14/2018	220,000	\$41,137,360
5/15/2018	220,000	\$40,479,883
5/16/2018	220,000	\$40,354,785
5/17/2018	220,000	\$40,343,839
5/18/2018	237,000	\$43,391,467
5/21/2018	237,000	\$43,683,830
5/22/2018	220,000	\$40,553,419
5/23/2018	220,000	\$40,618,621
5/24/2018	220,000	\$40,934,971
5/25/2018	220,000	\$40,745,841
5/29/2018	220,000	\$40,790,973

Trade Date	Shares	Insider Sale Proceeds
5/30/2018	220,000	\$41,182,290
5/31/2018	220,000	\$41,937,965
6/1/2018	237,000	\$45,853,073
6/4/2018	237,000	\$45,737,922
6/5/2018	220,600	\$42,718,882
6/6/2018	220,000	\$41,897,754
6/7/2018	220,000	\$41,413,594
6/8/2018	220,000	\$41,513,378
6/11/2018	220,000	\$42,033,413
6/12/2018	220,000	\$42,309,938
6/13/2018	237,000	\$45,760,485
6/14/2018	267,000	\$52,214,130
6/15/2018	250,000	\$48,974,895
6/18/2018	247,500	\$49,027,822
6/19/2018	240,000	\$47,044,460
6/20/2018	240,000	\$48,417,988
6/21/2018	240,000	\$48,461,671
6/22/2018	240,000	\$48,211,475
6/25/2018	240,000	\$47,074,618
6/26/2018	240,000	\$47,451,913
6/27/2018	257,000	\$51,140,945
6/28/2018	257,000	\$50,254,415

Trade Date	Shares	Insider Sale Proceeds
6/29/2018	236,615	\$46,329,394
7/2/2018	240,000	\$46,799,219
7/3/2018	212,600	\$41,166,309
7/5/2018	240,000	\$47,066,812
7/6/2018	240,000	\$48,316,665
7/9/2018	240,000	\$48,996,111
7/10/2018	257,000	\$52,357,773
7/11/2018	257,000	\$52,255,054
7/12/2018	240,000	\$49,371,961
7/13/2018	240,000	\$49,752,309
7/16/2018	240,000	\$49,841,323
7/17/2018	240,000	\$49,981,589
7/18/2018	240,000	\$50,343,432
7/19/2018	240,000	\$50,047,178
7/20/2018	240,000	\$50,404,452
7/23/2018	257,000	\$54,134,125
7/24/2018	257,000	\$55,141,446
7/25/2018	240,000	\$52,010,641
Total	29,451,835	\$5,297,581,009

745. Contemporaneously with defendant Zuckerberg's insider sales, Lead Plaintiffs purchased a total of 260,091 shares of Facebook Class A common stock for a total of more than \$44.6 million between February 3, 2017

and July 25, 2018. Lead Plaintiffs' contemporaneous purchases included:

Lead Pl.	Date	Shares	Purchase Amount	No. of Days After Zuckerberg Sale
Miss.	3/17/2017	4,050	\$566,329	Same day
Miss.	3/21/2017	16,219	\$2,272,893	1 day
Amal.	3/31/2017	3,611	\$512,961	Same day
Amal.	4/3/2017	1,387	\$197,349	3 days
Miss.	6/16/2017	4,035	\$607,796	7 days
Amal.	6/23/2017	3,937	\$610,530	1 day
Amal.	8/16/2017	100	\$17,013	1 day
Miss.	8/16/2017	5,200	\$883,812	1 day
Amal.	8/29/2017	300	\$50,428	1 day
Amal.	8/29/2017	10	\$1,681	1 day
Miss.	9/15/2017	1,311	\$225,008	7 days
Amal.	9/18/2017	1	\$170	10 days

Lead Pl.	Date	Shares	Purchase Amount	No. of Days After Zuckerberg Sale
Amal.	10/3/2017	20	\$3,401	1 day
Amal.	10/19/2017	10	\$1,741	7 days
Miss.	12/15/2017	3,218	\$579,787	7 days
Amal.	12/18/2017	226	\$40,866	10 days
Amal.	3/2/2018	1,200	\$210,823	Same day
Amal.	3/2/2018	50	\$8,784	Same day
Miss.	3/16/2018	2,898	\$536,368	Same day
Amal.	3/19/2018	1,414	\$244,007	Same day
Miss.	3/19/2018	62,000	\$10,634,662	Same day
Amal.	3/20/2018	1,800	\$293,672	Same day
Amal.	3/20/2018	50	\$8,158	Same day

Lead Pl.	Date	Shares	Purchase Amount	No. of Days After Zuckerberg Sale
Miss.	3/26/2018	55,000	\$8,590,126	Same day
Amal.	4/11/2018	300	\$49,995	Same day
Amal.	4/11/2018	10	\$1,666	Same day
Miss.	4/27/2018	18,978	\$3,305,763	Same day
Amal.	5/2/2018	60	\$10,599	Same day
Miss.	5/14/2018	9,444	\$1,766,417	Same day
Amal.	5/29/2018	100	\$18,632	Same day
Amal.	6/8/2018	2,021	\$382,191	Same day
Miss.	6/13/2018	34,609	\$6,690,716	Same day
Miss.	6/15/2018	3,132	\$613,372	Same day
Amal.	6/19/2018	100	\$19,562	Same day
Amal.	6/19/2018	10	\$1,956	Same day
Amal.	6/22/2018	6,155	\$1,241,771	Same day

Lead Pl.	Date	Shares	Purchase Amount	No. of Days After Zuckerberg Sale
Miss.	6/27/2018	16,214	\$3,211,359	Same day
Miss.	7/17/2018	911	\$189,251	Same day
	Total	260,091	\$44,601,615	

746. Tens of thousands of other Class members, if not more, also purchased shares contemporaneously with defendant Zuckerberg's insider sales during the Class Period. Facebook had a total of nearly 7.6 billion shares traded in the United States during the Class Period, or an average daily trading volume of more than 20.4 million shares. On each of the days that defendant Zuckerberg sold his Facebook shares, between \$8.5 million and \$129.8 million shares were traded to investors, including members of the Class.

747. Lead Plaintiffs and other Class members who purchased shares of Facebook common stock contemporaneously with defendant Zuckerberg's insider sales suffered damages because: (i) in reliance on the integrity of the market, they paid artificially inflated prices as a result of the defendants' violations of §§10(b) and 20(a) of the 1934 Act; and (ii) they would not have purchased Facebook common stock at the prices they paid, or at all, if they had been aware that the market prices had been artificially inflated by defendants' false and misleading statements and omissions.

XI. Prayer for Relief

WHEREFORE, Lead Plaintiffs pray for judgment as follows:

A. Determining that this action is a proper class action, designating plaintiffs as Lead Plaintiffs and certifying Lead Plaintiffs as class representatives under Rule 23 of the Federal Rules of Civil Procedure and Plaintiffs' Counsel as a Class Counsel;

B. Awarding Lead Plaintiffs and the members of the Class damages and interest;

C. Awarding Lead Plaintiffs' reasonable costs, including attorneys' fees; and

D. Awarding such equitable/injunctive or other relief as the Court may deem just and proper.

XII. Jury Demand

Lead Plaintiffs demand a trial by jury.

DATED: October 16, 2020

* * *