EFiled: Aug 06 2021 03:34PM EDT
Transaction ID 66784692
Case No. 2018-0307-JRS

IN THE COURT OF CHANCERY OF THE STATE OF DELAWARE

KAREN SBRIGLIO, FIREMEN'S RETIREMENT SYSTEM OF ST. LOUIS, CALIFORNIA STATE TEACHERS' RETIREMENT SYSTEM, CONSTRUCTION AND GENERAL BUILDING LABORERS' LOCAL NO. 79 GENERAL FUND, CITY OF BIRMINGHAM RETIREMENT AND RELIEF SYSTEM, and LIDIA LEVY, derivatively on behalf of Nominal Defendant FACEBOOK, INC.,

Plaintiffs,

v.

MARK ZUCKERBERG, SHERYL SANDBERG, PEGGY ALFORD, MARC ANDREESSEN, KENNETH CHENAULT, PETER THIEL, JEFFREY ZIENTS, ERSKINE BOWLES, SUSAN DESMOND-HELLMANN, REED HASTINGS, JAN KOUM, KONSTANTINOS PAPAMILTIADIS, DAVID FISCHER, MICHAEL SCHROEPFER, and DAVID WEHNER

Defendants,

-and-

FACEBOOK, INC.,

Nominal Defendant.

C.A. No. 2018-0307-JRS

PUBLIC INSPECTION VERSION
FILED AUGUST 6, 2021

SECOND AMENDED VERIFIED STOCKHOLDER DERIVATIVE COMPLAINT

TABLE OF CONTENTS

Plaintiffs California State Teachers' Retirement System, Construction and General Building Laborers' Local No. 79 General Fund, City of Birmingham Retirement and Relief System, Firemen's Retirement System of St. Louis, Karen Sbriglio, and Lidia Levy (collectively, "Plaintiffs"), by their attorneys, respectfully submit this Second Amended Verified Stockholder Derivative Complaint for the benefit of nominal defendant Facebook, Inc. ("Facebook" or the "Company") against certain current and/or former members of its Board of Directors (the "Board") and executive officers Konstantinos Papamiltiadis, David Fischer, Michael Schroepfer and David Wehner (collectively, the "Individual Defendants") seeking to remedy the Individual Defendants' breaches of fiduciary duties and/or *Brophy* insider trading violations from June 26, 2013 through July 23, 2019, the date before the FTC announced the $5 billion fines on Facebook the following morning (the "Relevant Period").

Plaintiffs make these allegations upon personal knowledge as to those allegations concerning Plaintiffs and, as to all other matters, upon information and belief based on the investigation of undersigned counsel, which includes the review and analysis of: (a) Facebook's public filings with the United States Securities and Exchange Commission ("SEC"); (b) press releases and other publications disseminated by Facebook, related parties and other related non-parties; (c) press releases, public letters, and other publicly disseminated information regarding

investigations into the Company by the Federal Trade Commission (the "FTC"), including the FTC's repository of documents, which includes the FTC consent order entered following the FTC's investigation into Facebook's disclosures and privacy practices in 2011 ("2012 Consent Order")[1], the FTC's Complaint for Civil Penalties, Injunction, and Other Relief ("2019 FTC Complaint")[2], and the Stipulated Order For Civil Penalty, Monetary Judgment, and Injunctive Relief ("2019 Consent Order")[3] entered in the action captioned as *U.S.A. v. Facebook, Inc.*, No. 19-cv-2184 (D.D.C.); (d) press releases, public letters, and other publicly disseminated information regarding investigations into the Company by the Department of Justice ("DOJ"), SEC, Federal Bureau of Investigation ("FBI"), Congress, and the Information Commissioner's Office of the United Kingdom ("ICO"); (e) certain of Facebook's internal Board minutes, Board-level materials, and email communications obtained through an action pursuant to 8 *Del. C.* § 220 seeking the

---

[1] *U.S. v. Facebook*, No. C-4365 (July 27, 2012) *available at*: https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.

[2] *U.S. v. Facebook*, 1:19-cv-02184 (D.D.C. July 24, 2019), Dkt. 1, *available at*: https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-24-19.pdf.

[3] *U.S. v. Facebook, Inc.*, No. C-4365 (Apr. 28, 2020) *available at*: https://www.ftc.gov/system/files/documents/cases/c4365facebookmodifyingorder.pdf.

inspection of Company books and records, which was successfully prosecuted by Plaintiffs under the caption *In re Facebook, Inc. Section 220 Litig.*, C.A. No. 2018-0661-JRS (the "Section 220 Action"); (f) the proceedings of a related pending shareholder derivative action filed on behalf of the Company, captioned *In re Facebook, Inc. Shareholder Derivative Privacy Litigation*, No. 4:18-cv-01792-HSG (N.D. Cal.); (g) Facebook's policies, statements, terms of service, and other Facebook documents published on Facebook's website and prior versions of data policies, terms of use, application developer policies, and related documents located on the Internet Archive; (h) transcripts of testimony, written statements, and documents submitted in connection with the U.K's House of Commons' Digital, Culture, Media and Sport Committee the "U.K. Committee"); (i) the U.K. Committee's Final Report on Disinformation and "fake news," dated February 14, 2019 (the "U.K. Disinformation Report");[4] (j) written statements and testimony by Cambridge Analytica whistleblower Christopher Wylie, former Facebook Operations Manager, whistleblower Sandy Parakilas, and Facebook's former Chief Security Officer Alex Stamos; (k) transcripts of testimony given by Zuckerberg

[4] House of Commons' Digital, Culture, Media and Sport Committee, Disinformation and 'fake news': Final Report (Eighth Report of Session 2017–19) (February 14, 2019), *available at*: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.

before the U.S. Senate's Judiciary and Commerce Committees and the U.S. House of Representatives Energy and Commerce Committee, and Facebook's submissions in response to questions posed by members of Congress, submitted on June 8, 2018 and June 29, 2018; (l) documents ("643 Docs") that are, on information and belief, internal Facebook documents obtained through public sources in connection with the litigation captioned as *Six4Three LLC v. Facebook, Inc. et al.*, No. CIV-533328 (San Mateo Cty. Cal. Sup. Ct.) (the "643 Litigation"); (m) document summaries ("643 Summaries") that are, on information and belief, summaries of internal Facebook documents produced in the 643 Litigation that were published and made publicly available on the internet;[5] (n) public documents filed in the matter of *Attorney General Maura Healey v. Facebook Inc.*, No. 1984-cv-02597-BLS-1 (Sup. Ct. Mass.) ("Mass. AG") and in the matter of *District of Columbia v. Facebook Inc.*, 2018 CA 008715 (D.C. Sup. Ct.) ("D.C. AG"); (o) documents and information secured by the Electronic Privacy Information Center ("EPIC") through litigation and Freedom of Information Act requests; (p) FTC documents and information secured by counsel for Plaintiffs through Freedom of Information Act requests; (q) statements made by Zuckerberg, Sandberg, Desmond-Hellmann, and other

[5] Both the 643 Docs and the 643 Summaries are available for download at: https://www.duncancampbell.org/facebookleaks (last visited July 20, 2021).

Facebook senior executives; (r) Facebook's governance policies and committee charters during the Relevant Period, including, but not limited to, the Corporate Governance Guidelines, Code of Conduct, and the Audit & Risk Oversight Committee Charter; and (s) other publicly available information concerning Facebook and the Individual Defendants.

I. SUMMARY OF THE ACTION

1. Facebook controls, and is legally obligated to protect, the personal data of over 2.8 billion people. Maintaining the privacy and security of this user data is a mission critical function for Facebook. If Facebook is not a good steward of user information, then users will be less likely to share personal information with Facebook or to use the platform to connect with others for social or transactional purposes. This would result in Facebook having less user data to support targeted ad placement, the sale of which constitutes substantially all of Facebook's operating revenue.

2. Facebook's founder, Chief Executive Officer ("CEO") and Chairman of the Board, Mark Zuckerberg ("Zuckerberg"), and other senior executives, including Director and Chief Operating Officer ("COO") Sheryl Sandberg ("Sandberg"), developed a growth model for Facebook by turning it into a broker for personal user information, whereby it would help generate, trade for, collect and

retain ever larger (and more valuable) amounts of personal user information as Facebook users interacted with the platform.

3. The Individual Defendants accomplished this by creating Facebook's Graph API—a database containing personal user information that also tracked social relations between these information points. As users created increasing amounts of personal information, the Individual Defendants opened Facebook's Graph API to an expanding number of third-party apps offered on its platform ("Platform Applications"). Those Platform Applications connected billions of users of Facebook's service, each of whom create a Facebook "profile" showing personal information, with other individuals in their community (or friends), who also have Facebook accounts and profiles. The Individual Defendants required this information to be fed back into Graph API, thereby allowing Facebook, through its users' accounts, to collect data on virtually every aspect of a user's social and personal life, including highly sensitive personal information, totaling ***more than 52,000 data points***.

4. In exchange for access to the platform, which included the trove of personal information that Facebook collected on its hundreds of millions, and now billions, of users, Facebook insisted that developers share the user data they collect and process it back into the Facebook platform.

5. As detailed herein, this business plan allowed the Individual Defendants to cause Facebook to surreptitiously collect, share, and profit from unprecedented amounts of personal information on its users that Facebook, in turn, used to further grow the platform, sell ad placements and generate billions of dollars annually in ill-gotten net income. This business plan was premised upon unfair, deceptive and illegal trade practices and subjected Facebook's users to the widespread harvesting and use of their personal information for further illicit purposes.

6. The Individual Defendants' business plan, pursuant to which Facebook would share personal user information without users' consent, incredibly, was in fact continued, and made more egregious on the heels of Facebook's entry into the 2012 Consent Order with the FTC. The 2012 Consent Order resolved claims that Facebook had previously violated user privacy by sharing of personal user data with third parties without proper authorization. The FTC later found that the Individual Defendants still had not reformed these improper practices as of July 2019. Given that the 2012 Consent Order was made final in July 2012, and that each Individual Defendant received a copy of that Order, the Individual Defendants' plan to illicitly utilize personal user information and inability to bring Facebook into compliance with governing law spanned a period of over seven years.

7. Implementation of the Individual Defendants' information sharing business model was referred to internally as "full reciprocity" because Facebook received the personal user information generated through Platform Applications, and then granted those third-party app developers access to all the information on the platform. The Individual Defendants also implemented a practice known as "whitelisting" to maintain nominal control over the personal user information that it also widely shared. Whitelisted entities were those third-party companies that Facebook viewed as a "partner" or not otherwise a competitive threat. A whitelisted entity could access all of the personal information of the user and of the user's "Friends" even if the user had not authorized such access.

8. The Individual Defendants thereby caused Facebook to override user privacy preferences. For example, even if a Facebook user chose to "restrict" "Friends' apps" from access to the user's information, the Individual Defendants caused Facebook to continue to openly share that information with commercial third parties through the Platform Applications that they had caused Facebook to approve. Meanwhile, the user's privacy controls would deceptively indicate that the information was not being shared. Internal company documents and emails further revealed that certain developers were whitelisted based on personal relationships to Facebook directors and employees, including at least, Defendants Zuckerberg, Sandberg, Andreessen and Konstantinos Papamiltiadis ("Papamilitiadis"), as well as

current or former Facebook officers and/or executives (non-parties identified herein) such as Sam Lessin, Michael Vernal, and Ime Archibong. For example, Netflix was whitelisted, and Netflix's founder, CEO, and President is Defendant Hastings. Dropbox was also whitelisted, and Drobox's co-founder and CEO is Director Drew Houston.

9. Moreover, the Individual Defendants' disregard for the privacy of Facebook's users' data went beyond the Company's whitelisting practices. For example, in line with direction from Facebook's growth team (of which Zuckerberg is a member), Facebook's product developers created a means to collect call logs, text messages and location data from Android users and then found a surreptitious workaround to prevent Android Facebook users from being alerted to the additional data Facebook was collecting.

10. Thus, Facebook, under the control of the Board, made the choice to expand sharing of personal user information to Platform Applications in defiance of the 2012 Consent Order. This included sharing core identifying demographic information (*e.g.*, user birthdates, gender, location, Friend lists, likes, Facebook User ID), the ability to read a user's mailbox and messages, and open access to the personal user information of all Friends of a given user.

11. With virtually no meaningful limits in place on Facebook's sharing of personal user information, which occurred either without users' knowledge or in

express contravention of users' consent, it is unsurprising that other companies would collect and use such information for their own purposes. Thus, the Individual Defendants' oversight and management of Facebook's practices facilitated the widespread dissemination of personal user information, which, in turn, facilitated Cambridge Analytica's harvesting of the personal user information from ***over 87 million Facebook users*** even though the Platform Application that Cambridge Analytica used to collect such data only received consent from ***roughly 270,000 users***.

12. Cambridge Analytica's use of personal user information was the destined consequence of the Individual Defendants' platform business plans, which were premised on the open sharing of personal user information in the spirit of "full reciprocity" and through agreements with its Platform Application partners, with or without user knowledge or consent, in violation of the 2012 Consent Order. The Individual Defendants caused Facebook to fail to take any steps to verify how personal user information was being used by those partners.

13. Worse, the Individual Defendants knew that the private information of millions of Facebook users had been used for nefarious purposes since at least 2015, but failed to cause Facebook to acknowledge or disclose this information. Instead, the Individual Defendants caused Facebook to actively obfuscate the extent of its information privacy and compliance failures. The Individual Defendants'

dishonesty knew few limits, as Zuckerberg misled United States Congress in hearings conducted in the wake of Cambridge Analytica, and UK authorities found that Facebook's responses to its inquiries had been conducted in "***bad faith***."

14. The Individual Defendants' efforts to cause Facebook to bury its misconduct under misinformation were ultimately unsuccessful. After the *New York Times* and *The Guardian* reported the Cambridge Analytica data breach, Sandberg was forced to admit Facebook had committed a "breach of trust" by failing to protect user data and failing to notify users of the data breach. Despite these concessions, and with the knowledge that Facebook's own business practices had facilitated the data breach, the Individual Defendants did nothing to cause Facebook to change its underlying business model or comply with the 2012 Consent Order, and instead continued their wrongful practices. In fact, ***the Company's whitelisting practices continued well into 2018***.

15. The internal Company books and records obtained in the Section 220 Action (the "220 Documents") show a stunning breakdown in Facebook's governance functions, such that the Board had virtually no oversight of the foregoing practices despite their knowledge that they had set forth a policy of sharing of personal user information with third parties. This oversight failure is particularly egregious in the context of the requirements imposed by the 2012 Consent Order, which, *inter alia*, affirmatively required the Board to ensure the Company: (i)

implemented and maintained a comprehensive new privacy program; (ii) maintained records relating to user data privacy and security; and (iii) obtained users' affirmative consent before sharing their information.

16. While the Board received [redacted], the 220 Documents provide no evidence of any Board effort or action to change Facebook's policies or practices concerning the handling and protection of the personal users information (beyond cosmetic changes). Similarly, the 220 Documents provide no evidence that the Board understood how their policies had enabled the Company to share information through Platform Applications. The Board also engaged in no meaningful inquiry into, or oversight over, Facebook's practices with respect to ensuring that Facebook complied with its legal obligations under the 2012 Consent Order, dealt candidly with regulatory inquiries, or appropriately limited the corporation's massive exposure to legal liability.

17. Facebook's internal audit function similarly failed to address these core business practices according to the 220 Documents received by Plaintiffs. The 220 Documents produced had no copies of management-conducted compliance audits, no copies of audits to ensure the existence of appropriate risk mitigation controls, and no copies of any periodic reviews conducted by an internal audit department based on identified risks touching on these core issues that were reviewed by the Board. [redacted]

[redacted]

18. Facebook had not even [redacted] And it would not be until April 26, 2018 that Facebook would create any oversight, even at the management level, for privacy and data use in the Company's engineering organization. Prior to that, Facebook was not gathering reports necessary to examine how the Company's Facebook platform truly shared personal user information. The sole reports produced to Plaintiffs that could even be considered internal testing, service organization control ("SOC") reports conducted by Ernst & Young, do not even discuss Facebook's compliance with the 2012 Consent Order; nor do they test whether a Facebook user's personal data was being shared with third parties without the user's consent. Instead, Facebook's internal audit efforts focused on [redacted]

19. During the course of this epic corporate governance failure, the Individual Defendants were well aware of (or at best recklessly disregarded) the tremendous risks that Facebook's illegal course of conduct posed to the Company, in light of: (a) the steady drumbeat of numerous red flags that marched past each Individual Defendant warning that user privacy and data sharing liability issues plagued the Company and were not being addressed; (b) a core business strategy that

was based on the illicit sharing of massive amounts of personal user information; and (c) the lack of testing or controls in place to ensure its compliance with the 2012 Consent Order. Indeed, Facebook never seriously attempted to comply with the requirements of the 2012 Consent Order. For example, Facebook removed a disclaimer required by the 2012 Consent Order on Facebook's Privacy Settings page (warning users that information shared with Facebook Friends could also be shared with the apps those Friends used) a mere four months after the 2012 Consent Order was finalized.[6]

20. Facebook's profound governance failures have also led to a complete breakdown in Board independence, leaving no one to check Zuckerberg's consolidation of decision-making power as any director attempting to assert independence, or even disagree with Zuckerberg, faces the serious threat of removal. The litany of directors forced out include Defendants Koum, Hastings, Desmond-Hellmann, Bowles, Chenault, and Zients.

21. Unfortunately, the Individual Defendants' failure to take action to institute proper governance, shore up Board independence, and secure the personal information of its users has brought significant harm upon the Company. On July 24, 2019, the FTC and Facebook entered into a settlement involving a $5 billion fine,

[6] 2019 FTC Complaint, *supra* note 2, at ¶ 7.

the largest penalty ever imposed for violating consumer privacy rights. The FTC also required reforms that the Company refused, or was otherwise unable to impose by itself, to resolve the FTC's allegations that Facebook violated the 2012 Consent Order by deceiving its users, sharing personal user information with hundreds of companies, and ignoring privacy setting restrictions set by users.

22. The misconduct described herein is the same misconduct that led to Facebook's entry into the 2012 Consent Order in the first place: namely, Facebook's deceitful statements that users could keep their information private when, in fact, the Individual Defendants had set forth processes whereby Facebook actively engaged in the widespread, surreptitious sharing of such information with third parties. Beyond the FTC's fine, the Company also agreed to settle a claim brought by the SEC for $100 million in July 2019, which alleged that Facebook made certain false and misleading statements to investors "[f]rom 2016 until mid-March 2018" regarding its awareness of misuse of user information.[7]

23. The Individual Defendants' misconduct has also drawn the ire of the DOJ (which worked closely with the FTC in its investigation and pursuit of claims against Facebook), the United Kingdom's House of Commons, and the European

[7] *S.E.C. v. Facebook*, 3:19-cv-04241 (N.D. Cal. July 24, 2019), Dkt. 1, at ¶¶ 1, 6, 7 (hereinafter, the "SEC Complaint").

Union's Information Commissioner's Office, among others. This is to say nothing of Facebook's loss of trust with the public generally.

24. Investigations and litigation concerning Facebook's corporate misconduct remain ongoing. And Facebook still faces the possibility of substantial additional liability in numerous other private lawsuits by consumers and other Facebook stakeholders. It has also suffered a severe loss of user and public trust, and Facebook's size and business have been subsequently placed under a regulatory spotlight, the full impact of which remains unknown.

25. Despite the extreme damages continuing to inure to the Company as a result of the foregoing governance failures, Facebook remains rudderless with respect to protecting its users' information. In fact, in April 2021, cybersecurity experts discovered that a vast trove of ***the user data of over 530 million users had been scraped from Facebook's website and made freely available online***. The information included full names, locations, birthdays, email addresses, phone numbers, and relationship status of the Facebook users.[8]

[8] Facebook likely harbors many more undiscovered truths about what it is really doing with user data. Facebook's stated policy of prioritizing "image management" and profits over the data transparency foreseeably indicates that Facebook, once again, controls what the public knows and needs to know about its policies concerning personal user information. *See* Kevin Rose, *Inside Facebook's Data Wars*, N.Y. TIMES (July 14, 2021), *available at*:

26. Facebook's initial response to this additional revelation of its abuse of user information was as disappointing as it was familiar: the Company failed to notify any of its customers that their information had been exposed. And as a leaked internal Company memoranda later evidenced, Facebook's broader planned response to its failure to secure the user data of over 530 million users was ***not*** to take steps to sufficiently secure personal information or ensure that users were aware that their data had been exposed. Instead, Facebook internally wrote, "[a]ssuming press volume continues to decline, we're not planning additional statements on this issue."[9] Instead of taking appropriate action, the internal memo further indicated Facebook's plans to "***normalize*** the fact that this [scraping of user data] activity is ongoing and avoid criticism that we aren't being transparent about particular incidents." Facebook thereby deliberated that it would not attempt to comply with its obligations to safeguard user data, further reflecting the Company's pervasive internal governance failures and the Individual Defendants' continuing breaches of fiduciary duty.

---

https://www.nytimes.com/2021/07/14/technology/facebook-data.html?referringSource=articleShare.

[9] Adam Smith, *Internal Facebook Memo Reveals Company Plan to 'Normalise' News of Data Leaks After 500 Million User Breach*, THE INDEPENDENT (April 20, 2021), https://www.independent.co.uk/life-style/gadgets-and-tech/facebook-memo-leak-normalise-breach-b1834592.html.

27. The Board's inaction can only be explained by its deference to Facebook's founder, Defendant Zuckerberg. Defendant Zuckerberg controlled (and continues to control) the Board. As Defendant Desmond-Hellmann conceded, members of the Board "believed that [they] had no real ability to say 'no' to Zuckerberg."[10] Considering Defendant Zuckerberg directed and approved the improper privacy practices and championed the unlawful business plan described below, the Board's inaction is unsurprising.

28. The Board's lack of independence from Zuckerberg in his pursuit of an illegal business plan continued through the Company's negotiation of the FTC's settlement regarding Facebook's violation of the 2012 Consent Order. Specifically, when the FTC pursued personal accountability for Defendant Zuckerberg for the data and privacy abuses, the Board demurred, categorically refusing to negotiate any settlement that included personal liability for Zuckerberg. The Board was thereby beholden to Zuckerberg and favored him in disregard of its duty of loyalty to the Company. The Board's failure to cabin Zuckerberg's conflicts caused the Board to

[10] *In re Facebook, Inc. Class C Reclassification Litig.*, No. 12286-JTL, Plaintiffs' Pre-Trial Brief, at 14 (Sept. 22, 2017) (hereinafter "*Facebook Class C Shares Litigation*") (Trans. ID 61152559); *see also* L. Stangel, *Silicon Valley Business Journal, Facebook's Board doesn't Challenge Zuckerberg Enough, Says Lawyer who Sued Company*, SILICON VALLEY BUS. J. (Oct. 6, 2017), *available at*: https://www.bizjournals.com/sanjose/news/2017/10/06/facebook-share-sale-plan-zuckerberg-control-suit.html.

approve a settlement that protected Defendant Zuckerberg at the cost of billions of dollars in additional fines to the Company and its shareholders.

29. In this action, Plaintiffs, on behalf of Facebook, seek to recover for the harm sustained by the Company as a result of the breaches of fiduciary duty by the Company's officers and directors. Plaintiffs also seek a return of the illicit insider trading profits made through the use of confidential company information.

II. JURISDICTION AND VENUE

30. This action arises under the laws of the State of Delaware because it pertains to breaches of fiduciary duty by directors, officers, and a controlling stockholder of a corporation incorporated in Delaware.

31. The Delaware Court of Chancery has *in personam* jurisdiction of each Individual Defendant herein, as (a) Facebook is a Delaware corporation and (b) each Individual Defendant was a director and/or senior officer of Facebook, and as such assented as a matter of law to the jurisdiction of this Court under 10 *Del. C.* §3114.

32. Venue is proper in this Court. Article IX of Facebook's Restated Certificate of Incorporation designates the Delaware Court of Chancery as "the sole and exclusive forum for (1) any derivative action or proceeding brought on behalf of the corporation, (2) any action asserting a claim of breach of fiduciary duty owed by, or other wrongdoing by, any director, officer, employee or agent of the

corporation or the corporation's stockholders . . . or (5) any action asserting a claim governed by the internal affairs doctrine."

III. PARTIES

A. Plaintiffs

33. Plaintiff California State Teachers' Retirement System ("CalSTRS") owns, and has owned, shares of Facebook common stock during the entire period of wrongdoing alleged herein. CalSTRS will fairly and adequately represent the interests of other shareholders and the Company in enforcing its rights.

34. CalSTRS was established for the benefit of California's public-school teachers over 100 years ago and is the largest educator-only pension fund in the world. CalSTRS' investment portfolio was valued at $306.7 billion as of May 31, 2021. CalSTRS serves the investment and retirement interest of more than 949,000 plan participants and their beneficiaries who hail from the state's 1,700 school districts, county offices of education, and community college districts.

35. Given the long-term nature of CalSTRS' liabilities, and its fiduciary responsibilities to its members, the fund is keenly interested in corporate governance

issues, and publicly pronounced that "good governance is good for business, and we expect that of any corporation within which we invest."[11]

36. CalSTRS invested in Facebook before the Company's IPO through its private equity allocation and has continuously held shares in the Company.

37. Commensurate with its substantial financial interest and long-held stake in the Company, CalSTRS has repeatedly petitioned Facebook's Board on corporate governance issues. For example, on February 7, 2012, CalSTRS wrote a letter to Zuckerberg urging the Company to adopt a "larger, more diverse board."[12] According to Janice Hester-Amey, a Portfolio Manager within CalSTRS' Corporate Governance unit, the petition was sought to protect "long-term, patient money [investors] like CalSTRS" given the proposed stock allocation and the way Zuckerberg "has set up the governance" such that "it will be very hard to influence

[11] Amy Norris, *CalSTRS Seeks to Join Lawsuit to Reform Governance at Facebook*, CALSTRS (Aug. 20, 2019), *available at*: https://www.calstrs.com/news-release/calstrs-seeks-join-lawsuit-reform-governance-practices-facebook.

[12] Letter from Anne Sheehan, Director of Corporate Governance, CalSTRS, to Mark Zuckerberg, Facebook Inc. (Feb. 7, 2012), *available at*: https://www.calstrs.com/sites/main/files/file-attachments/letter_facebook_1.pdf?1495128694.

him except if he's got some kind of a conscience."[13] CalSTRS subsequently encouraged Facebook to adopt certain "best practices," including "[i]ncreas[ing] the diversity of the all-male board to be more reflective of the company's user demographics; [e]qualiz[ing] the voting power of shares to be representative of investors' economic interests; and [s]eparat[ing] the roles of chief executive officer and chair of the board of directors."[14]

38. On April 5, 2018, CalSTRS issued another public statement regarding its efforts to "learn more about what controls are in place [at Facebook] today to protect users' data into the future" and to "understand what additional steps Facebook is taking to protect this data in order to regain the trust of their users, the public, and their shareholders."[15]

---

[13] Paritosh Bansal & Soyoung Kim, *Facebook Governance a Concern for California Pension Fund*, REUTERS (Feb. 6, 2012), *available at*: https://www.reuters.com/article/us-facebook-calstrs/facebook-governance-a-concern-for-california-pension-fund-idUSTRE81601Q20120207.

[14] Richard Duran, *CalSTRS Statement on the Governance Structure at Facebook*, CALSTRS (Feb. 8, 2012), *available at*: https://www.calstrs.com/statement/calstrs-statement-governance-structure-facebook.

[15] Krista Noonan, *CalSTRS Ongoing Engagement with Facebook Focuses on Risk Mitigation*, CALSTRS (April 5, 2018), *available at*: https://www.calstrs.com/statement/calstrs-ongoing-engagement-facebook-focuses-risk-mitigation.

39. The following month, on May 10, 2018, Aeisha Mastagni ("Mastagni"), a Portfolio Manager within CalSTRS' Corporate Governance unit, authored an opinion-editorial in the *Financial Times*, again encouraging the Company to end the dual-class voting shares and adopt the principle of "one share, one vote."[16] According to Mastagni, the "capital structure [of Facebook] has changed [since its IPO] and it is time for its governance to catch up."[17] Mastagni's letter referenced studies by Cornell, the European Corporate Governance Institute, and the SEC. These studies demonstrate that several years after an IPO, "perpetual dual-class stock trades at a substantial discount to dual class stock with a sunset provision."[18]

40. Two days later, on May 12, 2018, Anne Sheehan, the former Director of Corporate Governance at CalSTRS, wrote to Desmond-Hellmann, copying Zuckerberg, regarding its "keen interest to ensure the wealth accumulation in the Company's stock is maintained" and its concern that "[t]he recent scandal around the misuse of personal data pose[d] a significant risk to Facebook . . . [its] customers

---

[16] A. Mastagni, *Facebook's Dual-Class Share Structure is Akin to a 'Dictatorship'*, FINANCIAL TIMES (May 10, 2018) *available at*: https://www.ft.com/content/d22eb6e8-52b4-11e8-b24e-cad6aa67e23e.

[17] *Id*.

[18] *Id*.

. . . [and it's] shareholders."[19] CalSTRS specifically sought information regarding the steps the Company was taking to control and protect user data, and to "regain the trust of your users, the public, and your shareholders."[20]

41. Plaintiff Construction and General Building Laborers' Local No. 79 General Fund ("Laborers' Local No. 79") is a fund operated for the benefit of the over 10,000 members of Construction and General Building Laborers' Local No. 79, which is headquartered in New York, NY. Laborers' Local No. 79 is a shareholder of Facebook and has continuously held its shares at all relevant times hereto and will continue to hold Facebook shares throughout the pendency of this action, and will fairly and adequately represent the interests of other shareholders and the Company in enforcing its rights.

42. Plaintiff The City of Birmingham Retirement and Relief System ("Birmingham Retirement System") provides pension, retirement plans and various other benefits to its participants, and is headquartered in Birmingham, Alabama. The Birmingham Retirement System serves public workers and retirees throughout Birmingham. Birmingham Retirement System is a shareholder of Facebook and has

[19] FB220-00024685 at 24776.

[20] Krista Noonan, *CalSTRS Ongoing Engagement with Facebook Focuses on Risk Mitigation*, CALSTRS (April 5, 2018), *available at*: https://www.calstrs.com/statement/calstrs-ongoing-engagement-facebook-focuses-risk-mitigation.

continuously held its shares at all relevant times hereto and will continue to hold Facebook shares throughout the pendency of this action, and will fairly and adequately represent the interests of other shareholders and the Company in enforcing its rights.

43. Plaintiff Firemen's Retirement System of St. Louis (the "Firemen's Retirement System") owns and has owned shares of Facebook common stock during the entire period of wrongdoing alleged herein. The Firemen's Retirement System provides retirement, disability, death and survivor benefits to active and retired participants and their beneficiaries, and is headquartered in St. Louis, Missouri. The Firemen's Retirement System will fairly and adequately represent the interests of other shareholders and the Company in enforcing its rights.

44. Plaintiff Karen Sbriglio ("Sbriglio") owns and has owned shares of Facebook common stock during the entire period of wrongdoing alleged herein. Sbriglio will fairly and adequately represent the interests of other shareholders and the Company in enforcing its rights.

45. Plaintiff Lidia Levy ("Levy") is a shareholder of Facebook and has continuously held its shares at all relevant times hereto and will continue to hold Facebook shares throughout the pendency of this action. Levy will fairly and adequately represent the interests of other shareholders and the Company in enforcing its rights.

B. Director Defendants

46. Defendant Mark Zuckerberg (previously defined as "Zuckerberg") is the Founder, Chairman and Chief Executive Officer ("CEO") of Facebook. Zuckerberg is responsible for Facebook's day-to-day operations, as well as the overall direction and product strategy of the Company and is the Company's controlling stockholder with ownership of stock and proxies for stock representing more than 57% of Facebook's voting power, though he owns less than 13% of Facebook's total equity value.

47. Defendant Sheryl Sandberg (previously defined as "Sandberg") is Facebook's Chief Operating Officer, having served in that capacity since March 2008. Sandberg has been a member of the Board since June 2012.

48. Defendant Peggy Alford ("Alford") is a member of the Board and has been a director of the Company since May 2019. Since March 2020, Alford has served as Executive Vice President, Global Sales of PayPal Holdings, Inc., a company co-founded by Defendant Peter Thiel. From February 2017 to February 2019, Alford served as Chief Financial Officer and Head of Operations for the Chan Zuckerberg Initiative. Alford is a member of the Board's Audit & Risk Oversight Committee.

49. Defendant Marc L. Andreessen ("Andreessen") is a member of the Board and has been a director of the Company since June 2008. Andreessen is a member of the Board's Audit & Risk Oversight Committee.

50. Defendant Kenneth I. Chenault ("Chenault") was a member of the Board from February 2018 until his decision to not sit for reelection to the Company's Board in May 2020. Chenault was a member of the Board's Audit & Risk Oversight Committee during his time as a director.

51. Defendant Peter A. Thiel ("Thiel") is a member of the Board and has been a director of the Company since April 2005.

52. Defendant Jeffery D. Zients ("Zients") was a member of the Board from May 2018 until his decision to not sit for reelection to the Company's Board in May 2020.

53. Defendant Erskine B. Bowles ("Bowles") was a member of the Board from September 2011 until his decision not to sit for reelection to the Company's Board in May 2019. Bowles was also the Chairman for Facebook's Audit Committee (later known as the Audit & Risk Oversight Committee) from at least April 2013 through May 2019.

54. Defendant Susan Desmond-Hellmann ("Desmond-Hellmann") was a member of the Board from March 2013 until her decision to step down from the

Board in October 2019. Desmond-Hellmann also served as the Company's lead independent director from June 2015 until her departure.

55. Defendant Reed Hastings ("Hastings") was a member of the Board from 2011 until his decision not to sit for reelection to the Company's Board in May 2019. Hastings was also Chairman of the Company's Compensation & Governance Committee from April 2016 until his departure.

56. Defendant Jan Koum ("Koum") was a member of the Board from February 2014, when Facebook acquired his messaging app company, WhatsApp, until his decision not to sit for reelection to the Company's Board in April 2018.

57. Defendants Zuckerberg, Sandberg, Alford, Andreessen, Chenault, Thiel, Zients, Bowles, Desmond-Hellmann, Hastings and Koum are sometimes collectively referred to herein as the "Director Defendants."

C. Officer Defendants

58. Defendant Konstantinos Papamiltiadis ("Papamiltiadis") serves as Facebook's Vice President of Platform Partnerships, a role he was promoted to in March 2020. Papamiltiadis has a long history working on Facebook's strategic partnerships, serving as Director of Platform Partnerships from September 2016 until he was promoted to Vice President, and prior to that, as a Strategic Partner Manager for the Company starting in October 2012.

59. Defendant David Fischer ("Fischer") served as Facebook's Vice President of Business & Marketing Partnerships during the Relevant Period and became Facebook's Chief Revenue Officer in April 2019.

60. Defendant Michael Schroepfer ("Schroepfer") served as Facebook's Chief Technology Officer throughout the Relevant Period.

61. Defendant David Wehner ("Wehner") joined Facebook in 2012 as the Company's Vice President, Corporate Finance and Business planning. Since June 1, 2014, Wehner has served as Facebook's Chief Financial Officer.

62. Defendants Zuckerberg, Sandberg, Koum, Andreessen, Thiel, Fischer, Schroepfer and Wehner are sometimes collectively referred to as the "Insider Trading Defendants."

63. Defendants Zuckerberg, Sandberg, Alford, Andreessen, Chenault, Thiel, Zients, Bowles, Desmond-Hellmann, Hastings, Koum, Papamiltiadis, Fischer, Schroepfer and Wehner are sometimes collectively referred to as the "Individual Defendants."

D. Nominal Defendant

64. Facebook is a Delaware corporation with its headquarters located in Menlo Park, California. Facebook runs a social networking site and platform that allows registered users to create profiles, upload phots and videos, send messages

and communicate with friends, family, and colleagues. The Company's Class A common stock ("Class A Stock") trades on NASDAQ under the symbol "FB."

65. Facebook controls, and is legally obligated to protect, the personal data of over 2.8 billion people. Maintaining the privacy and security of this user data is a mission-critical function for Facebook. If users do not feel their information will be protected from unauthorized disclosure, then they are less likely to share personal information with Facebook or to use the Facebook platform to connect with others for social or transactional purposes; and this, in turn, would result in Facebook having less user data to support its marketing of targeted ad placements to advertisers—whose ad purchases constitute substantially all of Facebook's operating revenue. Indeed, Facebook's "key metrics are calculated using internal company data based on the activity of user accounts . . . including daily active users (DAUs), monthly active users (MAUs) and average revenue per user (ARPU) (collectively, our 'Facebook metrics')." 2019 10-K at 4.

E. Relevant Non-Party Directors

66. Non-party Nancy Killefer ("Killefer"), a Senior Partner at McKinsey & Company from 1992 until her retirement in August 2013, joined Facebook's Board on March 2020. On May 20, 2020, Killefer joined the newly created Privacy Committee and serves as the Chair of that Committee.

67. Non-party Robert M. Kimmitt ("Kimmitt"), a former Deputy Secretary of the Treasury and U.S. Ambassador to Germany, joined Facebook's Board on March 20, 2020, and joined Facebook's Privacy Committee on May 20, 2020. Kimmitt is the "Lead Independent Director" of Facebook but does not serve on the Audit & Risk Oversight Committee or the Compensation, Nominating, and Governance Committee.

68. Non-party Tracey T. Travis ("Travis"), the Executive Vice President and Chief Financial Officer of the Estee Lauder Companies, Inc., joined Facebook's Board in March 2020 and currently serves on its Audit & Risk Oversight Committee.

F. Relevant Non-Party Executives

69. Non-party Lee Atwahl ("Atwahl") served as Facebook's Chief Accounting Officer during the Relevant Period until February 17, 2017.

70. Non-party Sam Lessin ("Lessin") served as Vice President of Product Management for Facebook from March 2014 through September 2014. Until his promotion to the Vice President title, Lessin served as Director of Product Management for Facebook beginning in October 2010.

71. Non-party Christopher Cox ("Cox") served as Facebook's Chief Product Officer during the Relevant Period until he left the Company in March 2019.

72. Non-party Colin Stretch ("Stretch") served as Facebook's Vice President and General Counsel and Secretary during the Relevant Period until May 2019.

73. Non-party Sandy Parakilas ("Parakilas") served as Facebook's Platform Operations Manager from June 2011 to October 2012.

IV. ILLEGAL BUSINESS PLAN ALLEGATIONS

A. The FTC Investigates Facebook's Unfair And Deceptive Privacy Practices, Leading To The 2012 Consent Order

1. *Senators Call For An FTC Inquiry*

74. In 2010, Facebook launched major modifications to the Facebook platform. For example, by April 2010, Facebook had developed an open "Graph API" system, whereby applications ("apps") created by third-parties could not only "write" data (*i.e.*, effectively generate their own personal user information stored on the Facebook platform), but could also "read" (*i.e.*, view and extract) data—including the personal data of Facebook's users—without the knowledge or consent of Facebook's users.[21]

75. Graph API incentivized third-party app developers to create Facebook specific apps by permitting those developers to access Facebook users' data for free,

[21] The capability to both receive ("read") data and submit ("write") data into a system is commonly referred to as "read-write" capability.

such as the private information in user posts and messages. Going beyond the user, Facebook also permitted app developers to collect the information of users' friends even though the friends had not installed the app themselves and were unaware that their information was being shared and collected (at times referred to herein as "Friends data") including personally identifiable information.

76. Access to a users' Friends data was particularly important to third-party developers because it meant that even when users changed their privacy settings to limit app developers' access, developers could still access that users' private information if that users' friend downloaded an app and failed to change their default privacy settings. In addition, Facebook implemented "Instant Personalization," whereby Facebook, pursuant to arrangements it had entered into with certain website operators, would automatically provide a given user's personal information to such operators whenever Facebook users connected to the third party's website. As with the data sharing that Facebook had introduced through its offering of read/write capabilities to third parties via its Graph API system, third parties (for a fee) could also gain access to Facebook users' personal data through the "Instant Personalization" program—all without having to obtain users' consent.

77. Facebook also implemented certain related changes to its privacy policy that further reduced its users' ability to control the dissemination of their personal information. As a result of these developments, by the Spring of 2010,

increasing amounts of Facebook user data were being generated, shared with and provided to third parties automatically, without users' consent.

78. The foregoing changes to the Facebook platform and the Company's privacy policies did not go unnoticed. In particular, they attracted the attention of four United States Senators—Charles Schumer, Michael Bennet, Mark Begich, and Al Franken (the "Senators")—who sent a well-publicized letter to Defendant Zuckerberg on April 27, 2010. That letter expressed the Senators' serious concerns regarding Facebook's platform changes, watered-down privacy policy and the resulting reduction in users' ability to control their own personal information. The Senators' April 2010 letter specifically identified the following three areas of concern:

> 1. **Publicly available data**. Facebook's expansion of publicly available data to include a user's current city, hometown, education, work, likes, interests, and friends has raised concerns for users who would like to have an opt-in option to share this profile information. ***Through the expanded use of "connections," Facebook now obligates users to make publicly available certain parts of their profile that were previously private***. If the user does not want to connect to a page with other users from their current town or university, the user will have that information deleted altogether from their profile. We appreciate that Facebook allows users to type this information into the "Bio" section of their profiles, and privatize it, but we believe that users should have more control over these very personal and very common data points. These ***personal details should remain private unless a user decides*** that he or she would like to make a connection.

2. **Third-party data storage**. Previously, Facebook allowed third-party advertisers to store profile data for 24 hours. ***We are concerned that recent changes allow that data to be stored indefinitely***. We believe that Facebook should reverse this policy, or at a minimum require users to opt in to allowing third parties to store data for more than 24 hours.

3. **Instant personalization**. We appreciate that Facebook is attempting to integrate the functionality of several popular websites, and that Facebook has carefully selected its initial partners for its new "instant personalization" feature. ***We are concerned, however, that this feature will now allow certain third party partners to have access not only to a user's publicly available profile information, but also to the user's friend list and the publicly available information about those friends***. As a result of the other changes noted above, this class of information now includes significant and personal data points that should be kept private unless the user chooses to share them. Although we are pleased that Facebook allows users to opt-out of sharing private data, many users are unaware of this option and, moreover, find it complicated and confusing to navigate. Facebook should offer users the ability to opt-in to sharing such information, instead of opting out, and should make the process for doing so more clear and coherent.[22]

79. The Senators closed their April 2010 letter to Zuckerberg by calling on Facebook to "ensure that its policies protect the sensitive personal biographical data of its users and provide them with full control over their personal information." The Senators also informed Zuckerberg and Facebook that they had called on the FTC to investigate these privacy concerns and asked Facebook to take "swift and productive steps to alleviate the concerns of its users" before the government to force

[22] Emphasis throughout this Complaint has been added, unless otherwise noted.

them to act. Stressing the importance of clarity and transparency, the Senators also specifically asked Facebook to (a) jettison the Company's current practice of requiring users to go through a "complicated and confusing" process to affirmatively ***opt-out*** of Facebook's personal data sharing programs, and to instead (b) provide its users with clear ***opt-in*** mechanisms so that sharing of a user's personal information with third parties would be permitted only with that user's affirmative consent.

80. The Individual Defendants caused Facebook to take no action to address the Senators' request that the Company take voluntary action to remedy their concerns. The FTC, however, took the Senators' concerns seriously, and conducted a significant investigation into what it ultimately concluded were Facebook's "unfair and deceptive practices" with respect to user privacy and third-party access to user information.

2. *The FTC Complaint*

81. The FTC's inquiry into Facebook's practices commenced in or around April 2010. After 19 months of investigation, on November 29, 2011, the FTC issued a press release announcing that it had filed an eight-count complaint against Facebook charging the Company, in sum, with having "deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public."

82. The FTC Complaint described how, since approximately May 2007, Facebook operated its Facebook platform as an interface that enabled third parties to develop, run, and operate Platform Applications that users could interact with online. The FTC further described how Facebook derived revenue from the placement of third-party advertisements on its platform, and from the fees it charged to third-party app developers (who created Platform Applications) for their access to the Facebook platform.

83. The FTC Complaint then went on to describe what it was that made third parties' "access" to the Facebook platform so valuable: namely, the access that it gave them to the trove of personal information that Facebook collected and maintained on its hundreds of millions, and now billions, of users. As the FTC Complaint stated, Facebook "collected extensive 'profile information' about its users," including but not limited to the following:

a. mandatory information that a user must submit to register with the site, including Name, Gender, Email Address, and Birthday;

b. optional information that a user may submit, such as:

   i. Profile Picture;
   ii. Hometown;
   iii. Interested in (*i.e.*, whether a user is interested in men or women);
   iv. Looking for (*i.e.*, whether a user is looking for friendship, dating, a relationship, or networking);
   v. Relationships (*e.g.*, marital or other relationship status and the names of family members);

vi. Political and Religious Views;
vii. Likes and Interests (*e.g.*, activities, interests, music, books, or movies that a user likes); and
viii. Education and Work (*e.g.*, the name of a user's high school, college, graduate school, and employer); and

c. other information that is based on a user's activities on the site over time, such as:

i. a Friend List (*i.e.*, a list of users with whom a user has become "Friends" on the site);

ii. Pages (*e.g.*, any web page on Facebook's web site, belonging to an organization, brand, interest group, celebrity, or other entity, that a user has clicked an online button to "fan" or "like");

iii. Photos and Videos, including any that a user has uploaded or been "tagged in" (*i.e.*, identified by a user such that his or her name is displayed when a user "hovers" over the likeness); and

iv. messages that a user posts and comments made in response to other users' content.

84. Significantly, as the FTC Complaint also observed, this trove of personal information was not simply stored as a part of each Facebook user's online profile, ***but was maintained in a manner so that it could be made accessible to third parties without the user's consent***. The FTC Complaint described how certain user information could be both "read" (accessed) and "written" (generated or changed) by third party Platform Applications, and how such information would also be saved to Facebook's "Graph API"—a database that Facebook created and controlled, and which employed a "social graph" method of organizing and viewing Facebook user

data based on its analysis of connections between users (as tracked via the Facebook platform).

85. The FTC Complaint's descriptions of the nature and extent of Facebook's disregard for its users' privacy was damning. In particular, it described how, beginning at least as early as 2010, Facebook granted third-party Platform Applications access—without user consent—to Facebook's Graph API, including the personal and private information of users stored on that database. ***As the FTC Complaint stated, where Facebook allowed a third-party's Platform Application to access Facebook's Graph API, that third-party would get access to not only the personal information of the user who had decided to utilize the Platform Application, but would also get access to the personal information of the user's "Friends," even if the user had not authorized any such access by the third party***.

86. As discussed further below, this permissive information sharing was formalized amongst Facebook's business partners through a system of agreements known as "whitelisting," and was integral to the Company's business plan to monetize the Facebook platform. Facebook took additional steps to eliminate the ability of its users to curtail or "block" the sharing of their personal information through Platform Applications.

87. The FTC found that Facebook's practices of sharing its users' personal information while falsely assuring them that they could keep their information on

Facebook private, were unfair and deceptive, and in violation of federal law. As the FTC's chair, Jon Leibowitz stated in announcing the filing of the FTC Complaint:

> Facebook is obligated to keep the promises about privacy that it makes to its hundreds of millions of users. Facebook's innovation does not have to come at the expense of consumer privacy. The FTC action will ensure that it will not.

More specifically, the FTC found that Facebook had committed the following eight unfair and/or deceptive practices, in violation of the Federal Trade Commission Act (the "FTC Act"), in connection with Facebook's wrongful sharing of its users' personal and private information without their consent:

i. **Facebook's Ineffective and Deceptive Privacy Settings [FTC Count 1]**. Since at least 2009, Facebook offered its users certain "privacy settings," which purported to allow them to "[c]ontrol who can see your profile and personal information." The settings included the purported ability for users to restrict access to the different categories of "profile information" referenced at ¶83(a-c) above, which purportedly allowed users to "control who can see" their profile information by specifying who can access separate items (*e.g.*, "Only Friends," or "Friends of Friends"). For example, by selecting "Friends Only," a user was consenting to Facebook's ability to share the user's information ***only*** with a specified group of other Facebook users (namely, a list of "Friends" they had affirmatively "Friended"), while a user

selecting "Friends of Friends" was consenting to the sharing of their information only with their Friends and their "Friend's Friends"—while withholding their consent to broader sharing.

However, as the FTC stated, these settings did ***not*** prevent users' personal profile information from being sent to commercial third parties that were neither "Friends" nor "Friends of Friends." Instead, Facebook continued (for a fee) to share its users' personal information with the commercial third parties that had been permitted by Facebook to build Platform Applications into the Facebook platform. As the FTC Complaint further stated at ¶¶14–17, none of Facebook's basic privacy settings pages "disclosed that a user's choice to restrict profile information to 'Only Friends' or 'Friends of Friends' would be ineffective as to certain third parties"—notably, to operators of the Platform Applications that their Friends had used. Indeed, even if a Facebook user chose to "restrict" a "Friends' apps" from access to the user's information, Facebook continued to openly share that user's information with commercial third parties through the Platform Applications that Facebook had approved. Meanwhile, the user's privacy controls would deceptively indicate that the information was not being shared.

ii. **Facebook's Unfair and Deceptive 2009 Privacy Changes [FTC Count 2]**. On November 19, 2009, Facebook changed its privacy

policy to designate certain user information as "publicly available." On December 8, 2009, Facebook began implementing its new privacy policy (the "December 2009 Privacy Changes") to make public certain categories of information that users had previously designated as private.

Before December 8, 2009, Facebook users had been able to use settings to restrict access to certain information from Platform Applications on the Facebook platform. For instance, prior to the December 2009 Privacy Changes, users could, and did, use the "Friends' App Settings" function on Facebook to "block" Facebook Platform Applications that their friends used from accessing any of the user's own profile information (including the user's Name, Profile Picture, Gender, Friend List, Pages and Networks). After December 8, 2009, however, Facebook designated this information as "publicly available information" ("PAI"), such that (a) Facebook users could no longer restrict access to this PAI through the Friends' Apps Settings, and (b) all prior user choices to do so were overridden.

On December 8, 2009, Facebook also eliminated its "Search Privacy Settings," which had previously allowed users to restrict access to their personal information so that others who conducted searches on the Facebook platform would, even if they "found" the user, still be unable to access the user's Profile Picture and Pages information. For example, as of June 2009,

approximately 2.5 million users who had set their Search Privacy Settings to "Everyone" still hid their Profile Picture. After Facebook implemented its December 2009 Privacy Changes, however, users could no longer restrict the visibility of their Profile Picture and Pages through these settings (and all prior user choices to do so were overridden), thereby allowing this personal information to be accessed, without users' consent, through searches conducted by any other Facebook users.

To implement the December 2009 Privacy Changes, Facebook required each user to click through a multi-page notice, called the "Privacy Wizard." The Privacy Wizard required each user to choose either the new privacy settings that Facebook "Recommended" or the user's "Old Settings" with respect to ten types of profile information (*e.g.*, Photos and Videos of Me, Birthday, Family and Relationships, etc.).

In instructing its users to make these choices, Facebook's Privacy Wizard notice represented as follows:

> Facebook's new, simplified privacy settings ***give you more control over the information you share***. We've recommended settings below, but ***you can choose to apply your old settings*** to any of the fields.

However, the Privacy Wizard failed to disclose (i) that users could no longer restrict access to the information that Facebook had newly designated as

"publicly available information" through their Profile Privacy Settings, Friends' App Settings, and Search Privacy Settings, or (ii) that ***users' pre-existing choices to restrict access to such information via these settings would be overridden***. For example, the Privacy Wizard did not disclose that a user's prior choice to share her "Friend List" with "Only Friends" would be overridden, and that such information would become publicly accessible.

As the FTC Complaint alleged, Facebook's representations that it was providing users with "more control over the information you share" and the ability to continue to protect their personal information by choosing to maintain their "old settings" failed to disclose material information to Facebook users. As a result, Facebook's inadequate disclosures and the changes it actually implemented as part of its December 2009 Privacy Changes constituted unfair and deceptive practices pursuant to which its users could no longer restrict access to their Name, Profile Picture, Gender, Friend List, Pages or Networks. Indeed, as the FTC Complaint also pointed out, Facebook's new policy regarding "PAI" also exposed its users to potentially serious harm, including (a) threats to their health and safety as a result of the unauthorized disclosure of a user's location to persons wishing to do the user harm, and (b) prejudice to the user's current or prospective business or employment relations as a result of unauthorized disclosure of the user's

political views, social affiliations or other sensitive personal information to employers, government organizations or business competitors.

iii. **Lack of Users' Informed Consent to the December 2009 Privacy Changes [FTC Count 3]**. In connection with Facebook's implementation of the December 2009 Privacy Changes described above, the FTC Complaint also charged that, by taking certain user profile information that had previously been subject to protection under users' privacy settings and re-designating it as "publicly available information," Facebook had "materially changed its promises that users could keep such information private." The FTC Complaint further stated that Facebook had retroactively applied these changes to personal information it had previously collected from users, and had done so "without their informed consent, in a manner that has caused or was likely to cause substantial injury to consumers, was not outweighed by countervailing benefits to consumers or competition, and was not reasonably avoidable by consumers."

iv. **Facebook's Deceptive Statements Regarding the Scope of Its Platform Applications' Access to User Data [FTC Count 4]**. Facebook repeatedly stated to its users that the Platform Applications that they used would be able to access only the user's "profile information" that those Apps needed to operate. However, contrary to these representations, the FTC

concluded that in many instances Platform Applications were actually given access to users' profile information that was "unrelated to the Application's purpose or unnecessary to its operation." For example, a Platform Application with a narrow purpose, such as a quiz regarding a television show, in many instances could access a user's Relationship Status, as well as the URL for every photo and video that the user had uploaded to Facebook's website—even though such information was plainly irrelevant to the operation or purpose of the Platform Application.

v. **Facebook's Disclosure of User Information to Advertisers In Violation of Its Contrary Representations To Its Users [FTC Count 5]**. Facebook displays advertisements from third parties on its website and across its platform ("Platform Advertisers"). Facebook also allows Platform Advertisers to place "targeted" ads ("Platform Ads") by requesting that Facebook display them to users whose profile information reflects certain targeted information, such as location, age, sex, birthday, "interested in" response (*i.e.*, whether a user is interested in men or women), relationship status, likes and interest, education, and employer name. Facebook derives substantially all of its revenue from selling advertisement placements.

As the FTC Complaint alleged, Facebook repeatedly stated that it did not share personally identifiable information about its users with advertisers. For example, Facebook's November 19, 2009 Privacy Policy stated:

> We don't share information with advertisers without your consent . . . . We allow advertisers to choose the characteristics of users who will see their advertisements and we may use any of the non-personally identifiable attributes we have collected . . . to select the appropriate audience for those advertisements. For example, we might use your interest in soccer to show you ads for soccer equipment, but we do not tell the soccer equipment company who you are . . . . ***[W]e do not share your information with advertisers without your consent*** . . . .

Similarly, Facebook represented that "[w]e do not give your content to advertisers," and that "[t]he only information we provide to advertisers is aggregate and anonymous data" (July 6, 2010 Facebook blog of Defendant Sandberg).

Contrary to these representations, however, Facebook ***did*** share information about its users with its Platform Advertisers, including by identifying for Platform Advertisers the users who clicked on their ads, and those to whom their ads were targeted. In many instances, the unique "User ID" for a user who clicked on a Platform Ad was shared with the Platform Advertiser. As a result, Platform Advertisers could easily use the User ID ***to obtain a user's actual name*** (as well as numerous other pieces of personal user information) by accessing their Profile Page (as well as, after December

2009, their Profile Picture, Gender, Current City, Friend List, Pages and Networks). The Platform Advertiser would also know that the user had the traits that it had targeted in the ad that the user had clicked on (*e.g.*, if the ad targeted 23-year-old men who were "Interested In" men, and "liked" a prescription drug, the Platform Advertiser could associate this information with the user (and the user's actual name)). Advertisers could also combine this information with other data about the user's web browsing habits and responses to advertising over time to build a large amount of additional personally identifiable information about the user's interests and activities.

In addition, Facebook also shared personally identifiable information about its users with third parties that advertised on third-party Platform Applications that had been integrated into the Graph API on the Facebook platform. For example, Facebook identified the specific users who visited these Platform Applications by disclosing the user's User ID, in plain text, to third parties that advertised on a Platform Application. These advertisers could then take steps similar to those that Facebook's Platform Advertisers could take to obtain users' actual names and other personal information.

In short, as the FTC Complaint alleged, Facebook's representations that it did not provide advertisers with information about its users were false and misleading.

vi. **Facebook's Deceptive Verified Apps Program [FTC Count 6]**. Facebook also operated a "verified apps" program, through which it designated certain Platform Applications as "Facebook Verified Apps" ("Verified Apps"). Facebook gave these Verified Apps preferential treatment compared to other Platform Applications. Such preferential treatment included allowing them to display a "Verified Apps badge" (in the form of a conspicuous green check mark) signifying Facebook's verification of the App's "***trustworthy user experiences***," and Facebook's giving them a higher ranking among search results generated on the Facebook platform. An app developer could obtain the Verified App badge simply by paying Facebook $375 (or $175 for a student or nonprofit organization).

Facebook represented to its users that Facebook had conducted a "detailed" review to confirm that "Verified Apps" were "secure, respectful and transparent, and have demonstrated a commitment to compliance with [Facebook] Platform policies." Contrary to Facebook's representations, however, the FTC charged that Facebook took no steps to verify either the security of a Verified App's website or the security the application provided for the user information it collected, beyond such steps that it may have taken regarding any other Platform Application.

vii. **Facebook's Disclosure of User Photos and Videos [FTC Count 7]**. Facebook collects and stores vast quantities of photos and videos that its users upload, including the more than 100 million photos and 415,000 videos that its users collectively upload every day. Facebook assigns each photo and video a content uniform resource locator (or "Content URL") that specifies its location on Facebook's servers. Facebook users and Platform Applications can obtain the Content URL for any photo or video that they view on Facebook's website by simply right-clicking on it. If a user or Platform Application further disseminates this URL, Facebook will provide the user's photo or video to anyone who clicks on the URL.

Facebook had assured its users that, as part of their ability to restrict access to their personal profile information, a given user could terminate other users' ability to access the photos and videos that he or she had uploaded by deleting or deactivating their user account. Contrary to these representations, however, the FTC concluded that Facebook would continue to display a user's photos and videos to anyone who accessed Facebook's Content URLs for them, even after the user had deleted or deactivated their account.

viii. **Facebook's Misrepresentations As To Its Purported Compliance With the U.S.-EU Safe Harbor Framework [FTC Count 8]**. The U.S.-EU Safe Harbor Framework (the "U.S.-EU Framework") provided

a procedure for U.S. companies to transfer personal data outside of the EU without running afoul of EU privacy rules, which generally prohibited the transfer of personal data to countries outside the EU unless the European Commission ("EC") determined that the recipient jurisdiction's laws would adequately protect such data under the EU's "adequacy standards."[23]

The U.S.-EU Framework allowed a U.S. company to lawfully transfer personal data from the EU to the U.S. *if* it certified to the U.S. Department of Commerce that it complied with seven "safe harbor" principles (and related requirements) that were issued by the Commerce Department to satisfy the EU's adequacy standard. These principles included (1) a ***notice requirement*** (which required companies to inform individuals about the purposes for which it collected and used information about them, the types of third parties that it disclosed the information to, and the choices that the business gave individuals to restrict the use or disclosure of their information); and (2) a ***choice requirement*** (which required companies to allow individuals to opt-out of any personal information collection practices where the information

[23] The original U.S.-EU Framework, which came into effect in 2000, has since been replaced by a later framework, the EU-U.S. Privacy Shield Framework, which was adopted in July 2016.

might be disclosed to a third party, or used for a purpose unrelated to the reasons for which the information was originally collected).

Facebook self-certified to the Commerce Department that its transfers of data on its EU users to the U.S. "for processing" complied with the U.S.-EU Framework—and also repeatedly stated in its Privacy Policy that it participated in, adhered to, and/or complied with that Framework. However, as the FTC concluded: (a) "in many instances" Facebook failed to adhere to the Framework and U.S.'s safe harbor "notice and choice" requirements, and (b) as a result, Facebook's representations that it complied with the Framework or the related "notice and choice" requirements constituted deceptive acts or practices.

88. Facebook did not contest the FTC's investigative findings or the charges for violations of the FTC Action, and chose to enter into a consent decree with the FTC. The terms of that decree—which became final in 2012 following a notice and comment period and final approval by vote of the FTC Commissioners—are discussed below.

3. *The Terms Of Facebook's 2012 Consent Order*

89. On the same day (November 29, 2011) that the FTC published its Complaint, the FTC also announced that Facebook had agreed to settle the charges via a consent decree, the terms of which were also published by the FTC on

November 29. The FTC's November 29, 2011 Press Release summarized the proposed settlement that it "bars Facebook from making any further deceptive privacy claims, requires that the company get consumers' approval before it changes the way it shares their data, and requires that it obtain periodic assessments of its privacy practices by independent, third-party auditors for the ***next 20 years***." As the release further stated, under the settlement Facebook would be:

- barred from making misrepresentations about the privacy or security of consumers' personal information;
- ***required to obtain consumers' affirmative express consent before enacting changes that override their privacy preferences***;
- required to prevent anyone from accessing a user's material more than 30 days after the user has deleted his or her account;
- ***required to establish and maintain a comprehensive privacy program designed to address privacy risks*** associated with the development and management of new and existing products and services, ***and to protect the privacy and confidentiality of consumers' information***; and
- required, within 180 days, and every two years after that for the next 20 years, to obtain independent, third-party audits certifying that it has a privacy program in place that meets or exceeds the requirements of the FTC order, and to ensure that the privacy of consumers' information is protected.

90. An addendum to the release further clarified:

> A consent agreement is for settlement purposes only and does not constitute an admission by the respondent that the law has been violated. ***[However,] [w]hen the Commission issues a consent order on a final basis, it carries the force of law with respect to future actions***. Each violation of such an order may result in a civil penalty of up to $16,000.

91. By its final Decision and Order dated July 27, 2012, FTC Docket No. C-4365, Document No. 0923184, the FTC issued the consent decree as an order (previously defined the "2012 Consent Order"), without any modifications to the terms of the original version first published on November 29, 2011. A copy of the Consent Order as entered is attached hereto as Exhibit A.

92. Under the Consent Order, Facebook agreed to comply with a number of specific obligations for a period of twenty years (*i.e.*, until July 27, 2032). These obligations set forth mandatory rules and procedures that Facebook would be required to adhere to, notably with respect to what the Consent Order referred to as "Covered Information" and "Nonpublic user information." The Consent Order defined these two broad categories of user information as follows:

- "**Covered Information**" shall mean information from or about an individual consumer including, but not limited to: (a) first or last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a mobile or other telephone number; (e) photos and videos; (f) Internet Protocol ("IP") address, User ID or other persistent identifier; (g) physical location; or (h) any information combined with any of (a) through (g) above.

- "**Nonpublic User Information**" shall mean Covered Information that is restricted by one or more privacy setting(s).

93. Using this nomenclature, the Consent Order imposed the following nine legal obligations on Facebook [all emphases added]:

i. [***Prohibition Against Future Misrepresentations of Facebook's Privacy and/or User Information Policies and Practices***] "[Facebook] and its representatives . . . 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:

- its collection or disclosure of any Covered Information;
- 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;
- the extent to which [Facebook] makes or has made Covered Information accessible to third parties;
- the steps [Facebook] takes or has taken to verify the privacy or security protections that any third party provides;
- the extent to which [Facebook] makes or has made Covered Information accessible to any third-party following deletion or termination of a user's account with [Facebook] or during such time as a user's account is deactivated or suspended; and
- the extent to which [Facebook] is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy, security, or any other compliance program sponsored by the government or any third party, including, but not limited to, the U.S.-EU Safe Harbor Framework."

ii. [***Obligation to Obtain User's Affirmative Consent Before Sharing Their Nonpublic Information With Third Parties***] "[Facebook] and its representatives . . . ***prior to any sharing*** of a user's Nonpublic User

Information by [Facebook] with any third party, which materially exceeds the restrictions imposed by a user's privacy setting(s), shall:

> A. ***clearly and prominently disclose*** to the user, separate and apart from any "privacy policy," "data use policy" . . . or other similar document: (1) the categories of Nonpublic User Information that will be disclosed to such third parties, (2) the identity or specific categories of such third parties, and (3) that the sharing exceeds the restrictions imposed by the privacy settings; ***and***
>
> B. ***obtain the user's affirmative express consent***."

iii. [***Prohibition on Third Party Access to User Information After User Has Deleted It or Terminated Their Account***] "[Facebook] and its representatives shall . . . implement procedures reasonably designed to ensure that Covered Information cannot be accessed by any third party from servers under [Facebook's] control after . . . thirty (30) days from the time that the user has deleted such information or deleted or terminated his or her account . . . ."

iv. [***Obligation to Implement Comprehensive New Privacy Program.***] "[Facebook] shall . . . establish, 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. Such program, the content and

implementation of which must be documented in writing, shall contain controls and procedures appropriate to [Facebook]'s size and complexity, the nature and scope of [Facebook]'s activities, and the sensitivity of the Covered Information, including:

- the designation of an employee or employees to coordinate and be responsible for the privacy program;
- the identification of reasonably foreseeable, material risks . . . that could result in [Facebook]'s unauthorized collection, use, or disclosure of Covered Information and an assessment of the sufficiency of any safeguards in place to control these risks . . . ;
- the design and implementation of reasonable controls and procedures to address the risks identified through the privacy risk assessment, and regular testing or monitoring of the effectiveness of those controls and procedures;
- the development and use of reasonable steps to select and retain service providers capable of appropriately protecting the privacy of Covered Information they receive from [Facebook] and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such Covered Information; and
- the evaluation and adjustment of [Facebook]'s privacy program in light of the results of the testing and monitoring required [above], any material changes to [Facebook]'s operations, or any other circumstances [Facebook] knows or has reason to know may have a material impact on the effectiveness of its privacy program."

v. [***Obligation to Obtain Independent Biennial Assessments of Facebook's Reformed Privacy Program***.] "[I]n connection with its compliance with Part IV of this order, [Facebook] shall obtain initial and

biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional . . . . Each assessment shall (A) set forth the specific privacy controls that [Facebook] has implemented and maintained during the [relevant biennial] reporting period; (B) explain how such privacy controls are appropriate to [Facebook]'s size and complexity, the nature and scope of [Facebook]'s activities, and the sensitivity of the Covered Information; (C) explain how the privacy controls that have been implemented meet or exceed the protections required by Part IV of this Order; and (D) certify that the privacy controls are operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of Covered Information and that the controls have so operated throughout the reporting period."

vi. [***Obligation to Maintain Records Relating to User Data Privacy and Security***] "[Facebook] shall maintain and upon request make available to the [FTC] for inspection and copying, a . . . copy of:

- for a period of three (3) years from the date of preparation or dissemination, . . . all widely disseminated statements by [Facebook] or its representatives that describe the extent to which [Facebook] maintains and protects the privacy, security, and confidentiality of any Covered Information . . . ;
- for a period of six (6) months from the date received, all consumer complaints directed at [Facebook] or forwarded to

[Facebook] by a third party, that relate to the conduct prohibited by this order and any responses to such complaints;

- for a period of five (5) years from the date received, any documents, prepared by or on behalf of [Facebook], that contradict, qualify, or call into question [Facebook]'s compliance with this order;

- for a period of three (3) years from the date of preparation or dissemination . . . each materially different document relating to [Facebook]'s attempt to obtain the consent of users referred to n Part ii above, along with documents and information sufficient to show each user's consent; and documents sufficient to demonstrate, on an aggregate basis, the number of users for whom each such privacy setting was in effect at any time [Facebook] has attempted to obtain and/or been required to obtain such consent; and

- for a period of three (3) years after the date of preparation of each Assessment required under Part (v) of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of [Facebook], including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, for the compliance period covered by such Assessment."

vii. [***Obligation to Ensure that All Current and Future Officers, Directors and Managers are aware of Facebook's Obligations under the Consent Order.***] "[Facebook] shall deliver a copy of this order to (1) all current and future principals, officers, directors, and managers; (2) all current and future employees, agents, and representatives having supervisory responsibilities relating to the subject matter of this order; and (3) any business entity resulting from any change in [corporate] structure set forth in Part (viii).

[Facebook] shall deliver this order to such current personnel within thirty (30) days . . . and to such future personnel within thirty (30) days after the person assumes such position or responsibilities."

viii. [***Duty to Update FTC on Material Corporate Changes***.] "[Facebook] shall notify the FTC within fourteen (14) days of any change in [Facebook's corporate structure] that may affect compliance obligations arising under this order . . ." and

ix. [***Reporting obligations concerning compliance with Consent Order***.] "[Facebook], within ninety (90) days . . . shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of their own compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, [Facebook] shall submit additional true and accurate written reports."

B. Zuckerberg Responds To The FTC's November 2011 Announcements By Falsely Asserting Facebook's Innocence

94. On November 29, 2011, Defendant Zuckerberg, on behalf of Facebook, issued an extraordinary response to the FTC's press release, the FTC Complaint, and the disclosure of the terms of the 2012 Consent Order that Facebook had itself agreed to. As further detailed below, this response, in the form of a blog post (the "2011 Facebook Response") (attached hereto as Exhibit B), contained a host of materially

false and misleading statements concerning (a) the Company's past and future privacy controls (and its users' ability to control how their information was or would be shared), and (b) the facts and circumstances that led to the filing of the FTC Complaint and Facebook's settlement and agreement to enter into the 2012 Consent Order.

1. *Zuckerberg's November 2011 Misrepresentations As To Users' "Complete Control" Over Their Information, And Related False And Misleading Statements*

95. In effectively denying the FTC's allegations that Facebook had ever been insufficiently committed to user privacy or that it really needed to modify any of its privacy practices, Zuckerberg made the following materially false and misleading statements regarding Facebook's privacy practices in the 2011 Facebook Response:

- "I founded Facebook on the idea that people want to share and connect with people in their lives, but to do this ***everyone needs complete control over who they share with at all times***."
- "***With each new tool, we've added new privacy controls to ensure that you continue to have complete control over who sees everything you share***. Because of these tools and controls, most people share many more things today than they did a few years ago."
- "***Facebook has always been committed to being transparent about the information you have stored with us***—and we have led the internet in building tools to give people the ability to see and control what they share."

- "***I'm committed*** to making Facebook the leader in transparency and control around privacy. For Facebook, ***this means we're making a clear and formal long-term commitment to do the things we've always tried to do and planned to keep doing—giving you tools to control who can see your information and then making sure only those people you intend can see it***."

- "As a matter of fact, ***privacy is so deeply embedded in all of the development we do*** that every day tens of thousands of servers' worth of computational resources are consumed checking to make sure that on any webpage we serve, that you have access to see each of the sometimes hundreds or even thousands of individual pieces of information that come together to form a Facebook page. This includes everything from every post on a page to every tag in those posts to every mutual friend shown when you hover over a person's name. ***We do privacy access checks literally tens of billions of times each day to ensure we're enforcing that only the people you want see your content***. These privacy principles are written very deeply into our code."

96. However, users patently did not have "complete control" over the sharing of their own personal information on the Facebook platform as of November 2011—nor had they had such control for many years. As set forth in the 2012 Consent Order, Facebook shared its users' personal information with third parties, including third-party Platform Applications used by a user's friends, for which the user could not possibly have given consent. Facebook even went so far as to override prior user privacy preferences in order to advance its ability to share user information with third parties. And, as later events would only confirm, Zuckerberg's statements that he or the Company were "committed" to user privacy and giving users "control" over their information (or that such concerns were somehow "embedded in all of the

development we do") were simply ***false,*** and Facebook would fail to take any step to meaningfully reform its glaringly deficient privacy policies and information sharing practices after entry of the 2012 Consent Order. Indeed, over the following years, Facebook surreptitiously ***expanded*** its lucrative "whitelisting" and other data sharing practices—which became only further embedded in Facebook's business plans—while Facebook simply thumbed its nose at the FTC and its legally binding obligations under the 2012 Consent Order to ensure that Facebook would not share its users' information with third parties unless Facebook obtained the user's affirmative and express consent to do so. *See infra* §§IV.C-F.

97. Moreover, as Zuckerberg admitted, Facebook users relied on the Company's representations about protecting user privacy. Zuckerberg's November 2011 false assurances and other misleading statements induced users to share *more information* than they otherwise would have. Indeed, Zuckerberg's November 2011 statements were made for the express purpose of falsely reassuring Facebook users that Facebook was committed to ensuring that its users had (and would continue to have) "complete control" over their personal information and its dissemination to third parties, when in fact the Company's real commitment was to increasing its profits by secretly *expanding* its information-sharing practices, in blatant disregard of its legally binding obligations under the 2012 Consent Order.

2. *Zuckerberg's November 2011 Misrepresentations As To The FTC Complaint And The Circumstances Of The FTC Agreement*

98. Zuckerberg's November 11 comments also materially misrepresented the scope and nature of the Company's privacy violations in order to mislead the public as to the seriousness of the circumstances that caused Facebook to enter into the 2012 Consent Order. For example, Zuckerberg made the following false and misleading statements in the 2011 Facebook Response:

- "That said, I'm the first to admit that ***we've made a bunch of mistakes. In particular, I think that a small number of high profile mistakes***, like Beacon four years ago ***and poor execution as we transitioned our privacy model two years ago, have often overshadowed much of the good work we've done***."

- "Recently, the US Federal Trade Commission established agreements with Google and Twitter that are helping to shape new privacy standards for our industry. Today, the FTC announced a similar agreement with Facebook. ***These agreements create a framework for how companies should approach privacy in the United States and around the world***."

- "In addition to these product changes, ***the FTC also recommended improvements to our internal processes. We've embraced these ideas, too, by agreeing to improve and formalize the way we do privacy review as part of our ongoing product development process.*** As part of this, we will establish a biennial independent audit of our privacy practices to ensure we're living up to the commitments we make."

- "***Today's announcement formalizes our commitment to providing you with control over your privacy and sharing***—and it also provides protection to ensure that your information is only shared the way you intend. As the founder and CEO of

> Facebook, I look forward to working with the Commission as we implement this agreement. It is my hope that this agreement makes it clear that Facebook is the leader when it comes to offering people control over the information they share online."

99. Zuckerberg's statements were false and misleading because they misrepresented Facebook's history of rampant privacy violations as attributable to nothing more than a "small number of high profile mistakes" and "poor execution" in implementing its December 2009 Privacy Changes—especially given that it was Facebook's all-too-effective implementation of those Privacy Changes that was at the core of Facebook's deceptive trade practices. Further, Zuckerberg falsely presented the 2012 Consent Order as a cooperative agreement entered into with the FTC in order to establish a prospective framework for technology companies to approach privacy in the United States, and not the true nature of the agreement—an agreement to settle a detailed eight-count complaint with obligations placed on the Company to resolve outstanding privacy violations.

C. Facebook Concocts And Implements A Business Plan Based On Monetizing Increasing Amounts Of Personal User Information Immediately Following Entry Of The 2012 Consent Order

100. Within three months of the final entry of the 2012 Consent Order, Zuckerberg and Sandberg began discussions with other Facebook executives about modifying the Facebook platform to allow for the broader sharing of personal information with third parties. As internal Company emails show, Zuckerberg,

Sandberg, and other high-ranking Facebook executives sought to—and ultimately successfully—develop the Facebook platform into a broker of user information, turning the vast amount of information gathered by Facebook from user interaction on the platform into an economy of scale.

101. These changes caused the Facebook platform to become a vehicle that allowed it to trade in, collect and retain ever larger amounts of increasingly valuable personal information on Facebook users as they interacted with an expanding number of third-party apps on the Facebook platform. As shown below, this cunning business plan allowed Facebook to surreptitiously collect—through unfair, deceptive and illegal trade practices in violation of the Consent Order—unprecedented amounts of personal information on its users that Facebook, in turn, used to sell ad placements and generate billions of dollars in ill-gotten profits.

102. Zuckerberg, Sandberg, and Facebook executives decided to completely open Facebook's Graph API to hundreds of companies, so that Facebook could fully share any information generated by third-party Platform Applications, while allowing those Platform Applications full access to user data, conceptualized by Zuckerberg as "full reciprocity." Under this scheme, the Individual Defendants permitted Facebook to gain full access to personal user information generated and collected by an ever-growing number of third-party Platform Applications (which would track user activities on those apps), while Facebook, in turn, would allow

those Platform Applications full access to Facebook's user data. In connection with their scheme, the Individual Defendants determined to cause Facebook to engage in "white-listing," or allowing Facebook affiliates and close partners full and open access to Facebook's APIs.

1. *Zuckerberg Develops A Business Plan To Monetize Personal User Information By Granting Third-Party Access To Facebook's Graph API*

103. On October 7, 2012, Mike Vernal ("Vernal"), then Facebook's Vice President of Search, Local, and Developer Products and a co-creator of Facebook's Graph API and other key projects, wrote an October 12, 2012 email summarizing the views of Zuckerberg and other high-ranking Facebook executives with respect to Facebook's "platform business model." Within three months of entry into the 2012 Consent Order, as Vernal summarized, Zuckerberg had concluded that Facebook should adopt a business model under which it would sell all personal user information, including the information of a user's friends, to Platform Applications for either: (i) a flat rate of $0.10 per user each year, or (ii) a payment-in-kind by allowing developers of Platform Applications to "pay" Facebook back by importing additional user information the third party was able to collect through the Platform Application back into the Facebook platform. In this way, Facebook would establish one of the world's largest collections of personal user information, and become a "broker" that capitalizes on the personal user information, as an "information bank."

104. Vernal's October 2012 email, quoting an earlier email from Zuckerberg, stated:

> A basic model could be:
>
> - Login with Facebook is always free
> - Pushing content to Facebook is always free
> - ***Reading anything, including friends, costs a lot of money. Perhaps on the order of ~$0.10 / user each year***.
>
> For the money that you owe, you can cover it in any of the following ways:
>
> - Buy ads from us in neko [an acronym for Facebook's advertising platform] or another system
> - Run our ads in your app or website (canvas apps already do this)
> - Use our payments
> - Sell your items in our Karma store
>
> Or if the revenue we get from those doesn't add up to more than the fees you owe us, then you just pay us the fee directly.
>
> ***The rate of $0.10 / user each year might even be too low. For example, at that rate Spotify would have to spend just $3m per year with us in ads to be even and Pinterest would be around there too. We might be able to get this number to be meaningfully higher, especially if we don't charge until a dev has a meaningful number of users, like 50k or 100k***.
>
> ***I've been reading a lot of books on finance and banking recently, and even though the idea of an information bank is not identical to a financial bank, the comparison suggests some interesting things***.
>
> For example, banks charge you interest for as long as you have their money out. ***Rather than letting devs pay a one time fee to fetch data, we could effectively do this [i.e., charge interest] by mandating that devs must keep data fresh and update their data each month for anything they call***.

> Another idea is charging different developers different rates for things. The whole banking industry is based on charging people different rates. It may be that instead of having a flat fee for everyone, we should instead try [to] set a norm w[h]ere there's some range but the expectation is each developer gets some rate specific to them once they're at scale.

105. Facebook's then-Vice President of Product Management, Sam Lessin, further developed the concept of platform information sharing with Zuckerberg through a series of emails beginning October 26, 2012 laying out, in detail, the ways in which Facebook would maintain control over a user's personal information, like a broker, and make decisions on how unique user IDs and other personal user information would be shared with third parties developing Platform Applications on the Facebook platform. Lessin began the email chain, entitled, "re: notes on platform," by identifying steps that Facebook could take with respect to its platform in the short-term to begin implementing Zuckerberg's vision of generating increased profits through the sale or exchange of personal user information.

106. For example, Lessin in his October 26, 2012 email recommended to Zuckerberg that Facebook:

> (1) allow Platform Applications to write (*i.e.*, submit data, including personal user information) to Facebook's Graph API freely;
>
> (2) allow Platform Applications to use "Facebook login" freely and "have many avenues to getting user's IDs." This included (a) giving "any app" access to a user's ID in plaintext, not a hashed (or encrypted) ID; and (b) allowing "any app" to access additional pieces of information to uniquely identify users

through, *e.g.*, "email matching," "invisible pixels," "cookies," and "mobile tracking" (which are all methods for Platform Applications to surreptitiously gather additional personal user information);

(3) allow Platform Applications to read (*i.e.*, access and obtain) Facebook's "Basic [User] Information" freely, which includes identifying a user and his or her friends through a list of User IDs of the user and that user's friends who also use the Platform Application;

(4) develop a method for Platform Applications to read/use "***non-basic*** information and functions." Lessin further recommended that Facebook develop a "whole set of non-basic information datasets and APIs," ***including additional user data Facebook could provide to Platform Applications that a user would not themselves provide as part of registration for the Platform Application***, and which other services could not provide. Lessin also suggested that ***Facebook become a "brokering business"*** where Platform Applications could provide personal user information to other Platform Applications, ***with Facebook "run[ning] a marketplace in-between"***;

(5) openly provide the "data sets" of personal user information Facebook collected (as referenced immediately above at subsection (4)), including through Platform Applications, to advertisers via ad-targeting and other distribution channels. ***Lessin further described provision of these APIs as "best thought of as white-list / internal APIs which if you are owned by us, or a close ally, we will open them up for you"***; and

(6) exclude competitors from sharing of APIs. Although Lessin recommended that Facebook "share" personal user information with chosen third party app developers via Facebook's APIs who would be approved and identified on a "white list." Lessin also recommended, conversely, that Facebook "increase enforcement of competitive exclusions," to prevent Facebook's competitors from gaining access to that information.

107. While Lessin's October 26, 2012 email to Zuckerberg described an aggressive plan for Facebook to profit from the wholesale sharing of both "basic" and "non-basic" personal user information, including additional information that Facebook would collect directly from third-party Platform Applications that were plugged into the Facebook platform, conspicuously absent from such planning was any mention of the requirements of the 2012 Consent Order.

108. The obligations imposed on Facebook under the 2012 Consent Order were equally absent from Lessin's discussion, in the same email chain, of the overall goal of Facebook's plans to engage in wholesale sharing of personal user information: namely, the ability of Facebook to reap huge profits in its role as a broker and seller of its users' personal information. As detailed in Lessin's October 2012 email to Zuckerberg, Lessin included a four-part series of objectives he called his "Upshot," Facebook would become:

> --(1) an open, stable, and free platform for writing data to Facebook, ***getting the information you need to wire up a set of users you have engaged, and all the IDs / hooks you need to actively participate in our attention market (buy ads) as well as leverage any other services like payments or an ad-network we may want to offer in the future***.
>
> --(2) an ***ever increasingly valuable set of proprietary APIs for richer information***, etc. which are not openly available beyond perhaps a 'free sample', but which allow us to 'project' into the ecosystem the value of a *hopefully* ever deeper data-sets.[] giving us the ability *hopefully* to participate in a variety of deeply socially enabled businesses which ideally we would build

ourselves if we could, but in a heterogeneous enough set of industries with different margins and properties that it would be impossible for us to price effectively.

--(3) we have some 'starter' APIs which are free, and then we try to directly associate the cost of a given API for a developer with the API's value to that developer, rather than trying to subsidize one API with another, or put developers in a hard to measure / opaque position where they don't exactly know if using platform holistically is worth it to them[] so where there is an easy way to do that (advertising on FB, ad network on app partner, payments API) we can have very transparent pricing, and where it is not easy to do that we have to have a conversation / negotiate.

--(4) ***the messaging to the ecosystem becomes that we are deprecating a few things for privacy reasons / to simplify our model for users, we are enforcing non-competitive terms we have always had, and we are opening up a series of new white-list APIs for the best companies that want to build the best social services and want to work with us deeply***.

109. Lessin thus proposed sharing user IDs and an "ever increasingly valuable set of proprietary APIs" containing personal user information with third-party developers, based solely on a financial assessment of Facebook's ability to monetize that data. Tellingly, Lessin discussed personal privacy only in the context of "messaging," thereby providing cover for Facebook to charge third parties for personal information and APIs that had previously been free to developers of Platform Applications. In sum, Lessin envisioned a "series of new white-list APIs," which would greatly expand Facebook's capabilities to both collect and share personal user information with third parties without user consent.

110. Lessin also went on to note that Facebook had reached, or was about to reach an endpoint with respect to its ability to continue to grow revenue based on Facebook's value as a distribution platform. Accordingly, Lessin explicitly premised Facebook's future profitability on its ability to monetize the only resource Facebook could continue to generate, and share, at scale and in ever-increasing quantities: personal user information. As Lessin wrote:

> ***[W]e are .running out of humans (and have run-out of valuable humans from an advertiser perspective)*** (3) brand advertisers will get better, but they aren't that good at measuring their spend, so they have finite budgets. -- ***The upshot of which is that while being 'big' does provide us a return on scale currently, it isn't something which we are going to be able to more than 2X-4X in my mind anytime soon***, and in some ways I think we will face increasing pressure on the value we derive from our distribution scale.
>
> ***The second thing which we provide which is non commodity / where there *may be* return on scale is 'information' about people*** . . . [T]his is far less tried and true than the return on scale of distribution, which is well understood and practiced . . . ***but as far as I can tell, it is the bet we need to make as a company if our ambitions are long-term and grand, and to me at least it feels right***.
>
> * * *
>
> ***The challenge comes in not when we use the scale of our own information to drive our own business platform, but when we try to leverage the information with other parties to the system / business*** . . .

111. As Lessin's email to Zuckerberg makes clear, Facebook's wholesale generation, sharing and monetization of User IDs, "basic" personal user information,

and "non-basic" personal user information would be the way for Facebook to maximize profits going forward:

> ***Converting information into better 'merchandizing' means giving a third party the data to use as they see fit. There should be a bunch of value here . . . .***
>
> * * *
>
> Applications *should be allowed* to use 'Facebook login' freely & have many avenues to getting user's IDs
>
> - ***Applications currently use Facebook connect by-in-large in order to (1) get the 'friend' graph*** that enables their service to be compelling, (2) get the publication rights that resolve to free distribution for them (3) sometimes for the minor benefit of speeding signup* (though in reality FB converts worse than non-FB signup in many cases now) (4) sometimes for the minor benefit of providing easier login for users, (5) ***in a very few cases for specific access to a specific type of Facebook data (photos, etc.)***[] what they don't do in general is implement Facebook login in order to get user's UIDs and thereby better engage/re-engage them, advertise more effectively, and/or in order to use things like a connect payments solution or get high CPMs/CPCs on a future tense advertising network. The trade we should be pushing on / trying to establish with companies is not that Facebook login is in-and-of-itself good, but that by doing it we end up providing you as a company easy to understand, and easy to value benefits either on the cost side or the revenue side of your business. --- UPSHOT: Right now I believe that if you asked an application to implement Facebook connect but didn't give them the friend graph, publication rights in the same dialog, etc. people would have no reason for implementing it at all. There is no direct value for implementing FB connect. I think that as we add / if we add good service on top of FB connect / having users logged in like payments/ad network (which monetize on their own obviously) and better paid acquisition channels (which are easy to create a marketplace around and are easy for apps to measure / evaluate, then we have businesses in those areas, and we will want FB connect distributed as widely as possible / we will not want to charge for it.

Applications *should be allowed* to read basic information freely

- ***Applications currently get a bunch of 'basic information' and users are not confronted with exactly what they are giving to apps. We give out a lot of things under 'basic information', some of which really weaken our competitive position like 'email addresses' by opening up a non-facebook channel for applications to reach out to users***. This has troubled me greatly; however, ***I have come to terms with the fact that for friends already using the app, we simply can't remove what we have already promised and enabling the function provides a ton of user value / value for the world*** while still making the app go back through our platform for real new-user acquisition. For things like email, name, profile photo, etc[] making these signup elements slightly easier for an app certainly erases some cost / makes the app more valuable, but ***we really aren't in competitive landscape where these things have meaningful value / where we could charge a lot for them. First, a user will just give them to the app if the app is good. Second, tons of other people like apple can now give out the same information. --- UPSHOT, we should give this information away because it has become worthless to us and allowing users to give away their own basic info provides value to them***.

Applications *should be allowed* to read/use non-'basic' information & functions with some key caveats

- ***A scant few applications currently really use any of the APIs we offer beyond the basic information APIs. Most of the companies that use these APIs (message send, photos export, feed.get, etc.) exist in a competitive grey zone*** [] generally speaking though, there isn't currently all that much more you can do with our platform (though we have contemplated a lot of things that would add a lot of value to other partners). ***This is the category where I would put all my eggs in terms of building a dataset which has real return-on-scale dynamics / our actual information monetization scheme[] As we build up value in this type of data we should certainly / will certainly feed it into the market-mediated ads system. That should easily create more value for all if enabled widely[] the question is who do we give the actual data out to and on what terms. here we face an issue[]. which is that the same data is just worth massively different amounts to different***

> ***players. If we price it too high apps will not consume it, if we price it too low we are giving away one of our only scaleable profit centers. If we give it to competitors we are sewing the seeds of our own destruction[] and if we give it out on any general model we are going to lose the ability to effectively negotiate with people where we really want a piece of the action / a tight business. – UPSHOT, we should sell this, but I just don't see any way we can sell it on standard terms***.

112. Lessin's email to Zuckerberg ultimately concluded that (1) Facebook should freely share through many avenues User IDs, or unique identifying information allowing a company to track and gather together all information collected about a particular user, and a user's "friend graph," or the identity of all of a user's friends, to demonstrate Facebook's value to its partners; (2) Facebook should freely share "basic information" like user emails, names, sex, profile photos, addresses, and more, because the information was of low commercial value to Facebook; and (3) Facebook should develop and monetize additional "non-basic information" by developing its Graph APIs to allow for even more invasive and granular data-sharing, and create a monetization scheme by contract with certain partners not in competition with the Company, in order to effectively continue to monetize such information as a "scaleable profit center[]."

113. Zuckerberg responded to Lessin's October 26, 2012 email the next morning. Zuckerberg boiled Lessin's email down to "three main questions":

(1) What is a revenue model that scales to build the kind of business we want?

(2) What is a read model that reduces the strategic risk to our business (and doesn't undercut that revenue growth)?

(3) What is a model that developers will participate in rather than abandoning?

In answering these questions, Zuckerberg went on to conclude that, "whatever we do needs to be very widely adopted," because it was untenable for Facebook to be in a position with 10-20 partnerships, with Facebook owning 10-20% of those companies. Zuckerberg went on to ponder how Facebook could get developers to "buy in" to the Facebook ecosystem—a way to give developers access to Facebook's distribution services in exchange for information created through their Platform Applications.

114. Nowhere did Zuckerberg mention user privacy as a topic worthy of concern in crafting Facebook's business model throughout the October 27, 2012 email. Instead, ***Zuckerberg indicated that he was aware that Facebook was leaking valuable user information to developers, but was unperturbed as long as the information did not provide a strategic risk to Facebook's business model***. And yet, the only way Zuckerberg approached the topic of controlling access to user information was in discussing how Facebook could maintain control over the user information in its ecosystem to prevent developers from sharing that information with each other, cutting out Facebook as the middleman:

> For (2) [What is a read model that reduces the strategic risk to our business (and doesn't undercut that revenue growth)?]:
>
> I'm getting more on board with locking down some parts of platform, including friends' data and potentially email addresses for mobile apps.
>
> ***I'm generally skeptical that there is as much data leak strategic risk as you think. I agree there is clear risk on the advertiser side, but I haven't figured out how that connects to the rest of platform. I think we leak info to developers, but I just can't think of any instances where that data has leaked from developer to developer and caused a real issue for us. Do you have examples of this?***

Zuckerberg then went on to conclude that, because the strategic risk of information sharing from one developer to another was small, Facebook should continue to expansively share user information, even to the Company's competitors:

> I also think your argument about not selling down our advantage is too rigid. ***Businesses pay for new customer acquisition and then for reengagement. Eventually you run out of new customers and need to focus more on reengagement. We shouldn't prevent ourselves from helping business get new customers just because one day they might run out of new customers to acquire. It doesn't scale infinitely, but it does scale pretty far.***

115. From this discussion, Lessin and Zuckerberg came to the conclusion that Facebook would have a two-tier information sharing system, "where some APIs are widely available at scale, [] but there are a set of APIs that really are just for partners." Facebook would allow a vast swath of user information to be generally available to the Company's third-party Platform Application developers, advertisers, and other third parties, but reserve some APIs to a class of "partners" whom Facebook had formed closer strategic relationships with. In exchange, Facebook

would be able to obtain "a ton of value" that would all funnel through Facebook as a distribution and advertising platform.

2. *Zuckerberg And Sandberg Decide On A Business Model Of "Full Reciprocity," Allowing Access To Personal User Information with Facebook Being The Broker*

116. Shortly after Lessin and Zuckerberg had their exchange on Facebook's business model, Zuckerberg and Sandberg decided that the principle of "full reciprocity" of information sharing, including access to app friends (one of the practices identified as illegal in the 2012 Consent Order), would be in the Company's interest moving forward from the 2012 Consent Order. "Full reciprocity" meant that Facebook would maintain granular control over the information gathered on its platform, so that information generated by a user's interaction with a Platform Application would be transmitted back to Facebook, and vice versa. Any information known about Facebook users and their friends through the Facebook platform would be available to developers of Platform Applications and other third parties, and any information generated through a user's interaction with Platform Applications or otherwise recorded would similarly be transmitted back to Facebook. This allowed Facebook, third-party developers of Platform Applications, and advertisers to all have maximum access in order for Facebook to generate and capitalize on increasing amounts of personal user information.

117. On November 19, 2012, Zuckerberg sent Sandberg and fourteen other top executives at Facebook, including Lessin, an email to relate his answer on what Facebook's "platform business model" should be—***full reciprocity***—allowing partners access to user information at no charge, so long as all the information generated by the Platform Applications connecting to the Facebook platform shared that information back to Facebook.

118. Zuckerberg posed in the November 19, 2012 email the driving question for the future of the platform: the amount Facebook would be able to charge its partners for personal user information while still allowing the Facebook platform to achieve ubiquity. The users themselves only entered into the question obliquely—as an "audience problem" to be solved and a source of increased "net sharing" to be exploited. Zuckerberg shared the following:

> After thinking about platform business model for a long time, I wanted to send out a note explaining where I'm leaning on this. This isn't final and we'll have a chance to discuss this in person before we decide this for sure, but since this is complex, I wanted to write out my thoughts. This is long, but hopefully helpful.
>
> ***The quick summary is that I think we should go with full reciprocity and access to app friends for no charge***. ***Full reciprocity means that apps are required to give any user who connects to FB a prominent option to share all of their social content within that service*** (ie all content that is visible to more than a few people, but excluding 1:1 or small group messages) ***back to Facebook***. In addition to this, in the future, I also think we should develop a premium service for things like instant personalization and coefficient, but that can be separate from this next release of platform. A lot more details and context below.

Critically, Zuckerberg never mentions any notice or consent requirement that a user be aware of or consent to Facebook's sharing of personal information with its partners. Instead, the only prompt he envisioned would alert users to the option to share certain social communications generated in a Platform Application back to the Facebook platform.

119. Instead of addressing the propriety of offering up a user's information in order to entice partners to the Facebook platform, Zuckerberg continued in the November 19, 2012 email by addressing how to charge partners for access to the platform while still allowing Facebook to grow to the level of ubiquity. Ultimately, Zuckerberg decided that both the "write" and "read" permissions—the ability for partners to both "write" additional user information back to the Facebook platform, and the ability for partners to "read" already-existing user data—were essential for Facebook's monetization efforts:

> First, to answer the question of what we should do, the very first question I developed an opinion on was what we should be optimizing for. ***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***.
>
> If we do this well, we should be able to unlock much more sharing in the world and on Facebook through a constellation of apps than we could ever build experiences for ourselves. ***We should be able to solve the audience problem partially by giving people different audiences in different apps and linking them all together on Facebook***. The current state of the world supports that more social apps enables sharing, so the biggest challenge for us is to link them all together.
>
> * * *
>
> For charging, ***the question is whether we could charge and still achieve ubiquity***. Theoretically, if we could do that, it would be better to get ubiquity and get paid. My sense is there may be some price we could charge that wouldn't interfere with ubiquity, but this price wouldn't be enough to make us real money. Conversely, we could probably make real money if we were willing to sacrifice ubiquity, but that doesn't seem like the right trade here. After looking at all the numbers for a while, ***I'm coming around to the perspective that the write side of platform is a much bigger opportunity for us and we should focus the vast majority of our monetization effort on that and not this***.

120. In this quest for ubiquity, Zuckerberg predicted that the Facebook APIs—those nodes and fields in the Facebook platform containing personal user information—would be exploited by Facebook's partners. Zuckerberg's prediction would turn out to be frightfully accurate, as made clear by Cambridge Analytica and the hundreds of other partners to whom Facebook gave personal user information. But, Zuckerberg decided, this "abuse" of personal user information could also be monetized, and so a "full accounting system" tracking the use of personal user information was not justified. Instead, Zuckerberg judged the vast and unchecked

distribution of personal user information as a worthwhile risk to take, so long as Facebook prevented its competitors from openly obtaining such information:

> First, in any model, ***I'm assuming we enforce our policies against competitors much more strongly. The good news about full reciprocity is that for bigger social companies we might otherwise be worried about, if they're enabling their users to push all of their social content back into Facebook, then we're probably fine with them***. However, for folks like WeChat, we need to enforce a lot sooner.
>
> * * *
>
> Fifth, not charging still means ***people will overuse and abuse our APIs and waste money for us, so I still think we should implement some kind of program where you have to pay if you use too many of our resources. That said, the goal of this won't be to charge for actual usage so we can build a less precise system of for monitoring than the full accounting systems we would have had to build for the other system we discussed. What I'm assuming we'll do here is have a few basic thresholds of API usage and once you pass a threshold you either need to pay us some fixed amount to get to the next threshold or you get rate limited at the lower threshold***. One basic implementation of this could be to have a few different fees for developers, with basic starting at $100 and then having levels at $10k, $1m, $10m, etc. This should be relatively simple, achieve the goal of controlling costs and make us some money if we want.
>
> * * *
>
> Overall, I feel good about this direction. ***The purpose of platform is to tie the universe of all the social apps together so we can enable a lot more sharing and still remain the central social hub. I think this finds the right balance between ubiquity, reciprocity and profit***.

121. Sandberg replied to Zuckerberg's November 19, 2012 email the same day, agreeing completely with the concepts Zuckerberg had described: "I think the

observation that we are trying to maximize sharing on [F]acebook, not just sharing in the world, is a critical one. ***I like full reciprocity and this is the heart of why***."

3. *"Full Reciprocity" And "Whitelisting" Information Sharing Agreements Are Implemented in Facebook Platforms v3 And v4 Beginning In 2012*

122. The foregoing plans to share vast swaths of personal user information openly, with deeper information-sharing "whitelisting" agreements for choice Facebook partners, were actually and successfully implemented by Facebook beginning on June 26, 2013 with the "roll-out" of "v3" (version three) of the Facebook platform and continuing through the present. Entering into whitelisting agreements with certain Facebook partners meant that those companies maintained full access to personal user information, including user friends' data, after the platform changes.

123. Facebook began reviewing Platform Applications before allowing them to go "live," or actively integrate with Facebook beginning in January 2012. The app review included quality assurance measures and a review ensuring that the precept of "full reciprocity" was followed. Conspicuously absent from the review was any assurance that personal user information was protected: no assurance that users had consented to have their data reciprocally shared, and no apparent Facebook privacy policy to gauge that adequate user data protection was ensured through reciprocity with these Platform Applications. Instead, app review was limited to

ensuring that Facebook received as much value from the information that it gave to Platform Applications, as explicated in Facebook's own internal memorandum for the "Platform 3.0 Plan":

> App Review & Reciprocity
>
> Since the launch of Open Graph in Jan. 2012, we have moved toward an app review model w[h]ere we review and approve an app[']s integration with Facebook social channels (News Feed, Timeline, etc.). We extended this model to the App Center. With this announcement taking the next step in this evolution. In 90 days, we will begin to review and approve all apps that integrate with Platform. This will ensure that we are maintaining a high-level of app quality and that our user and developer interests are aligned. Developers may continue to develop and test on Facebook Platform as they always have, but before they can take their app "live" to non-developers/testers, their app must be approved and reviewed by Facebook.
>
> ***As part of this review process, we will examine the quality of the app, but also if the app is in compliance with our policies. In particularly, [sic] we will determine if the app is following our reciprocity and duplicative functionality policy. All apps may use Platform for Login and Social Plugins, but if the app accesses extended user information such as the friend graph, photos, etc. the app must also make it possible for the user to bring their data from the app back to Facebook***. In order to help developers with this requirement, we are releasing tools collective[ly] known as Action Importers.
>
> Further, for the small faction of developers who's app may duplicate existing FB functionality, we can make this determination at review time, before the app launches, to ensure that [we] can work together to see if we can come to an equitable resolution.

Facebook's policy ensured that any data generated in a Platform Application was shared back to Facebook; but did not even examine the volume of personal user

information shared to the Platform Applications, nor provide any assurances regarding what a partner could do with the data once it was obtained.

124. A series of emails among Facebook executives in the fall of 2013 confirms that any effort Facebook took to control the sharing of user information was limited by its analysis of competitive business threats. Rather than ensuring that all information shared with Facebook's partners was within clearly established user privacy controls, Facebook conducted an extremely limited "audit" of access to user data to decide whether Facebook wanted to maintain a business relationship with a select group of businesses competing with Facebook. Access to personal user information was only limited where Facebook decided that the partner in question was a "high-risk" or "threat" company that could compete with Facebook's business model and refused to enter into a contract agreement with Facebook to limit that competition.

125. On September 4, 2013, Defendant Papamiltiadis, Facebook's Director of Developer Platforms and Programs, wrote an email to several of the Company's Product Managers raising a few issues regarding the Company's "P3.0 Rollout Planning." Papamiltiadis wrote:

> I think you [Simon Cross, Product Manager] are right to suggest that ***a full audit is a huge task with unclear value*** . . . . I would recommend that we do a thorough audit on the apps that have been whitelisted for capabilities equivalent to the public APIs we will be deprecating . . . .

[T]he capability will remain to give access features which are publicly deprecated, but available to whitelisted apps.

In other words, through these plans, Facebook would restrict access to certain personal user information in order to induce partners into signing "whitelisting" agreements with the Company, in order to monetize the user data.

126. Simon Cross, a Facebook Product Manager, responded on September 5, 2013, detailing the process for the whitelisting "audit":

What we need to do to make this happen is the following:

- Draw up a list of the Capabilities, the Gatekeepers and the non-capability sitevars that we want to include in the audit—perhaps tiering them by significance
- ***Draw up a list of the high-risk/threat companies (and their apps) that we want to audit—we should order these by MAU [monthly active users]***
- Build a spreadsheet for use in the hack where we list out the apps, companies and capabilities we've audited, and ou[r] decision about any action we take. I think this comes down to 4 options:

    1. Keep access (and verify we have an agreement with them)
    2. Revoke access
    3. Keep access, but need to get an extended Platform agreement with them
    4. Escalate (need someone else to make a call, or to provide more context)

* * *

> We should also check with Marie about the scope of what the Talent tool covers, and if they have imminent plans to migrate whitelists currently controlled by Sitevars or Gatekeeper into this tool.

Facebook's "audit" was thus limited only to the "high-risk/threat companies (and their apps)"—and even then, only extended to Platform Applications with large numbers of monthly active users. Moreover, once Facebook had identified a company as a competitive risk to be "audited," ***the decision of whether to keep or revoke access revolved entirely around whether the competitive partner currently had, or would agree to, enter into a whitelisting agreement with the Company***.

127. As Ashkan Soltani, former chief technologist at the FTC ("Soltani"), told a UK House of Commons Subcommittee regarding Facebook's supposed review of Platform Applications:

> In short, I found that time and time again ***Facebook allows developers to access personal information of users and their friends, in contrast to their privacy settings and their policy statements***. This architecture means that if a bad actor gets a hold of these tokens . . . there is very little the user can do to prevent their information from being accessed. Facebook prioritises these developers over their users.

128. Facebook's v4 Platform changes, enacted in January 2014, included an even greater attempt by Facebook to monetize the sharing of user information. Due to the success of information sharing on the Facebook platform in its v3 iteration, Facebook decided to "privatize" certain previously openly shared personal user information. Facebook expanded the whitelisting agreements with partners as a

requirement for partners to attain the same access to user data, while phasing out, or "deprecating," the previously open APIs. However, certain "Core APIs" would still be openly shared, without a whitelisting agreement:

API Deprecations

- Access to friend data [likes, photos, checkins, etc]
- Questions, Subscriptions, Checkins, Pokes
- Apps reading public posts for TOS'ed users

HIGHLY CONFIDENTIAL FB-01352119

Core APIs

User Fields	APIs	Other
id	GET /permissions	iOS / Android / JS SDKs
name	POST /feed	PHP SDK
first_name	POST /photos	Login
last_name	POST /videos	Payments
picture		Like Button
gender		Ads
locale		
age_range		
link		
timezone		
currency		
birthday		
email		

HIGHLY CONFIDENTIAL FB-01352141

129. Critically, the January 2014 v4 platform changes continued to allow Facebook partners to access to NAFs, "non-app friends" of a user. These NAFs

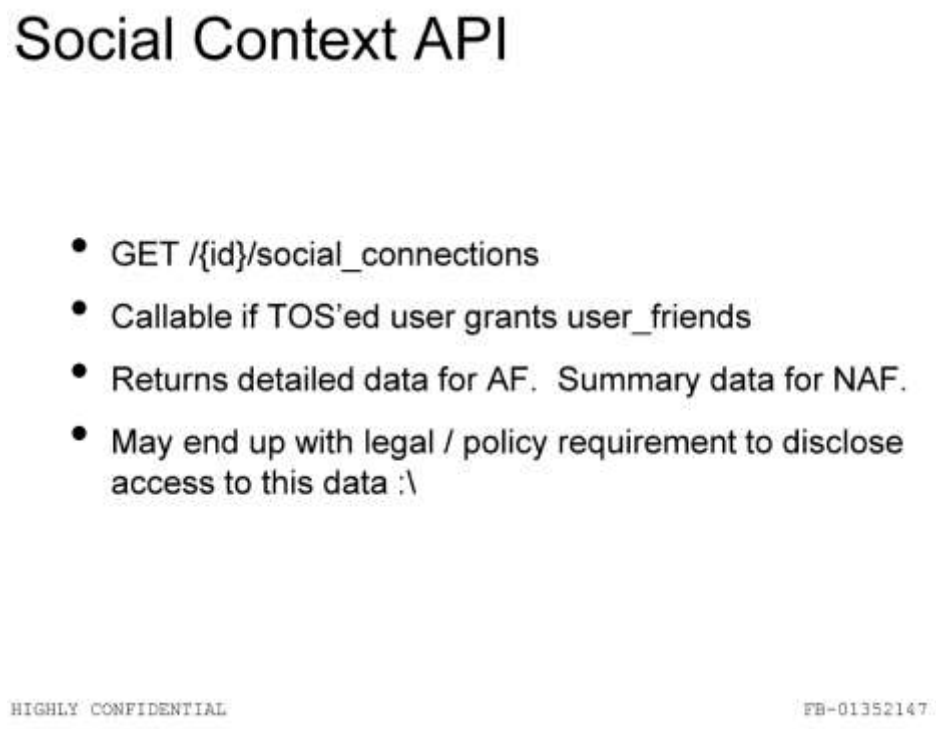
were friends of a user who had never consented to share any information with the Platform Application in question, yet inexplicably Facebook allowed such information to continue being shared:

APIs returning friends

	Use Case	ID Space	API	Can be cached	# of apps	Notes
1	Login [no friends]	A	N/A	Y	10^6	In the limit, we want all apps using Login
2	Login w/ friends [app friends + NAF]	A	/me/friends	Y	App Friends: 10^5 NAF: 10^2	Currently used for cross app promotion
3	Tagging	B	/me/taggable_friends	N	10^4	Requires approval
4	Social Context	B	/me/social_connections	N	10^4	
5	Invites	A	/me/inviteable_friends	Y	10^3	Response sorted by likelihood of conversion Available only to Canvas games that use Credits

HIGHLY CONFIDENTIAL FB-01352146

130. Facebook knew that such activity was illegal under the Consent Order and would likely result in legal trouble for the Company, as the same slide presentation indicates that Facebook ***"[m]ay end up with legal / policy requirement to disclose access to this data*** **:** ":



131. The scope of this information sharing was vast. As of January 2014, Facebook openly shared personal user information through its APIs with millions of business partners. ***At a minimum, Facebook knowingly shared personal user information with its partners in 49,060,000 separate instances in January 2014 alone***, without user consent or appropriate privacy protections, in violation of the Consent Order. Facebook measured this information sharing by the number of monthly active users (MAUs) of a Platform Application, as the below internal Facebook slides prepared on January 27, 2014 demonstrate:

Affected Apps

	Total	> 1,000 MAU	> 10,000 MAU
API callers [last 30d]	1.4M	17K	3,206
Affected apps	27,019	7,744	2,532
Affected games	3,111	1,475	521
Affected Credits apps	338	315	253
Affected Ad Spenders	89	82	60
Affected Salesforce apps	1,639	1,262	812
Affected Salesforce games	458	375	253
Affected Salesforce non-games	1,181	887	559

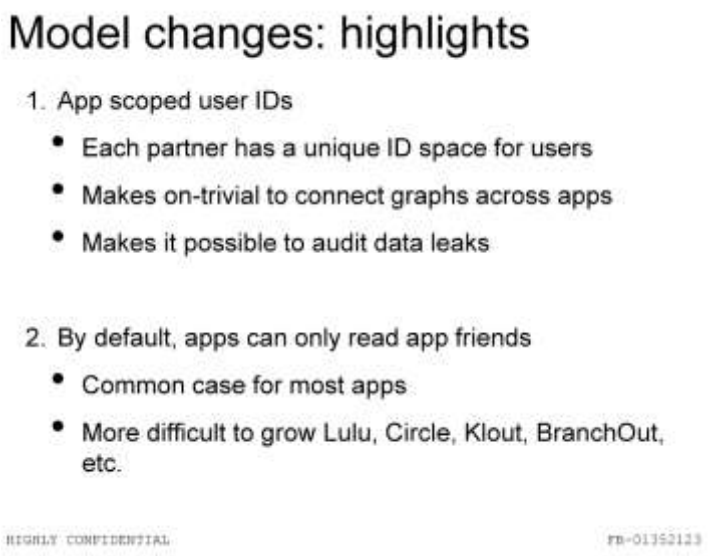
Key apps

	# of apps	% requesting read_stream
Mark's friends	31	76%
Sheryl's friends	66	62%
Generating TPV	332	51%
Neko spenders	831	59%
Noisy	23	82%
T0 / T1 partners	160	77%

All on a list for pre-launch outreach

In addition, the majority of all "Key apps" (whitelisted partners) requested the "read_stream" Graph API, allowing them to receive all information displayed on a user's personal Facebook page, or "wall." Perhaps most surprisingly, ***Facebook was making exceptions in the form of personal favors for "Mark's friends" and "Sheryl's friends," 99 Platform Applications Facebook specifically catered to because they were personally favored by Zuckerberg and Sandberg*** and allowed increased access to personal user information.

132. The goal of the January 2014 v4 platform changes had nothing to do with user privacy. Instead, Facebook was ensuring that it could maintain control over personal user information while still sharing it with the partners Zuckerberg, Sandberg and the Company found favorable, while restricting access to Platform Applications that sought to provide competition to the Facebook platform:



As the above slides demonstrate, Facebook was aware that its policies could cause "data leaks," which meant the sharing of information to Facebook competitors. Facebook only took steps to limit the ability of competitors to compete with the Facebook platform, but took no action to limit information leaking to "good" Platform Applications such as Venmo.

133. Missing from Facebook's plans was any consideration of whether sharing a user's friend data generally was a "leak," despite the requirement that Facebook refrain from such sharing in the 2012 Consent Order. Instead, this illegal conduct was an intentional part of Facebook's business plan, and compliance with privacy requirements gave way to monetization and growth of the platform. Facebook, under Zuckerberg's and Sandberg's leadership, made the unfortunate choice to continue sharing a wide swath of personal user information in defiance of

the 2012 Consent Order, including sharing core identifying demographic information, the ability to read a user's mailbox and messages, and open access to the data of all friends of a given user.

134. Facebook allowed preferred partners to circumvent users' privacy settings and maintain access to user friends' information, even when the user disabled those settings, through whitelisting. The whitelisting agreements Facebook entered into and otherwise implemented—an example of the "full reciprocity" model driving privacy violations—began in 2013, included agreements with a wide range of companies, including: Royal Bank of Canada ("RBC"), Netflix, Nissan Motor Co., Walgreens, Lyft, GoDaddy, Airbnb, Badoo, and Hootsuite. In March 2015, Defendant Papamiltiadis corresponded with Skype representatives, ultimately granting Skype whitelist access as well.[24] Those whitelisting agreements allowed for full access to personal user information through a suite of APIs on the Facebook platform, including access to the user's entire list of friends (including non-app friends).

135. Facebook's whitelisting agreements with RBC and Lyft are instructive both as to Facebook's business purpose behind the arrangement and the mechanics of how whitelisting enables a Platform Advertiser to access a user's full friends list,

[24] 643 Summaries, *supra* note 5, at 41 (citing FB-00596473).

regardless of whether the user's friends have consented to that Platform Advertiser's ability to access their data. After Facebook announced changes to the platform that would eliminate a Platform Advertisers' access to a user's full friends list unless the friends had also opted-in to the Platform Application, RBC expressed concern, noting, "[w]ithout the ability to access non-app friends, the Messages API becomes drastically less useful."[25] Following internal discussions, including that RBC was currently running "one of the biggest neko [advertising spending] campaigns ever run in Canada," RBC was whitelisted and provided access to friends' data. Thus, Facebook's willingness to whitelist a partner for purposes of generating increased advertising revenue is apparent.

136. Lyft similarly expressed concern that the utility of its application of the Facebook platform would be undermined if Lyft's access to user data was limited only to the user's friends who were also using Lyft (rather than the user's full friends list).[26] In response, Papamiltiadis facilitated Lyft's access to users' full friends list, explaining "[w]e have designed the Mutual Friends API for use cases exactly like yours."[27]

[25] FB-00427400 at 405 (document released by Parliament).

[26] FB-00042899 at 908 (document released by Parliament).

[27] FB-00042899 at 907 (document released by Parliament).

137. While some whitelisting agreements were terminated in May 2015, an untold number of developers were granted extensions past this time period, and hundreds were reported to still have access to personal user information well after April 2018.

138. Facebook used a standard form agreement for all whitelisted companies called a "Private Extended API Addendum," which reads in part:

> Access to the Private Extended APIs. Subject to the terms of the Agreement, FB may, in its sole discretion, make specific Private Extended APIs available to Developer for use in connection with Developer Applications. FB may terminate such access for convenience at any time. The Private Extended APIs and the Private Extended API Guidelines will be deemed to be a part of the Platform and the Platform Policies, respectively, for purposes of the Agreement. . . . 'Private Extended APIs' means a set of APIs and services provided by FB to Developer that enables Developer to retrieve data or functionality relating to Facebook that is not generally available under Platform, which may include persistent authentication, photo upload, video upload, messaging and phonebook connectivity.

139. Facebook only restricted access to partners when those partners threatened Facebook with business competition. For instance, by email on January 24, 2013, Zuckerberg personally ordered that "friends API" access be "shut down" for Twitter's Vine app, because it was competing in Facebook's social media space by allowing users to share short video segments with each other. Microsoft was also denied a whitelisting agreement and was shut out from access to personal user information. Facebook did not take such steps for partners with whitelisting

agreements, or for which Facebook was otherwise not concerned on a level of business competition.

140. Moreover, Facebook entered into whitelisting agreements with numerous companies that were linked to certain Director Defendants and other non-party directors.

141. For instance, in January 2015, Defendant Papamiltiadis was part of an email conversation concerning ongoing whitelist negotiations with Dropbox's CEO Drew Houston, who is now a director at the Company, wherein Facebook offered Dropbox access to Friends data.[28]

142. That same month, Defendant Papamiltiadis was encouraged to give Tinder a Whitelist Agreement to receive special access Friends data before the CEO of Tinder starts "***an email thread with Mark [Zuckerberg]***."[29]

143. The next month, February 2015, Defendant Papamiltiadis met with representatives from Netflix to discuss Netflix's "upgrade path" and answer technical questions regarding the user information available since Netflix would "be whitelisted for getting all friends, not just connected friends."[30] Director Defendant Hastings was a co-founder of Netflix and remains its Chairman and CEO.

---

[28] *Id*. at 39 (citing FB-00046066).

[29] *Id*. at 39 (citing FB-00047134) (emphasis added).

[30] 643 Docs, *supra* note 5, at FB-00045736.

4. *Facebook's Whitelisting Practices Directly Contradict Defendant Zuckerberg's Public Statements That Facebook Had Restricted Third Party Access To Friends Data*

144. At the F8 Developers Conference on April 30, 2014, Defendant Zuckerberg announced his decision to restrict third-party app developers' access to Friends data, stating:

> We've also heard that sometimes you can be surprised when one of your friends shares some [] data with an app. And the thing is we don't ever want anyone to be surprised about how they're sharing on Facebook and that's not good for anyone. So we're going to change how this works.
>
> [] In the past, when one of your friend blogged [sic] into an app . . . the app could ask him not only to share his data but also data that his friends had shared with him – like photos and friend list here. So now we're going to change this and we're going to make it so that now everyone has to choose to share their own data with an app themselves. So we think that this is a really important step for giving people power and control over how they share their data with the apps. And as developers, this is going to allow you to keep building apps with all the same great social features while also giving people power and control first. So I am really happy that we are doing this.[31]

[31] S, Pangambam, *Facebook's CEO Mark Zuckerberg F8 2014 Keynote (Full Transcript)*, THE SINGJU POST (July 5, 2014), *available at*: https://singjupost.com/facebooks-ceo-mark-zuckerberg-f8-2014-keynote-full-transcript/2/. The speech was drafted by Defendant Zuckerberg with the support of other Facebook executives such as Vernal. *See* 643 Summaries, *supra* note 5, at FB-00854613, FB-00187292.

145. These statements regarding limiting third-party developers' access to Friends of Friends data was in direct contradiction to Facebook's actual practice of granting favored business partners access to such data through whitelisting agreements; Facebook always intended to allow certain favored third-party developers to continue to access Friends data. For instance,

- In October 2012, Sam Lessin, Douglas Purdy (Director of Products), Dan Rose (former Vice President of Partnerships), and Justin Osofsky (former Vice President of Global Operations, and now the Chief Operating Officer of Instagram) discussed preparing for an upcoming meeting "w/ Zuck + mteam"[32] wherein they needed to gather information to help the executives understand changes to third-party access.[33] One issue identified by Vernal in the email is: "API Change Analysis – what is impacted on the ecosystem of killing friends information . . . [it] would be good to understand how many apps impacted, biggest apps impacted, whether we'd whitelist folks, etc.)"[34]

- Also in October 2012, Facebook executive Vernal notified

[32] "mteam" or "m-team" refers to Facebook's "Mark Team"—a "smaller coterie" of Facebook's upper management— consisted of Defendants Sandberg, Schroepfer, Wehner and Koum, and Non-Parties Cox, Vernal and Stretch. *See e.g.*, FB220-00015887 at 15868–69; 643 Docs, *supra* note 5, at FB-01370844. *See also* Mike Isaac, Sheera Frenkel & Cecilio Kang, *Now More Than Ever, Facebook Is a 'Mark Zuckerberg Production'*, N.Y. TIMES (May 16, 2020), *available at*: https://www.nytimes.com/2020/05/16/technology/zuckerberg-facebook-coronavirus.html; Alex Heath, *The People With Power at Facebook*, The Information (Oct. 3, 2019), *available at*: https://www.theinformation.com/articles/the-people-with-power-at-facebook-1003.

[33] 643 Docs, *supra* note 5, at FB-01221432-33.

[34] *Id*.

some Facebook employees on the "series of conversations w/ Mark [Zuckerberg] [ ] about the Platform Business Model" and "why do we let apps access all this data today?" Vernal states that a decision has been made to restrict data access, including removing friends permission, "without a formal deal in place," suggesting that not all app developers would be denied access to friend's data.[35]

- In June 2013, Vernal wrote an email to his team regarding his concern "about our ability to truly remove friend data permissions and break marquee partners. Default assumption is we'll have a whitelist of apps."[36]

- In an October 2013 email chat, Eddie O'Neil (Director of Product Management) asked several other Facebook employees to list non-app games that use the full friends list.[37] The employees respond by naming several apps, including Instagram, Spotify, Nike, among others.[38] Then, in December 2013, O'Neil, writes Simon Cross (a member of the Strategic Product Partnerships team), regarding "Whitelist Pre-Approvals Master Table of all apps impacted by PS12n deprecations,"[39] suggesting that Facebook was pre-approving apps for Friends access that would be denied under the new Platform.

- In January 2014, O'Neil was tasked with preparing a "Whitelist Process Agree Legal requirement for whitelist access."[40]

---

[35] 643 Summaries, *supra* note 5, at 6 (citing FB-00423235-36).

[36] *Id*. at 76 (citing FB-00905314).

[37] *Id*. at 24 (citing FB-00422062).

[38] *Id*.

[39] *Id*. at 25 (citing FB-00434554).

[40] *Id*. at 27 (citing FB-00528201).

- In February 2014, Facebook executive Ime Archibong wrote an email to O'Neil, Cross, and Jackie Chang (Director of Product Partnerships), stating that Rose is "of the mindset that we shouldn't have a whitelist for anything, so we'll have to explain to him why these [ ] buckets are necessary."[41] Chang responds that with an updated version and notes that "[w]here I've labeled 'exemptions' are actually private apis today that allow for friend data to be read . . . I believe we should keep maintaining these apis as private strategic ones . . ."[42]

146. It was therefore known internally that Defendant Zuckerberg's stated plan to remove third party access to Friends data was false, as certain Whitelisted Developers had retained access.[43] Specifically, in a chat conversation between O'Neil and T.R. Vishwanath, a Principal Software Engineer, it was noted that:

> O'Neil: We've been saying that apps can't access non-app friends, but that's a slightly inaccurate phrase, right? Want to confirm the proposed model ahead of talking to Javi today: 1/all apps can access non-app friends 2/apps can access these fields for each non-app friend: {first name, third_party_id, picture) 3/ GET /(third_party_id) doesn't do anything 4/ and of course friends_* are deprecated."
>
> Vishwanath: "In this model giving the actual ids of friends would be a capability rather than a permission."

[41] *Id*. at 29 (citing FB-00587485).

[42] *Id*.

[43] *Id*. at 19 (citing FB-00493943).

> O'Neil: "Ah – ok, so API would support reading via GET /(3rd_party_id). That's cool. Ok – so some whitelisted apps (presumably w/ contracts) could access id. Makes sense – thanks for confirming."[44]

147. Granting certain developers' access to users' Friends data directly contradicted Defendant Zuckerberg's public statement that such data would not be shared with third-party developers and thereby violated the 2012 Consent Order. And this decision—*i.e.*, the policy of privately granting certain friendly companies continued access to Friend data—came at the insistence of Defendant Zuckerberg and with the Board's knowledge or reckless disregard.

148. Indeed, Facebook's relationship with third-party developers was discussed at Board meetings dating back to 2012.[45] For instance, three weeks after Defendant Zuckerberg's announcement at the F8 conference, at a May 2014 board meeting, Defendant Andreessen complained (again) that "developers don't like us,"

[44] *Id*.

[45] 643 Docs, *supra* note 5, at FB-01368446 (regarding a board deck that discussed "[p]artners monetizing the data accessible via our read APIs and we share some of that value (today this is mostly through users acquired due to friends/traffic")); 643 Summaries, *supra* note 5, at 157 (citing FB-01369317) (discussing the same board deck and statistics related to the Platform's "Read API").

which caused Defendant Sandberg to initiate an effort to evaluate Facebook's relationships with third-party developers.[46]

149. Accordingly, Facebook's whitelisting agreements directly contradict Zuckerberg's April 2014 statement that Facebook would no longer share user data with third-part app developers. This false statement, in and of itself, runs afoul of the 2012 Consent Order's requirement that Facebook not mislead or deceive its users about the extent to which their data would be shared with third parties without their affirmative consent.

5. *Facebook Successfully Monetizes User Data, Prioritizing Growth At All Costs*

150. Facebook failed to restrict access even to partners who presented a competitive risk to Facebook, so long as they provided revenue allowing the Facebook platform to grow. Even for those partners for which Facebook did harbor competitive misgivings, if the partner spent enough on Facebook advertising (abbreviated internally as "NEKO" spend), Facebook was willing to maintain data sharing with those partners. As a September 18, 2013 email from Papamiltiadis outlined, even if Facebook did not want to share data with certain Platform Applications due to competitive concerns (such as a partner hoovering up personal

[46] *Id*. at 146 (citing FB-01366319).

user information in order to reproduce a Facebook-like platform), Facebook would still share personal user data if NEKO spending was high enough:

> Key points:
>
> ***1/ Find out what other apps [] are out there that we don't want to share data with and figure out if they spend on NEKO***
>
> **** Communicate in one-go to all apps that don't spend that those permission [sic] will be revoked***
>
> **** Communicate to the rest that they need to spend on NEKO at least $250K a year to maintain access to the data***
>
> 2/ Review future submissions and reject/approve as per the requirements above
>
> 3/ Update our policies if need be
>
> 4/ Comms / PR plan if # of apps affected is significant

151. This strategy, along with the whitelisting agreements and other platform changes, allowed Facebook to successfully monetize personal user information to the extreme, at the expense of user privacy. As Lessin commented in a January 20, 2013 email between the Platform v3 and v4 integrations, "The nekko [NEKO] growth is just freaking awesome. Completely exceeding my expectation re what is possible re ramping up paid products."

152. On reviewing the foregoing business practices, Soltani, the former chief technologist at the FTC, noted that, "[i]t shows the degree to which the company

knowingly and intentionally prioritized growth at all costs." The foregoing also demonstrates that Facebook's business model drove its privacy violations.

D. Facebook's Privacy Settings Failed To Disclose The Extent Of Facebook's Data Sharing With Third Parties In Violation Of The 2012 Consent Order

153. Despite internally whitelisting third parties, Facebook continued to publicly mislead its users about Facebook's dissemination of personal user data to third parties.

154. For example, "[i]n the wake of the FTC's initial investigation . . . [Facebook] added a disclaimer to its Privacy Settings page, warning users that information shared with Facebook Friends could also be shared with the apps those Friends used."[47] But then, just "four months after the 2012 Consent Order was finalized, Facebook removed this disclaimer," immediately and fully reverting back to the very practices that led to the FTC action in the first place.[48]

155. Facebook further failed to disclose to users that: users' privacy choices would be undermined by default settings that allowed Facebook to share users' data with third-party developers of their Friends' apps; and users who shared their posts to a more limited "Friends" or "Custom" audience could still have that information

[47] 2019 FTC Complaint, *supra* note 2, at ¶ 7.

[48] *Id*.

shared with any of the tens of millions of third-party developers whose apps where being used by their friends through Friends data collection.[49]

156. Facebook's mobile privacy settings were similarly deceptive. From March 2012 through March 2013, Facebook's mobile interface contained a disclaimer near the top of the privacy settings page stating, "You can manage privacy of your status updated, photos, and information inline audience selector—when you share or afterwards. *Remember: the people you share with can always share your information with others, including apps*."[50] But around March 2013, this disclaimer was removed from the mobile privacy settings page even though such information continued to be shared with others, including apps.[51]

157. The mobile privacy settings page also purported to allow users to restrict who could see their past and future posts, as well as users' birthday and contact information. But Facebook ensured users would continue sharing that information with apps to the fullest extent possible by: (a) removing the link to apps setting page from the privacy setting page;[52] (b) making the privacy settings for apps

[49] *Id*.

[50] *Id*. at ¶ 35.

[51] *Id*. at ¶ 36.

[52] *Id*. at ¶¶ 35-36.

difficult to locate;[53] and (c) sharing users' bios, birthdays, family and relationships, websites, status updates, photos, videos, links, notes, hometowns, current cities, education histories, work histories, activities, interests, "likes", app activity, and status of being online, with app developers *by default*.[54]

158. Facebook further misled users by placing disclaimers on the Platform settings that did not fully explain the significance of turning off the default settings. Facebook's disclaimer stated "that turning off the Platform setting would prevent users from using any Facebook apps themselves and prevent Friends from being able to 'interact and share *with you* using apps and websites,"[55] thus only focusing "on information that would be shared with the user rather than information Facebook would share about the user" and failing to "alert users to the fact that: (a) Facebook shared their Profile Information with third-party developers of Friends' apps by default; or (b) the Platform settings allowed them to opt out of such sharing."[56]

[53] *Id*. at ¶¶ 63, 74-75.

[54] *Id.* at ¶ 76 (emphasis added).

[55] *Id*. at ¶¶ 79-80.

[56] *Id*.

E. Zuckerberg And Sandberg Use Facebook To Spy On Android Users by Continuously Stealing Their Call Logs And Text Messages

159. By 2015, Facebook's information brokering activities had extended to include snooping on Android phone users' telephone call logs, text messages and location data. Facebook executives made technical changes updating the Facebook Android mobile application in or about February 2015 to allow for this extra access to the information stored on Android mobile phones. This was accomplished through exploitation of additional Android system "permissions." Both Zuckerberg and Sandberg were briefed on these plans.

160. Moreover, Facebook executives realized that such an invasive change would be "pretty high-risk" for the Company should the extra access to user call logs, text messages and location data become public. However, Facebook's product developers found a surreptitious workaround to prevent Android Facebook users from being alerted to the additional data Facebook would attain through its update. Facebook executives thought only of the risk of "PR fallout"—of the public finding out about this change—and nowhere discussed privacy considerations or the legal requirements imposed by the 2012 Consent Order.

161. Vernal, along with other high-ranking Facebook product managers and other executives, discussed the changes to the Android Facebook app through an email chain on February 4, 2015. On the email chain, Michael LeBeau, a Facebook

Product Manager, noted that the push for call logs and text messages came from Facebook's "growth team," a group spearheaded by Zuckerberg, while the "Gravity team" was responsible for an update allowing Facebook to obtain user location data from a weakness in mobile phones' Bluetooth capabilities. LeBeau wrote:

> ***Hey guys, as you all know the growth team is planning on shipping a permissions update on Android at the end of this month. They are going to include the "read call log" permission, which will trigger the Android permissions dialog on update, requiring users to accept the update. They will then provide an in-app opt-in NUX for a feature that lets you continuously upload your SMS and call log history to Facebook*** to be used for improving things like PYMK, coefficient calculation, feed ranking, etc.
>
> ***This is a pretty high-risk thing to do from a PR perspective but it appears that the growth team will charge ahead and do it***.
>
> Separately, Gravity team had been intending to ship the Bluetooth permission on Android at the same time—in fact we'd already delayed to accommodate more permissions from the growth team, but we didn't realize it was going to be something this risky. ***We think the risk of PR fallout here is high, and there's some chance that Bluetooth will get pulled into the PR fallout. Screenshot of the scary Android permissions screen becomes a meme (as it has in the past), propagates around the web, it gets press attention, and enterprising journalists dig into what exactly the new update is requesting, then write stories about "Facebook uses new Android update to pry into your private life in ever more terrifying ways—reading your call logs, tracking you in business with beacons, etc."***

Significantly, LeBeau indicated that Facebook users would be unable to discern that Facebook was reading their call logs, text messages, and location data from the disclosure, if any, that the Company gave to them. Instead, it would take the work

of an enterprising journalist with knowledge of the technology and industry to figure out what, exactly, the effect of Facebook's update was.

162. LeBeau went on to discuss the timing of the updates, which were split between the update allowing Facebook to access call log/text messages (pushed by the "growth team") and the update allowing Facebook access to location data through Bluetooth (pushed by the "Gravity team"). LeBeau noted that timing was problematic, as there did not seem to exist a solution to both avoid the "PR risks" and ensure that users actually adopted the new Facebook updates:

> Normally we'd have to wait until July for the chance to ship again, since ***we only ship Android permissions updates a couple times a year as they tank upgrade rates. So our options, aside from the "ship together and pray" option which feels too risky to me, are to wait until July to ship the Bluetooth permission on Android or ask for a special exception to ship our permissions update sooner***.
>
> Shipping permissions updates on Android has the downside of tanking upgrade rates, so we try to do it infrequently. But there could be an argument to doing it sooner in this case, as a compromise to allow both teams to continue moving fast, without unnecessarily conflating two PR risks into one.
>
> Wanted to make everyone aware of these options and welcome any thoughts/feedback about this.

163. In response, Yul Kwon, then a purported Privacy Officer for Facebook, indicated that the growth team had found a solution. Through an exploit in Android permissions, Facebook would find a way to "upgrade" users to obtain their call logs—without any dialog screen, completely eliminating the chance that anyone

would uncover the changes happening to the Facebook Android app behind the scenes:

> Based on their initial testing, ***it seems that this would allow us to upgrade users without subjecting them to an Android permissions dialog at all. It would still be a breaking change, so users would have to click to upgrade, but no permissions dialog screen***. They're trying to finish testing by tomorrow to see if the behavior holds true across different versions of Android.

164. Yul Kwon additionally indicated that Zuckerberg would meet with the Growth team to discuss this surreptitious update at a meeting to be held the following day. Sandberg was also scheduled for the meeting but could not attend due to a scheduling error. It is reasonable to infer that, if Sandberg could not attend the Growth team meeting, she was appraised of these developments shortly thereafter.

F. Cambridge Analytica

165. Cambridge Analytica was a political consulting firm that combined data mining and analysis with strategic communication, via traditional and emerging media, to try to affect political discourse and electoral outcomes in the United States. Alexander Nix served as Chief Executive Officer of Cambridge Analytica, and Christopher Wylie ("Wylie"), a young political operative, was charged with assembling a team and carrying out Cambridge Analytica's political influence hypothesis.

166. Wylie brought together psychologists and data scientists who worked to identify individuals' psychological traits and use them to influence individual voters' behavior.

167. Cambridge Analytica's ability to acquire and analyze data was greatly enhanced after Wylie found a researcher, Dr. Aleksandr Kogan ("Kogan"), who was able to bring in individualized psychological data on tens of millions of people. This new approach consisted of getting individuals to take a personality quiz and download an app, developed by Kogan and first employed in mid-2014, which enabled access to that individual's private information—as well as that of the individual's Facebook friend network. Kogan only disclosed to Facebook and its users that he was collecting information for academic purposes.

168. By gaining access to personal user information, including the personal information of users' friends, in total, Kogan provided Cambridge Analytica with over ***87 million*** raw profiles from Facebook, even though only about ***270,000*** users had actually participated in the survey and consented to the use of their data ***Facebook thus obtained the consent of roughly 0.31% of users whose data was shared***. The data including enough information to construct detailed profiles about

Facebook users—including places of residence—that allowed Cambridge Analytica to build "psychographic profiles" designed to influence political opinion.[57]

169. Wylie called the Facebook data "the saving grace" that let his team deliver the psychographic profiling requested by Cambridge Analytica's donors. The Facebook data was so comprehensive that it allowed Cambridge Analytica to "predict" and sell the following personality traits to those who wished to influence public opinion, according to a May 9, 2014 email from Kogan to Wylie.

- openness;
- conscientiousness;
- extraversion;
- agreeableness;
- neuroticism;
- life satisfaction;
- IQ;
- gender;

[57] Transcript of M. Zuckerberg's Appearance before House Committee, THE WASH. POST (Apr. 11, 2018) (**ESCHOO**: When did Facebook learn that Cambridge Analytica's research project was actually for targeted psychographic political campaign work? . . . **ZUCKERBERG**: When — when we learned about that, we . . . **ESHOO**: So, in 2015, you learned about it? **ZUCKERBERG**: Yes.) (hereinafter "Zuckerberg House Testimony") *available at*: https://www.washingtonpost.com/news/the-switch/wp/2018/04/11/transcript-of-zuckerbergs-appearance-before-house-committee/.

- age;
- political views;
- religion;
- job;
- university subject concentration;
- self-disclosure (do you tell people about yourself or not?);
- fair-mindedness (fair or suspicious in dealings with others?);
- self-monitoring (do you change personality depending on who you're with); and
- sensational interests (has 5 factors, "militarism" (guns and shooting, martial arts, crossbows, knives), "violent occultism" (drugs, black magic, paganism), "intellectual activities" (singing and making music, foreign travel, the environment), "credulousness" (the paranormal, flying saucers), "wholesome interests" (camping, gardening, hill-walking) [used in forensic psychology to understand criminality].

170. As noted, the Facebook data was also used by Cambridge Analytica during the 2016 election cycle, when it worked for the campaigns of Senator Ted Cruz and President Donald Trump. Cambridge Analytica used data from Facebook to design target audiences for digital ads and fund-raising appeals, model voter turnout, determine where television ads should be bought, and determine where President Trump should travel to best drum up support.

171. As the issues concerning Facebook and Cambridge Analytica surfaced and exploded into public consciousness, Facebook, Sandberg and Zuckerberg were apprised of other platform-based privacy issues.

172. For example, in 2016, the Max Planck Institute, a privacy advocacy group, complained to Facebook that it could extract personal data of Facebook users from the Platform, including the ability to locate telephone numbers of its users. After Facebook took the position that such sharing of telephone numbers did not pose a data sharing or privacy issue, a complaint was filed with the French data protection agency Commission Nationale de l'Informatique et des Libertés ("CNIL"). On April 27, 2017, CNIL sanctioned Facebook for "persisting breaches to the French Data Protection Act" after finding that Facebook was sharing personal user data without users' explicit consent. Defendant Sandberg received a copy of the CNIL's sanctions and findings.

173. On May 16, 2017, a joint statement was issued by the data protection authorities of The Netherlands, France, Spain, Hamburg, Germany and Belgium, regarding the conclusion of investigations into "the quality of information provided to users, the validity of consent, and the processing of personal data for advertising purposes." The statement noted that France pronounced a sanction of €150,000, after finding evidence that Facebook engaged in "unlawful tracking" and collecting information from users who do not "clearly understand that their personal data are

systematically collected as soon as they navigate on a third-party website that includes a social plug in." Belgium also found that "Facebook continues to act in non-compliance with both Belgian and EU data protection laws . . . [i]n particular the legal requirements regarding consent, fairness, transparency, and proportionality are not met . . . ." Similar findings were reached by the Netherlands, Germany, and Spain. Facebook's management team, which included Defendant Zuckerberg, Defendant Sandberg, and many Facebook executives were specifically apprised of this development.

174. On May 23, 2017, The *Australian* published a piece citing the violation of millions of minor children's privacy when Facebook employees sought to sell to advertisers a list of youth who were susceptible because, based on their posts, they were marked as having low self-esteem.

175. On June 1, 2017, the Audit Committee met to discuss, among other things, [redacted] A [redacted] was also recirculated to the Committee. The meeting materials do not, however, address the growing list of verified, specific [redacted] which would ultimately cause the Company to violate the 2012 Consent Order.

G. Facebook's Unfettered Sharing Of Personal User Information Becomes Public Knowledge And The Individual Defendants Engage In A Cover-Up

176. On March 17, 2018, *The New York Times* reported that Cambridge Analytica had harvested the private information of more than 50 million (later confirmed to be over 87 million) Facebook users without their permission. Facebook thereby allowed Cambridge Analytica to exploit the private social media activity of a huge swath of the American electorate. Facebook knew that the private information of millions of users had been used for nefarious purposes since at least 2015, but failed to acknowledge or disclose this information. Instead, in response to a week of inquiries from *The New York Times*, Facebook "downplayed the scope of the leak and questioned whether any of the data still remained out of its control." *The New York Times* investigation relied on interviews with former employees and contractors, and a review of Cambridge Analytica emails and documents.

177. The March 17, 2018 article from *The New York Times* reported that, beginning in 2016, Cambridge Analytica paid Kogan to acquire Facebook users' identities, personal identifying information, friends, and "likes"—the very same information covered by the 2012 Consent Order. Only a tiny fraction of the users, however, had agreed to release their information to a third party. Cambridge Analytica at the time claimed it had deleted the information, while for its part, Facebook questioned whether any of the data still remained out of its control.

1. *The Massive Harvesting Of Personal User Information Is The Result Of A Willful Business Plan*

a. Facebook's Nonexistent Controls Over User Information Allows Cambridge Analytica To Access The Personal User Information Of At Least 87 Million Facebook Users

178. One day after the March 17, 2018, *The New York Times* article was published, Facebook mobile advertising executive Andrew Bosworth tweeted: "This was unequivocally not a data breach. No systems were infiltrated, no passwords or information were stolen or hacked." This was true. Cambridge Analytica had no need to hack Facebook in order to obtain vast amounts of personal user information.

179. The Individual Defendants ***allowed*** Kogan to harvest vast amounts of personal user information from Facebook without user consent and sell that information to Cambridge Analytica. As Kogan has publicly noted, the terms of service of the app he used to collect Facebook user information were for a typical commercial use Facebook uniformly granted to other developers, through which Facebook allowed the sharing of personal user information.

180. On April 4, 2018, it was widely reported that Cambridge Analytica improperly gathered detailed information from 87 million users—up from the 50 million users originally reported. Media reports also disclosed that a vulnerability in Facebook's search and account recovery functions potentially exposed most of Facebook's two billion users to having their profile information harvested by outside

parties—additional breaches showcasing the haphazard treatment Facebook gave to its duties to protect the personal information of its users.

181. *The Guardian* reported shortly thereafter, on April 17, 2018, that according to employees of Cambridge Analytica, far more than 87 million Facebook users' data had been compromised, and many other parties than Cambridge Analytica had accessed Facebook user data. Brittany Kaiser, former Cambridge Analytica employee, said, "I believe it is almost certain that the number of Facebook users whose data was compromised through routes similar to that used by Kogan is much greater than 87 million; and that both Cambridge Analytica and other unconnected companies and campaigns were involved in these activities."

182. Further, Cambridge Analytica's use of personal user information was the natural consequence of Facebook's platform business plans, which were premised on the open sharing of personal user information in the spirit of "full reciprocity" and through agreements with its Platform Application partners, with or without user consent, in violation of the 2012 Consent Order. Facebook did nothing to verify how personal user information was being used by those partners it granted access to the Facebook platform.

b. UK Regulators Find Facebook's Business Plan Drives The Illicit Sharing Of Personal User Information

183. The fact that Facebook's business plan relied on the illicit sharing of vast swaths of personal user information without proper protections or the knowing consent of its users was confirmed by UK regulators. On February 14, 2019, the Digital, Culture, Media and Sport Committee for the UK House of Commons (the "UK Committee") released a report entitled, "Disinformation and 'fake news': Final Report" (the "UK Disinformation Report"), detailing the UK Committee's findings on, *inter alia*, individuals' rights over their privacy and how release of private personal information could lead to disinformation and political interference for democratic systems.

184. In releasing the UK Disinformation Report, UK Committee Chair Damian Collins on February 18, 2019 made the following public statements, in part, regarding the UK Committee's intent in investigating threats to democracy and Facebook's role in the perpetuation of those threats:

> Much of the evidence we have scrutinized during our inquiry has focused on the business practices of Facebook; before, during and after the Cambridge Analytica data breach scandal.
>
> ***We believe that in its evidence to the Committee Facebook has often deliberately sought to frustrate our work, by giving incomplete, disingenuous and at times misleading answers to our questions***.
>
> ***Even if Mark Zuckerberg doesn't believe he is accountable to the UK Parliament, he is to the billions of Facebook users across the world.***

> ***Evidence uncovered by my Committee shows he still has questions to answer yet he's continued to duck them, refusing to respond to our invitations directly or sending representatives who don't have the right information. Mark Zuckerberg continually fails to show the levels of leadership and personal responsibility that should be expected from someone who sits at the top of one of the world's biggest companies***.

185. Facebook's unrestrained sharing of personal user information, which facilitated Cambridge Analytica's ability to harvest personal user information, was at the center of the UK Disinformation Report. Specifically, the UK Disinformation Report explored, in detail, Facebook's data sharing and targeting practices, including "a disturbing disregard for voters' personal privacy," which had not changed after Facebook's entry into the 2012 Consent Order. Disturbingly, the UK Disinformation Report observed that Facebook, with Zuckerberg's knowledge, failed to curtail access to user data and brazenly allowed unfettered access to user information:

> When Richard Allan, Vice President of Policy Solutions at Facebook, gave evidence in November 2018, he told us that "our intention is that you should not be surprised by the way your data is used [. . .] It is not a good outcome for us if you are." Yet, ***time and again, this Committee and the general public have been surprised by the porous nature of Facebook data security protocols and the extent to which users' personal data has been shared in the past and continues to be shared today. The scale of this data sharing risks being massively increased, given the news that, by early 2020, Facebook is planning to integrate the technical infrastructure of Messenger, Instagram and WhatsApp, which, between them, have more than 2.6 billion users***.

* * *

In reply to a question as to whether CEO Mark Zuckerberg knew that Facebook continued to allow developers access to that information, after the [Consent Order], Richard Allan replied that Mr. Zuckerberg and "all of us" knew that the platform continued to allow access to information. As to whether that was in violation of the FTC Consent [Order] (and over two years after Facebook had agreed to it), he told us that "as long as we had the correct controls in place, that was not seen as being anything that was inconsistent with the FTC consent order."

Richard Allan was referring to Count 1 of the Federal Trade Commission's complaint of 2011, which states that Facebook's claim that the correct controls were in place was misleading:

> ***Facebook has represented, expressly or by implication, that, through their Profile Privacy Settings, users can restrict access to their profile information to specific groups, such as "Only Friends" or "Friends of Friends." In truth and in fact, in many instances, users could not restrict access to their profile information to specific groups, such as "Only Friends" or "Friends of Friends" through their Profile Privacy Settings. Instead, such information could be accessed by Platform Applications that their Friends used.***

Richard Allan's argument was that, while Facebook continued to allow the same data access—highlighted in the first count of the FTC's complaint and of which the CEO, Mark Zuckerberg, was also aware—that was acceptable due to the fact that Facebook had supposedly put "controls" in place that constituted consent and permission.

Ashkan Soltani, an independent researcher and consultant, was then a primary technologist at the Federal Trade Commission, worked on the Facebook investigation in 2010 to 2011 and became the Chief Technologist at the FTC in 2014. Before our Committee, he questioned Richard Allan's evidence:

> Mr. Allan corrected one of the comments from you all, specifically that apps in Version 1 of the API did not have unfiltered access to personal information. In fact, that is false. In the 2011 FTC settlement, the FTC alleged that if

> a user had an app installed, it had access to nearly all of the user's profile information, even if that information was set to private. I think there is some sleight of hand with regards to V1, but this was early v1 and I believe it was only addressed after the settlement.

Mr. Soltani clarified the timeline of events:

> The timelines vary, but this—in my opinion—was V1, if they are considering the changes in 2014 as V2. In short, ***I found that time and time again Facebook allows developers to access personal information of users and their friends, in contrast to their privacy settings and their policy statements***.

Richard Allan did not specify what controls had been put in place by Facebook, but they did not prevent app developers, who were not authorized by a user, from accessing data that the user had specified should not be shared (beyond a small group of friends on the privacy settings page). The FTC complaint took issue with the both the fact that apps had unfettered access to users' information, and that the privacy controls that Facebook represented as allowing users to control who saw their personal information were, in fact, inconsequential with regards to information to which the apps had access.

* * *

The Cambridge Analytica scandal was facilitated by Facebook's policies. If it had fully complied with the FTC settlement, it would not have happened. The US Federal Trade Commission (FTC) Complaint of 2011 ruled against Facebook—for not protecting users' data and for letting app developers gain as much access to user data as they liked, without restraint—and stated that Facebook built their company in a way that made data abuses easy. When asked about Facebook's failure to act on the FTC's complaint, Elizabeth Denham, the Information Commissioner, told us: "I am very disappointed that Facebook, being such an innovative company, could not have put more focus, attention and resources into protecting people's data. We are equally disappointed.

186. The UK Disinformation Report also raised the following business practices as further unrectified violations of the 2012 Consent Order and Facebook user privacy:

- whitelisting agreements;
- sharing of friends' data;
- the linkage of data access with spending on advertising at Facebook;
- data reciprocity between Facebook and Platform Applications;
- Facebook collecting call logs, text messages, and location data from Android users;
- Facebook's monitoring of how often other apps on a person's device were used; and
- Facebook's targeting of direct competitors to deny them access to data.

2. *The Individual Defendants Knew For Years That Cambridge Analytica Harvested Massive Amounts Of Personal User Information From Facebook, But Hid That Information From Public Disclosure*

187. Facebook had reason to know that Cambridge Analytica and GSR were harvesting massive amounts of data as early as 2014. Indeed, as Wylie testified to the U.K. House of Commons, Facebook's own servers flagged TIMDL's transmission of data in 2014 and even throttled the app's transfer of data from

Facebook's server.[58] Wylie specifically noted that when TIMDL transferred the data in 2014, Facebook's servers flagged the transmission due to its size and throttled the app's transfer of data from Facebook's server.[59] Kogan subsequently requested assistance from Facebook's engineers who then helped GSR successfully secure the data.[60] Thus, "Facebook [sh]ould have known from that moment about the project."[61]

188. Moreover, Kogan also had another "conversation with Facebook's engineers" concerning the data "or at least that's what he told [Wylie]."[62] Kogan told the U.K. House of Commons that Facebook "created these great tools for developers to collect the data. And [Facebook] made it very easy. I mean, this was not a hack. This was, 'Here's the door. It's open. We're giving away the groceries.

---

[58] *See* British Parliament House of Commons, Digital, Culture, Media and Sport Committee, *Oral Evidence: Fake News*, Testimony of C. Wylie (March 27, 2018) (hereinafter "Wylie Tr."), at Q1335, *available at*: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/fake-news/oral/81022.pdf..

[59] *Id.*

[60] *Id*.

[61] *Id*. at Q1336.

[62] *Id.*; *see also* Carole Cadwalladr, *Meet Wylie*, THE GUARDIAN (Mar. 18, 2018) (wherein Wylie explained: "Facebook could see it was happening . . . Their security protocols were triggered because Kogan's apps were pulling this enormous amount of data, but apparently Kogan told them it was for academic uses . . . So they were like: 'Fine.'").

Please collect them.'"[63] And while Kogan admits he violated Facebook's stated policy, which prohibits developers from disseminating, transferring, or selling gathered user data, Kogan emphasized that he did so openly, and in the direct view of Facebook. Kogan's user terms of service were publicly available and stated that users who clicked "OKAY" permitted him to "disseminate . . . transfer . . . or . . . sell . . . your . . . data."[64] Facebook "never cared. I mean, it never enforced this agreement."[65] TIMDL's terms of service "up there for a year and a half that said [it] could transfer and sell the data. Never a word."[66]

189. Later, in March 2018, Facebook Chief Technology Officer Schroepfer was asked by the British Parliament about Facebook's records detailing instances of known developer to developer platform abuses. Schroepfer responded that "[d]ue to system changes, we do not have records for the time-period before 2014."[67]

---

[63] L. Stahl, *Interview with A. Kogan*, 60 MINUTES, (Apr. 22, 2018), *available at*: https://www.cbsnews.com/news/aleksandr-kogan-the-link-between-cambridge-analytica-and-facebook/.

[64] *Id.*

[65] *Id.*

[66] *Id.*

[67] Letter from R. Stimson, Head of Public Policy, Facebook UK, to Damian Collins, Member of Parliament of the U.K. (May 14, 2018) ("Damian Collins Letter") at 3, *available at*: https://www.parliament.uk/globalassets/documents/commons-committees/culture-media-and-sport/180514-Rebecca-Stimson-Facebook-to-Ctte-Chair-re-oral-ev-follow-up.pdf.

Records did not exist because Facebook did not vet or monitor its third-party app developers' utilization of user information. *See e.g.* ¶¶18, 262, 282–83.

190. Indeed, in an October 2012 email to Sam Lessin, Defendant Zuckerberg acknowledged and dismissed the risk to Facebook arising from third-party data leakage, writing:

> "I am generally skeptical that there is as much data leak strategic risk as you think. I agree there is clear risk on the advertiser side, but I haven't figured out how that connects to the rest of the platform. I think we leak info to developers, but I just can't think of any instances where that data has leaked from developer to developer and caused a real issue for us."[68]

191. By 2015, Facebook knew that the personal user information it had been openly sharing with partners through Platform Applications was being used for nefarious ends by Cambridge Analytica. The Office of the Attorney General for the District of Columbia obtained and later released documents showing that Facebook's employees raised concern about "sketchy" Cambridge Analytica months before Facebook initially claimed to have knowledge of Cambridge Analytica's data harvesting. In connection with the release of such documents in 2019, the Office of the Attorney General for the District of Columbia stated that, according to the documents, "Facebook employees were raising alarms about political partners and

[68] 643 Docs, *supra* note 5, at FB-01389021.

doubts about their compliance with Facebook's data policies as far back as September 2015."

192. By December 2015, Facebook also became aware that Cambridge Analytica was using private Facebook data to help Senator Ted Cruz's campaign.

193. Rather than taking action to verify that Kogan and Cambridge Analytica had destroyed the data, Facebook merely requested that they delete the personal user information Facebook allowed to be disclosed. Facebook took no action to verify that Cambridge Analytica destroyed the data in question and did not release any further statements to the public until investigative journalists discovered that Cambridge Analytica held vast amounts of Facebook personal user information. Facebook only obtained written certifications from Kogan and Cambridge Analytica that the data had been destroyed in June 2016 and April 2017, respectively.

194. A Facebook spokesman stated: "[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." Facebook made no further statements regarding Cambridge Analytica until after March 17, 2018, when joint reporting from *The New York Times*, *The Observer* of London, and *The Guardian* subjected the Company to vast amounts of scrutiny from regulators and the public. Instead of welcoming the disclosure, in an attempt to keep the incident private, Facebook

threatened to sue *The Observer* in order to prevent media coverage regarding the sharing of personal user information from attracting more scrutiny.

195. The UK Disinformation Report confirms that Facebook had known about the Cambridge Analytica data breach for years before it had become public in 2018. As the UK Disinformation Report noted, the ICO confirmed that at least three "senior managers" at Facebook were involved in email exchanges in early 2015 concerning the Cambridge Analytica data breach. But, because there was a "profound failure of governance within Facebook," the Company failed to treat the fact that Cambridge Analytica had obtained vast amounts of personal user information with the seriousness it merited.

H. Sandberg Admits That Facebook Knew About Cambridge Analytica For Two And A Half Years, But Took No Action

196. Sandberg appeared on *NBC*'s "Today Show" on April 6, 2018, acknowledging that Facebook had (i) known that Cambridge Analytica had obtained and mishandled users' data; and (ii) committed a "breach of trust" with users by failing to protect user data and failing to notify users of the data breach. Sandberg stated that the Company "could have done these [audits regarding data breaches] two

and a half years ago," after the Company first learned about Cambridge Analytica's improper access to user data in December 2015.

197. Sandberg gave no explanation as to why Facebook chose to forego such an audit. Nor did she address why Facebook had failed to meet its obligations under the 2012 Consent Order. Instead, she stated that Facebook executives thought the data had been deleted and failed to "check" after Facebook's sharing of the personal information of 87 million users, relying on assurances from Cambridge Analytica that the data had been deleted.

I. Congress Calls Defendant Zuckerberg To Question And Is Met With Dishonesty

198. On April 10, 2018, Zuckerberg was called to testify before the U.S. Senate Committee on Commerce, Science and Transportation and Committee on the Judiciary (the "Senate Hearing"), and on April 11, 2018, he was called to testify before the House of Representatives Committee on Energy and Commerce (the "House Hearing"). In both instances, Congress sought Zuckerberg's testimony concerning Cambridge Analytica's access to Facebook user data, Facebook's privacy policies and practices generally, and certain other matters.

199. As he did at the time of the FTC's November 2011 allegations, Zuckerberg again relied on a familiar pattern of misrepresentations. Specifically, he testified repeatedly that Facebook users had complete control over their who they

share their data with, despite the Cambridge Analytica Breach and the various programs approved by Zuckerberg precisely to skirt this supposed control.

200. *First,* Zuckerberg falsely insisted that, despite the Cambridge Analytica breach, Facebook users had ***full control*** over their data. For example, as reflected in the transcript of his April 10, 2018 Senate testimony:

a. When asked whether he considered a user's personally identifiable data to be "the company's data, not [the user's] data?," Zuckerberg stated: "No, Senator. ***Actually, the first line of our terms of service say that you control and own the information and content that you put on Facebook***.

b. In describing Facebook's core principles, Zuckerberg stated: "This is the most important principle for Facebook: Every piece of content that you share on Facebook, you own and ***you have complete control 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."

c. Similarly, in response to another question, Zuckerberg stated "Yes, Senator. I think everyone should have control over how their information is used.

And as we have talked about in some of the other questions, I think that that is laid out in some of the documents, but more importantly, you want to give people control in the product itself. So the most important way that this happens across our services is that ***every day people come to our services*** to choose to share photos or send messages, ***and every single time [users] choose to share something, they have a control right there about who they want to share it with***."

d. As Zuckerberg also testified, (i) "That's what the [Facebook] service is, right, is 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 who you share it with,*** you can take it down if you want, and you do not need to put anything up in the first place if you do not want;" and (ii) "The two broad categories that I think about are ***content that a person [has] 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.***"

e. In sum, as Zuckerberg put it: "***Every person gets to control who gets to see their content***."

201. On April 11, 2018, during his House Hearing testimony, Zuckerberg repeated a similar line of misrepresentations, stating:

a. ". . . on Facebook, ***you have control over your information***."

b. "***[E]very 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 is not just kind of an add-on feature, it is something we have to comply with."

d. "Congresswoman, ***all the data that you put in, all the content that you share on Facebook is yours. You control how it's used***."

202. On June 8, 2018, Facebook also submitted certain written *Responses to Additional Questions from the Senate Commerce Committee* on Zuckerberg's behalf. These responses further built on Zuckerberg's false and misleading statements in his live testimony by representing, *inter alia*, that "Privacy is at the core of everything we do [at Facebook], and our approach to privacy starts with our commitment to transparency and control . . . . ***Our approach is 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***."

203. However, as with Zuckerberg's and Facebook's previously discussed statements from 2011, the statements referenced in ¶¶198-201 above were all materially false and misleading because users did not have "complete control" over the sharing of their own personal information "every time," and any assertion that the Company's "most important principle" was to give its users such control was laughable.

a. *First*, even as Zuckerberg was testifying in 2018, Facebook continued to have numerous "whitelisting" agreements in place, including with other large companies such as Amazon, Microsoft, Netflix, Spotify and the United Parcel Service—and Facebook was also snooping on Android phone users' telephone call logs, text messages and location data to amass even more personal and private information on its users.

b. Similarly, *The New York Times* reported on June 3, 2018 that "most of [Facebook's] whitelisting partnerships remained in effect, as Facebook had exempted the companies it favored from any data sharing restrictions." On December 18, 2018 the *New York Times* also revealed that ***Facebook had whitelisting agreements with more than 150 companies, many of which continued past the date of Zuckerberg's testimony,*** from tech businesses, online retailers and entertainments sites, to automakers and media organizations.

c. The applications for these whitelisted partners were active starting in 2010, through at least 2018. In response to a December 18, 2018 *New York Times* article on Facebook's continuing practice of sharing personal user information with its whitelisting partners, Facebook's director of privacy and public policy claimed that "the partnerships were 'one area of focus,'" and admitted that Facebook was, belatedly, "***in the process*** of winding many of them down."

204. *Second*, Zuckerberg gave false testimony regarding the data shared through Android phones and other digital devices. In particular, during the April 2018 Senate Hearing, Zuckerberg gave the following false and misleading responses to questions by Senators Roger Wicker and Roy Blunt:

> **[Senator WICKER.]** Let me move on to another couple of items. Is it true, as was recently publicized, that Facebook collects the call and text histories of its users that use android phones?
>
> **Mr. ZUCKERBERG**. Senator, we have an app called Messenger for sending messages to your Facebook friends, and that app offers people an option to sync their text messages into the messaging app and to make it so that—basically, so you can have one app where it has both your texts and your Facebook messages in one place. We also allow people the option——
>
> **Senator WICKER**. You can opt in or out of that?
>
> **Mr. ZUCKERBERG**. Yes.
>
> **Senator WICKER**. Is it easy to opt out?
>
> **Mr. ZUCKERBERG**. It is opt-in. ***You have to affirmatively say that you want to sync that information before we get access to it.***

Senator WICKER. Unless you opt in, you do not collect that call and text history?

Mr. ZUCKERBERG. That is correct.

* * *

Senator BLUNT. Am I able to opt out? Am I able to say it is OK for you to track what I am saying on Facebook, but I do not want you to track what I am texting to somebody else off Facebook on an android phone?

Mr. ZUCKERBERG. Oh, OK. Yes, Senator. ***In general, Facebook is not collecting data from other apps that you use.*** There may be some specific things about the device that you are using that Facebook needs to understand in order to offer the service, ***but if you are using Google or you are using some texting app, unless you specifically opt-in that you want to share the texting app information, Facebook would not see that information.***

205. The Zuckerberg testimony quoted in the immediately preceding paragraph was materially false and misleading. Simply stated, a Facebook user on an Android device would unknowingly give Facebook the ability to access and store information concerning, among other things, the user's: (a) call and text history, (b) identifiers and IDs for all other apps associated with the device, (c) Bluetooth signals, (d) GPS location, (e) camera and photos, and (f) cookie IDs and settings—all of which Facebook acknowledged it had gathered in its supplemental responses to questions asked by Senators during the hearing. Facebook also was forced to acknowledge in its supplemental responses that "These partners [advertisers, app developers and publishers] provide information about a person's activities off

Facebook—including information about their device, ***websites they visit, purchases they make, the ads they see, and how they use their services—whether or not they have a Facebook account or are logged into Facebook.***"

206. In fact, the whole point of Facebook's pursuit of its Android integration program was to allow Facebook to obtain access to this personal user information ***without*** the users ever realizing that such access was being granted (let alone having to obtain their express consent), as the Facebook internal emails described *supra* ¶¶103-64, demonstrate.

207. The extent to which Facebook extracted personal user without consent is highlighted by a December 2018 report by Privacy International entitled *How Apps on Android Share Data with Facebook*. As that report concluded, based on testing conducted earlier that month, "***at least 61 percent of apps we tested automatically transfer data to Facebook the moment a user opens the app. This happens whether people have a Facebook account or not, or whether they are logged into Facebook or not***." A March 2019 updated report from Privacy International, *Investigating Apps interactions with Facebook on Android*, similarly concluded that "many apps still exhibit the same behaviour we described in our original report. ***These apps automatically transfer personal data to Facebook the moment a user opens the app, before people are able to agree or consent. This***

happens whether people have a Facebook account or not, or whether they are logged into Facebook or not."

208. *Third*, in his April 2018 Congressional testimony, Zuckerberg gave a highly misleading defense of Facebook's failure to verify that the data appropriated by Prof. Kogan and Cambridge Analytica had been deleted, and of Facebook's failure to notify Facebook users that their data had been breached.

209. Among other things, Zuckerberg testified in his prepared statement for the Senate Hearing as follows:

> In 2015, we learned from journalists at The Guardian that Kogan had shared data from his app with Cambridge Analytica. ***It is against our policies for developers to share data without people's consent, so we immediately banned Kogan's app from our platform***, and demanded that Kogan and other entities he gave the data to, including Cambridge Analytica, formally certify that they had deleted all improperly acquired data—***which they ultimately did***.

210. It did not take long to identify that Zuckerberg was not telling the truth. Contradicting Zuckerberg's testimony, during the April 10, 2018 Senate Hearing itself, Senator Richard Blumenthal ("Blumenthal") noted that Facebook's policies violated the 2012 Consent Order. Blumenthal noted that the terms of service Facebook agreed to enter into with Kogan, the researcher who sold the user data of 87 million Facebook users to Cambridge Analytica for $800,000, explicitly allowed Kogan to sell user information. Blumenthal further noted that these terms of service, which allowed third parties to sell user data, conflicted with the 2012 Consent Order,

which specifically required Facebook to protect user privacy and amounted to "***willful blindness***." Zuckerberg responded that, "[Facebook] should have been aware that this app developer submitted a term that was in conflict with the rules of the platform."

211. Further, as Zuckerberg knew, Facebook did not obtain certifications from Kogan or Cambridge Analytica until June 2016 from Kogan and until ***2017*** from Cambridge Analytica, well after Facebook first learned of the data breach.[69] As confirmed by the UK Committee's observations from its investigation into Facebook's practices (*infra* ¶¶217–26), Kogan's app was not an outlier and did not stand outside Facebook's policies: instead, ***Facebook "worked with such apps as an intrinsic part of its business model," many other Platform Applications conducted the same personal user data mining operations, and Facebook's arguments to the contrary were in "bad faith."*** This shows a shocking lack of regard for ensuring the privacy of data misappropriated for 87 million Facebook customers. Also, Facebook knew that both Kogan and Cambridge Analytica had

[69] Previously, Facebook had relied solely on oral confirmations.

lied to it about the data that had been provided to Cambridge Analytica.[70] Yet, rather than taking any other steps to audit or verify, Facebook took their word.

212. Zuckerberg also stated in his prepared statement that:

> We made some big changes to the Facebook platform in 2014 to dramatically restrict the amount of data that developers can access and to proactively review the apps on our platform. ***This makes it so a developer today can't do what Kogan did years ago.***

213. In fact, the underlying user data was taken by Kogan only ***after*** the platform change, which Facebook announced in April 2014. As the SEC Complaint states on this subject:

> ***In the summer and early fall of 2014***, a business entity created and controlled by the researcher [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.***

SEC Complaint ¶24.

214. Further, as alleged *supra* ¶¶103–64, Facebook's platform changes did nothing to shore up user privacy, but were instead focused on the means by which

[70] Specifically, Kogan and Cambridge Analytica both represented to Facebook that Cambridge Analytica had received only the personality scores created by Kogan, and not the underlying user data Kogan obtained from Facebook. But in June 2016, Kogan entered into a "Confidential Settlement Agreement and Mutual Release" settlement with Facebook, in which he stated that the he had transferred highly sensitive user information including names, birthdays, location and certain page likes to Cambridge Analytica, and not just the personality scores.

Facebook could make personal user information more lucrative for the Company. Whitelisting agreements continued at the time of Zuckerberg's testimony, and the sharing of data without consent remained in place. As the FTC stated in connection with their eventual settlement with the Company, 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***." FTC Complaint at ¶¶173-74.

215. Zuckerberg also testified that Facebook did not notify customers or the FTC of the Cambridge Analytica breach "because we considered it a closed case" based on Kogan's and Cambridge Analytica's word. For example, in response to a question by Senator Bill Nelson, Zuckerberg testified:

> ***Senator, when we heard back from Cambridge Analytica that they had told us that they were not using the data and they had deleted it, we considered it a closed case.*** In retrospect, that was clearly a mistake. We should not have taken their word for it, and we have updated our policies and how we are going to operate the company to make sure that we do not make that mistake again.
>
> Senator NELSON. Did anybody notify the FTC?
>
> Mr. ZUCKERBERG. No, Senator, for the same reason, that ***we had considered it a closed case.***

216. But Facebook did not obtain a certification from Cambridge Analytica until ***2017***, and Facebook's privacy policy (in place since at least February 2017) did not exempt notifications for customers whose data was breached merely because the exploitation of that data may have ended, based solely on the exploiter's word.

J. Facebook Also Misleads UK Regulators

217. Compounding Zuckerberg's misleading responses to Congress, Facebook also was not forthcoming with the UK Committee. As the UK Disinformation Report notes, the opposite was true: "Facebook has continually hidden behind obfuscation." Facebook refused to give evidence to the UK Committee, then was forced to respond to revelations regarding its unlawful business plans unearthed by internal documents released to the public.

218. Facebook's response was to try to cast the Platform Applications that Facebook shared data with as "sketchy apps." But, as the UK Disinformation Report noted, Joseph Chancellor, a director of GSR, the organization responsible for the Platform Application that shared user information with Cambridge Analytica ("Chancellor"), was hired by Facebook as a quantitative researcher on the User Experience Research team within two months of his leaving the purportedly "sketchy" company. Facebook provided the UK Committee with no explanation for its recruitment of Chancellor, despite Facebook presenting his company's work as a

very serious breach of its terms and conditions after the full extent of Facebook's information sharing became public.

219. When Aleksandr Kogan was asked by the UK Committee whether it was strange that Facebook hired Chancellor, Kogan responded: "The reason I don't think it's odd is because, in my view, ***Facebook's comments are PR crisis mode. I don't believe they actually think these things, because I think they realise that the platform has been mined left and right by thousands of others***."

220. The UK Disinformation Report found Kogan's analysis credible, noting that Facebook's own internal documents showed that the Facebook platform had been designed to violate user privacy from its inception. As the UK Committee observed:

> We believe that Mark Zuckerberg's response to the publication of the [internal Facebook documentary] evidence was, similarly, to use Dr. Kogan's description, "PR crisis mode." ***Far from Facebook acting against "sketchy" or "abusive" apps, of which action it has produced no evidence at all, it, in fact, worked with such apps as an intrinsic part of its business model. This explains why it recruited the people who created them, such as Joseph Chancellor. Nothing in Facebook's actions supports the statements of Mark Zuckerberg who, we believe, lapsed into "PR crisis mode," when its real business model was exposed. This is just one example of the bad faith which we believe justifies governments holding a business such as Facebook at arms' length . . . . Despite specific requests, Facebook has not provided us with one example of a business excluded from its platform because of serious data breaches. We believe that is because it only ever takes action when breaches become public. We consider that data transfer for value is Facebook's business model and that Mark***

> ***Zuckerberg's statement that "we've never sold anyone's data" is simply untrue***.
>
> The evidence that we obtained from [internal Facebook] documents indicates that Facebook was willing to override its users' privacy settings in order to transfer data to some app developers, to charge high prices in advertising to some developers, for the exchange of that data, and to starve some developers . . . of that data, thereby causing them to lose their business. ***It seems clear that Facebook was, at the very least, in violation of its Federal Trade Commission settlement***.
>
> The Information Commissioner told the Committee that Facebook needs to significantly change its business model and practices to maintain trust. ***From the documents we received . . . it is evident that Facebook intentionally and knowingly violated both data privacy and anti-competition laws***. The ICO should carry out a detailed investigation into the practices of the Facebook Platform, its use of users' and users' friends' data, and the use of 'reciprocity' of the sharing of data.

221. While Facebook treated Cambridge Analytica as a lone bad actor, it took no apparent action in response to the Cambridge Analytica scandal to protect its users' personal information on the Facebook platform or otherwise ensure compliance with the 2012 Consent Order. Facebook did not publicly acknowledge or verify that it had allowed personal user information to be released *en masse* through its Platform Applications, a practice that continues through the present. Facebook did not inform users that their personal data had been harvested and used for political gain; nor is there any indication that Facebook attempted to identify and notify the users affected.

222. In fact, Cambridge Analytica was not a lone bad actor but was instead one of many developers that Facebook provided access to user data, including Friends data, without regard for their privacy selections. For example, Ashkan Soltani, the "primary technologist at the Federal Trade Commission" who "worked on the Facebook investigation in 2010-11" and who later became the "chief technologist at the FTC in 2014" testified to Parliament that, "time and time again Facebook allow[ed] developers to access personal information of users and their friends, in contrast to their privacy settings and their policy statements . . . Facebook prioritise[d] [sic] these developers over their users."[71]

223. The U.K. Disinformation Report went on to summarize evidence that Facebook explicitly implemented a business plan to "override its users' privacy settings in order to transfer data to some app developers."[72] The Report also noted that Facebook executives—who at the time included Defendant Zuckerberg and Defendant Sandberg—were aware of data privacy breaches, and that Defendant

[71] British Parliament House of Commons, Digital, Culture, Media and Sport Committee, *Oral Evidence: Fake News*, Testimony of Ashkan Soltani (Nov. 27, 2018) at Q4327, *available at*: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake-news/oral/92924.pdf.

[72] U.K. Disinformation Report, *supra* note 4, at ¶ 135.

Zuckerberg and Defendant Sandberg attempted to "deflect attention" from those breaches to avoid scrutiny.[73]

224. The U.K. Disinformation Report further found that the controls Facebook put in place after the 2012 Consent Order "did not prevent app developers, who were not authorized by a user, from accessing data that the user had specified should not be shared (beyond a small group of friends on the privacy settings page),"[74] and that "Facebook was willing to override its users' privacy settings in order to transfer data to some app developers."[75]

225. As Schroepfer, later testified to Parliament that Facebook made a mistake not to alert users to the fact that Facebook's data was misappropriated by Cambridge Analytica in 2015,[76] apologized for the breach of users' trust,[77] and confirmed that Facebook was investigating whether Palantir—a secretive

[73] *Id.* at ¶ 250.

[74] *Id*. at ¶ 74.

[75] *Id.* at ¶ 135.

[76] British Parliament House of Commons, Digital, Culture, Media and Sport Committee, *Oral Evidence: Fake News*, Testimony of Mike Schroepfer ("Schroepfer Tr."), at Q2175, *available at*: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake-news/oral/82114.pdf.

[77] *Id*. at Q2200.

intelligence firm that may have worked with Cambridge Analytica with ties to Defendants Thiel and Andreessen—had accessed Facebook user data.[78]

226. Richard Allan ("Allan"), the Vice President of Policy Solutions at Facebook, also testified before Parliament's Digital Committee that "the CEO and senior management—'all of us'—knew that Facebook was continuing to allow [data access by app developers] to occur, despite the public statements about its change of policy."[79] At the time, senior management included Defendant Zuckerberg, Defendant Sandberg, and many of the Facebook's officers identified herein. The British Parliament thus concluded Facebook's disinformation "constituted deceit."[80]

K. The FTC And Other Regulators Open Investigations Into Facebook's Continuing Illegal Conduct

1. *The FTC Announces An Investigation Into Facebook's Violations Of The 2012 Consent Order*

227. On March 20, 2018, following public knowledge of the fact that Facebook had allowed Kogan and Cambridge Analytica to obtain a vast swath of personally identifiable user information for millions of Facebook users, a large group of U.S. consumer privacy advocates joined in writing a letter to the Acting Chairman and Commissioner of the FTC calling for the FTC to open an investigation into

[78] *Id*. at Q2338.

[79] U.K. Disinformation Report, *supra* note 4, at ¶ 75.

[80] *Id*.

whether Facebook had violated the 2012 Consent Order. The March 20, 2018 letter read as follows:

> Dear Acting Chairman Ohlhausen and Commissioner McSweeney:
>
> On behalf of leading consumer privacy organizations in the United States, we urge you to immediately investigate whether Facebook's alleged disclosure of the personal data of 50 million Americans to the data mining firm Cambridge Analytica violated the FTC Consent Order with Facebook we helped obtain.
>
> As the Facebook Order makes clear, Facebook must "get consumers' approval before it changes the way it shares their data," and must "obtain consumers' affirmative express consent before enacting changes that override their privacy preferences." The FTC also barred Facebook form "making misrepresentations about the privacy or security of consumers' personal information."
>
> Yet Facebook's business practices resulted in the disclosure of consumers' "names, education, work histories, birthdays, likes, locations, photos, relationship statuses, and religious and political affiliations" to Cambridge Analytica without their knowledge or consent. In 2014, Facebook acknowledged that it allowed app developers to access profile information on an app user's friends without the friend's knowledge or consent, stating that consumers "are often surprised when a friend shares their information with an app." Facebook's admission that it disclosed data to third parties without users' consent suggests a clear violation of the 2011 Facebook Order.
>
> The 2011 Facebook Order was the result of an extensive complaint filed by EPIC and a coalition of consumer organizations in 2009, following Facebook's repeated changes to the privacy settings of Facebook users that allowed the company to transfer user data without the knowledge or consent of the user. We documented this practice, noted the views of many users, and established the FTC's authority to act as we had in other similar matters.
>
> The FTC agreed with us, charging that "Facebook changed its website so certain information that users may have designated as private—such

as their Friends List—was made public. They didn't warn users that this change was coming, or get their approval in advance." The FTC also found that, "Facebook represented that third-party apps that users installed would have access only to user information that they needed to operate. In fact, the apps could access nearly all of users' personal data—data the apps didn't need.

Facebook's transfer of personal data to Cambridge Analytica was prohibited by the 2011 Facebook Order. The FTC's failure to enforce its order has resulted in the unlawful transfer of 50 million user records to a controversial data mining firm to influence a presidential election.

The FTC has an obligation to the American public to ensure that companies comply with existing Consent Orders. It is unconscionable that the FTC allowed this unprecedented disclosure of Americans' personal data to occur. The FTC's failure to act imperils not only privacy but democracy as well.

We have also repeatedly warned the FTC that it has an affirmative duty to undertake a review of substantial changes in business practices of a company subject to a consent order that implicates the privacy of Internet users. The FTC's apparent failure to pursue such review has led to a downward spiral in the protection for American consumers.

The Commission must immediately undertake an investigation and issue a public report as to whether Facebook complied with the 2011 Order.

Sincerely,

Electronic Privacy Information Center
Access Now
Campaign for Commercial Free Childhood
Center for Digital Democracy
Constitutional Alliance
Consumer Action
Consumer Federation of America
Consumer Watchdog
Cyber Privacy Project
Defending Rights & Dissent

Government Accountability Project
Patient Privacy Rights
Privacy Rights Clearinghouse
Privacy Times
Public Citizen
U.S. PIRG
World Privacy Forum

The letter was also copied to the U.S. House of Representatives Committee on Oversight and Reform.

228. On March 26, 2018, the FTC issued a press release announcing that it was pursuing an open, non-public investigation into Facebook's privacy practices and compliance with the 2012 Consent Order. Tom Pahl, the FTC's Acting Director ("Pahl"), noted in the press release that the FTC's foremost tool for protecting consumer privacy was to bring an enforcement action against companies that fail to honor prior privacy promises. Pahl also reiterated that Facebook had an obligation to comply with the 2012 Consent Order's imposition of privacy and data security requirements on the Company.

2. *The SEC, DOJ And FBI Open Their Own Inquiries Into Facebook's Treatment Of User Information*

229. Facebook's flagrant disregard for the protection of its users' personal information also resulted in investigation by other agencies. As first reported in *The Washington Post* on July 2, 2018, as of that date a federal investigation into Facebook's sharing of data with Cambridge Analytica had broadened to focus on the

actions and statements of the Company and involved the SEC, FBI and DOJ. *The Washington Post* reported that the regulators had confirmed that Facebook knew Cambridge Analytica had obtained Facebook data in 2015, yet failed to disclose that information until March 2018, as confirmed by five people with knowledge of the probes discussing the ongoing investigation anonymously.

230. *The Wall Street Journal* reported on further details regarding the SEC's investigation on July 12, 2018. The SEC reportedly had requested information from Facebook on how much the company knew about Cambridge Analytica's use of user data. The report stated that the SEC was also investigating how Facebook analyzed the risk it faced from developers who shared data. It was also widely reported that representatives from the FBI and FTC had joined the DOJ in its inquiries into Facebook's sharing of personal user information, suggesting that the probes had a wide-ranging nature, and centered on why Facebook failed to reveal its knowledge of data-sharing at the time to its users and shareholders.

L. Facebook's Impaired Governance Function Prevents It from Coming into Compliance with the 2012 Consent Order

231. Unfortunately for Facebook and its shareholders, the Individual Defendants failed to bring Facebook into compliance with the 2012 Consent Order, even in the wake of the public release of Facebook's unprecedented violations of user privacy, regulatory investigations, calls for action from privacy advocates, and

statements from UK authorities that the Company was a threat to democratic processes and privacy rights and did not take its obligations seriously. Instead, the Individual Defendants caused Facebook to continue to expand its violations of the 2012 Consent Order and obfuscate in response to investigations into its illegal activity.

1. *The Extent Of Facebook's Ongoing, Vast Information Sharing Is Gradually Uncovered*

232. A June 3, 2018 article published by *The New York Times* revealed that Facebook had struck deals for sharing personal user information with over 60 electronic device manufacturers. Facebook allowed the device companies continued access to the data of users and users' friends without their consent, even after declaring that it would no longer share such information with outsiders. Some device makers could also retrieve personal information even from users' friends who had set Facebook's privacy settings to explicitly deny the permission to share information with any third parties. Moreover, *The New York Times* also disclosed that ***the Company's whitelisting partnerships remained in effect, as Facebook had exempted the companies it favored from any data sharing restrictions***. And as later reported in September 20, 2019 by *CNBC*, Facebook had allowed personal user information to be shared, without user consent, with "***tens of thousands of apps***."

At this late date, the Company stated that it was still belatedly suspending these Platform Applications, ***which involved 400 companies***, from the Facebook platform.

233. A follow-up June 5, 2018 article published by *The New York Times* further reported that Facebook maintained data-sharing partnerships with at least four Chinese electronic companies, which dated back to at least 2010. The companies included the manufacturing firm Huawei Technologies Co., Ltd. ("Huawei"), a telecommunications equipment company that had been cited in congressional reports as having a "close relationship" with the Chinese Communist Party, and had been flagged by American intelligence officials as a national security threat. Facebook also maintained its data-sharing with Lenovo Group Ltd., OPPO Mobile Telecommunications Corporation, and TCL Corporation.

234. Facebook officials responded to *The New York Times* June 5, 2018 article by stating that the agreements with Chinese companies allowed them to access detailed information about both the users of the device and all of their friends—including religious and political leanings, work and education history, and relationship status. Facebook's Vice President of Mobile Partnerships, Francisco Varela, stated, "[a]ll Facebook's integrations with Huawei, Lenovo, Oppo, and TCL were controlled from the get-go—and Facebook approved everything that was built."

235. On June 8, 2018, *The Wall Street Journal* reported that Facebook struck customized data-sharing deals with companies including Royal Bank of Canada and Nissan Motor Co. The deals were notable for showing that Facebook shared personal user information to a broader universe of companies than it had previously disclosed, and that Facebook had not disclosed the full range of companies with whom it was sharing personal user information. The news was also significant because it showed that Facebook continued to share personal user information, despite prior statements by Facebook that the Company had "walled off" other companies from using personal user information.

236. On July 1, 2018, *The Wall Street Journal* reported that Facebook continued to share user data, including the data of friends of users who had not consented to third-party sharing, with 61 app developers, including the dating app Hinge and shipping giant United Parcel Service Inc., nearly six months after Facebook had purported to stop access to this data in 2015. And, as later reported in September 20, 2019 by *CNBC*, Facebook had allowed personal user information to be shared, without user consent, with "***tens of thousands of apps***." At this late date, the Company stated that it was still belatedly suspending these Platform Applications, ***which involved 400 companies***, from the Facebook platform.

237. On June 29, 2018, Facebook sent 747 pages of additional information to Congress in response to its probe into the Company's data sharing practices,

revealing that Facebook had maintained whitelisting agreements with dozens of companies, including developers of Platform Applications, months after the Company stated it had stopped such practices. The new information contradicted Facebook's prior statements that it had restricted personal information to outsiders in 2015 and came only after news organizations, including *The New York Times* and *The Wall Street Journal*, had already revealed that Facebook continued to share personal user information with third parties.

238. *NBC News* further reported, on July 11, 2018, that Russian internet company Mail.ru, one of the top five largest internet companies in the world, with ties to the Kremlin, had been granted the ability to access and collect Facebook user data, including those who had explicitly denied permission for data-sharing with third parties. That day, Senator Mark Warner (D-Va) wrote in an email:

> ***In the last six months we've learned that Facebook had few controls in place to control the collection and use of user data by third parties. Now we learn the largest technology company in Russia, whose executives boast close ties to Vladimir Putin, had potentially hundreds of apps integrated with Facebook, collecting user data***. We need to determine what user information was shared with Mail.ru and what may have been done with the captured data.

239. On December 18, 2018, *The New York Times* further reported that Facebook gave some of the world's largest technology companies more intrusive access to personal user information than it has disclosed, "effectively exempting those partners from its usual privacy rules." The reporting, based on internal records

and interviews conducted by *The New York Times*, revealed that Facebook maintained an internal system for tracking partnerships through at least 2017.

240. The documents obtained by *The New York Times* showed Facebook's profound failure to cease whitelisting agreements. Facebook continued to allow Microsoft's Bing search engine through at least 2017 to see the names of virtually all Facebook users' friends without consent, and gave Netflix and Spotify the ability to read Facebook users' private messages. The documents also showed that Facebook continued to allow Amazon to obtain users' names and contact information through their friends, and continued to allow Yahoo! to view streams of users' friends' posts as recently as summer 2018, despite public statements by Facebook and Zuckerberg that it had stopped this type of sharing years earlier.

241. Further, as *The New York Times* discovered, ***Facebook continued to have whitelisting agreements with more than 150 companies***, from tech businesses, online retailers and entertainments sites, to automakers and media organizations. ***The Platform Applications for these Facebook partners continued to obtain the data of hundreds of millions of people a month, and were active starting in 2010 through 2018***. Steven Satterfield, Facebook's director of privacy and public policy, confirmed that "the partnerships were 'one area of focus'" and claimed that, as of December 2018, Facebook was "in the process of winding many of them down." But, as later reported in September 20, 2019 by *CNBC*, Facebook had allowed

personal user information to be shared, without user consent, with "***tens of thousands of apps***." At this late date, the Company stated that it was still belatedly suspending these Platform Applications, ***which involved 400 companies***, from the Facebook platform.

242. Facebook's response was that it had found no evidence of abuse by its partners, and therefore the whitelisting agreements somehow did not violate the 2012 Consent Order. ***Quizzically, Satterfield stated that Facebook was within the bounds of the 2012 Consent Order and was not required to secure user consent before sharing data because Facebook considered the partners, including device makers, retailers and search companies, to be extensions of itself***.

243. Soltani, former chief technologist at the FTC, disputed that contention, noting that the only similarity between the partners was that they allowed Facebook access to development or growth in business sectors they could not otherwise obtain access to. David Vladeck, former Director of the FTC's Consumer Protection Bureau, also stated:

> This is just giving third parties permission to harvest data without you being informed of it or giving consent to it. I don't understand how this unconsented-to data harvesting can at all be justified under the [Consent Order].

2. *The Board Ignores Widespread Defection And Internal Warnings From Employees*

a. Alex Stamos Departure

244. On March 19, 2018, two days after the Cambridge Analytica scandal broke, *The New York Times* reported that Alex Stamos, then Chief Information Security Officer for Facebook, had decided to leave the Company. According to current and former employees, the departure was the result of internal disagreement about how much Facebook should publicly disclose about how the Facebook platform was being misused for political purposes.

245. Stamos had advocated for more disclosure but was met with resistance internally. Specifically, Stamos was encouraged by the Facebook communications team to "tweet," or release messaging on social media app Twitter, regarding the Cambridge Analytica data harvesting in response to the March 17, 2018 reporting by *The New York Times* immediately following public release of the reporting. Stamos was instructed to tweet in defense of the Company, but only after the communications team had approved the tweets. The tweets reportedly set off a furious response internally, causing Stamos to delete them.

246. On November 14, 2018, *The New York Times* released an explosive report regarding Alex Stamos's departure, based on interviews of more than 50 people, including current and former Facebook executives and other employees. *The*

New York Times had uncovered that, in the spring of 2016, Stamos's security team discovered that Russian hackers were probing Facebook accounts for the personal user information of people connected to United States presidential campaigns. The security team also found Facebook accounts linked to Russian hackers who were messaging journalists to share information from the stolen emails of presidential candidate Hillary Clinton.

247. Stamos met with Facebook's general counsel to discuss the fact that Facebook had no policy in place to deal with these developments, or any resources dedicated to searching for and putting a stop to these intrusions. Stamos organized a team to investigate the extent of Russian activity on Facebook. Meanwhile, Zuckerberg publicly discredited the idea that Russians were using the Facebook platform to gather personal user information and manipulate users.

248. Sandberg, for her part, became angry because Stamos began looking into the Russian activity without approval. But Sandberg and Zuckerberg eventually relented, deciding to expand Stamos's work by creating a group called "Project P" to investigate propaganda and other activity by the Russians. By January 2017, Stamos and his team knew that they had only scratched the surface of Russian activity on the platform and pressed to issue a public paper about their findings.

249. Joel Kaplan, Facebook's Vice President for Corporate Public Policy ("Kaplan"), who had attended Harvard University with Defendant Sandberg,

objected to the public release due to the negative PR Facebook could incur. Defendant Sandberg sided with Kaplan, and when Stamos's security paper was published in April 2017, the word "Russia" appeared nowhere in the document.

250. Defendant Zuckerberg was absent at this time, as he spent much of 2017 on a "listening tour," gathering ideas outside Facebook and away from his Company duties.

251. When the United States Senate began pursuing its own investigation into Russian hacking, throughout the spring and summer of 2017, Facebook officials, at Sandberg's direction, repeatedly played down Senate investigators' concerns and publicly claimed there had been no Russian effort of any significance on the Facebook platform. Internally, Facebook began tracing more advertisements and personal information, including pages, groups, and other Facebook activity back to Russia throughout the summer of 2017.

252. By August 2017, Facebook executives concluded the situation had become a "five-alarm fire." Zuckerberg and Sandberg reluctantly agreed to go public with some findings through a September 6, 2017 blog post, the day of the Company's quarterly Board meeting. Stamos drafted the blog post. However, Sandberg and Zuckerberg insisted that the release be less specific.

253. On September 6, 2017, Stamos informed the Board that Facebook had yet to regain control over its platform and that Russian agents were still harvesting

personal information and otherwise manipulating the Facebook platform. Stamos presented to Facebook's Audit Committee and went into more detail than Zuckerberg and Sandberg had planned. Bowles, the Facebook director who was then Chair of Facebook's Audit Committee, questioned how Facebook had allowed itself to become a tool for Russian interference, and demanded to know why it had taken so long to uncover the activity and why Facebook directors were only now being told.

254. The full Board met later on the day of September 6, 2017. Bowles "pelted questions" at Zuckerberg and Sandberg. Sandberg became visibly unsettled and apologized. Zuckerberg discussed technical fixes. Later that day, Facebook released an abbreviated version of Stamos's blog post, that said little about Russian activity on the Facebook platform.

255. After the September 6, 2017 Board and Audit Committee meetings, Sandberg reportedly became irate, regarding the fact that Stamos dutifully reported his findings to the Board as a "betrayal." She yelled at Stamos: "[y]ou threw us under the bus!"

256. Zuckerberg and Sandberg tried to handle manipulation of the Facebook platform in a now-familiar manner—by ignoring warning signs and trying to conceal them from public view, and apparently, the view of the Board.

257. Stamos, who reported directly to Facebook's general counsel, proposed that he begin reporting directly to the Board. Facebook executives rejected that proposal and instead reassigned Stamos's team, splitting the security team between its product and infrastructure teams and gutting Stamos's job responsibilities. As a result, Stamos's team of 120 people at Facebook was reduced to three, even as Facebook convinced Stamos to stay on until August because other Facebook executives thought his departure would "look bad."

258. Stamos's departure was also the result of wider internal tension between legal and policy teams at the Company versus Stamos's security team. The security team generally favored more disclosure about how the Facebook platform was being misused and manipulated, but legal and policy teams prioritized business imperatives.

259. Commenting on the internal conflict and Stamos's departure, Tavis McGinn, a Facebook employee who was recruited to head "executive reputation efforts," stated that, "Facebook cares so much about its image that the executives don't want to come out and tell the whole truth when things go wrong. But if they don't, it damages their image."

b. Sandy Parakilas Raises Red Flags And Is Ignored

260. Mere days later, on March 21, 2018, *Bloomberg News* reported that another Facebook executive, Sandy Parakilas, told a U.K. parliament committee

investigating Facebook that the Company ignored his concerns about lax data protection policies.

261. Parakilas stated that at the time he brought up the concerns, in 2011 or 2012, "My concerns were that all of the data that left Facebook servers to developers could not be monitored by Facebook," and that Facebook could have prevented Cambridge Analytica from happening. Paraklias' concern also "was that they'd allowed people to get all this data on people who hadn't really authorized it, and it was personally identifiable data."

262. Parakilas specifically informed senior Facebook executives that Facebook had allowed unknown, unvetted apps to "scrape" Facebook users' nonpublic information, including personally identifiable information, without users' express consent, thereby violating users' reasonable expectations of privacy regarding the information shared through their password-protected accounts.[81] Parakilas further warned that Facebook was failing to adequately vet the ever-growing number of app developers working off Facebook's Graph API V1 as the

[81] British Parliament House of Commons, Digital, Culture, Media and Sport Committee, *Oral Evidence: Fake News*, Testimony of S. Parakilas (March 21, 2018) (hereinafter "Parakilas Tr."), at Q1191-94, *available at*: http://data.parliament.uk/WrittenEvidence/CommitteeEvidence.svc/EvidenceDocument/Digital,%20Culture,%20Media%20and%20Sport/Disinformation%20and%20%E2%80%98fake%20news%E2%80%99/Oral/80809.html.

current process allowed "[a]nyone [to] create a Facebook app—there is no background check."[82] Parakilas pointed out that of the top 100,000 Facebook apps 60 percent, or 60,000 apps, failed to provide a privacy policy to Facebook's users.[83]

263. The following year, in 2012, Parakilas explicitly told senior managers that developers had collected and exploited the private information of hundreds of millions of Facebook users.

264. Parakilas again explained that there were no controls over the data these apps accessed: "[o]nce the data passed from Facebook servers to the developer, Facebook lost insight into what was being done with the data and lost control over the data . . . [and] Facebook had very few ways of either discovery abuse once data had been passed or enforcing abuse once it was discovered."[84, 85]

---

[82] *Id*. at Q1213.

[83] 643 Summaries, *supra* note 5, at 412 (quoting FB-00332289).

[84] Parakilas Tr., *supra* note 81, at Q1188.

[85] Parakilas' statements rang true years later, as noted by Wylie and counsel for Facebook. *See* Wylie Tr., *supra* note 58, at Q1341 (testifying, "You had all kinds of people having access to the data. Staff at Palantir had access to the data; all kinds of people had access to the data."); *see also* Paul Chadwick, How Many People Had Their Data Harvested By Cambridge Analytica?, The Guardian (Apr. 16, 2018) (admitting that "[w]e do not know precisely what data Dr. Kogan and GSR shared with Cambridge Analytica and other third parties or exactly how many people were impacted"), *available at*: https://www.theguardian.com/commentisfree/2018/apr/16/how-many-people-data-cambridge-analytica-facebook.

265. Parakilas further expressed his concern that Facebook:

> had built this platform that would allow people to get all of this data on people who had not really explicitly authorized—and it was personally identifiable data—it had your name in some cases and your email address in cases, and in some cases it could include your private messages. It was really personal data, and [Facebook] basically allowed that to leave Facebook's servers intentionally, and then there were not any controls once the data had left to ensure that it was being used in an appropriate way.[86]

266. Then, in a detailed presentation to "senior executives in charge of Facebook Platform and people in charge of privacy," Parakilas pinpointed areas where the Company was exposed, and user data was at risk. Parakilas's presentation provided the senior executives with "a map of the various data vulnerabilities of the Facebook platform," which "included lists of bad actors and potential bad actors," and "some of the things these people could be doing and [] what's at risk."[87] Parakilas also explained to senior management his concern that "Facebook had very few ways of discovering abuse once data had been passed or enforcing its policies once abuse was discovered."[88]

267. Parakilas recommended Facebook address these concerns by improving monitoring and enforcement of third-party app developers.[89] Parakilas

---

[86] Parakilas Tr., *supra* note 81, at Q1206.

[87] *Id.* at Q1192.

[88] *Id.* at Q1188.

[89] *Id.* at Q1194.

specifically "asked for more audits of developers and a more aggressive enforcement regime."[90] He explained that without routine audits, Facebook's data protection policies could be breached without the Company's knowledge.[91] But the Company, under the control of Director Defendants and Defendant Papamilitiadis, never undertook a serious effort to address Parakilas's concerns, despite the obligations made incumbent upon them by the 2012 Consent Order.

268. The Individual Defendants' response to Parakilas' flag-waving was to bury their heads in the sand and heedlessly proceed with their illegal business plans. According to Parakilas, executives at Facebook "did not want to [perform routine audits],"[92] and proactively discouraged "audit[ing] developers directly and see[ing] what's going on with the data," because Facebook believed it "was in a stronger legal position if it didn't know about the abuse that was happening."[93] For instance, in response to Parakilas proposal of "a deeper audit of developers' use of Facebook's

---

[90] *Id.* at Q1225.

[91] *Id.* at Q1192, Q1187 (explaining his primary responsibilities were not related to audits but rather concerned "policy and compliance for Facebook apps and data protection").

[92] *Id.* at Q1226.

[93] Paul Lewis, *'Utterly Horrifying': Ex-Facebook Insider Says Covert Data Harvesting was Routine*, THE GUARDIAN (Mar. 18, 2020), *available at*: https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas.

data, one executive asked [], '*Do you really want to see what you'll find?*'"[94] And even when Parakilas reported specific incidents of developer abuse to senior executives, those executes showed no interest and typically reacted by "try[ing] to put any negative press coverage to bed as quickly as possible, with no sincere efforts to put safeguards in place or to identify and stop abusive developers."[95]

269. In retrospect, Parakilas noted that throughout his 16 months as Facebook's Operations Manager, he could not recall "a single physical audit of a developer's storage."[96] He also recalled that policy enforcement lawsuits and bans initiated by Facebook were "quite rare."[97] Rather, the "main enforcement mechanism" for developers who improperly accessed user data was that Facebook would "call them and yell at them"—and Facebook only took that meagre step after someone outside the Company complained.[98] These responses left Parakilas with

---

[94] Sandy Parakilas, *We Can't Trust Facebook to Regulate Itself*, N.Y. TIMES (Nov. 19, 2017) *available at*: https://www.nytimes.com/2017/11/19/opinion/facebook-regulation-incentive.html (emphasis added).

[95] *Id*.

[96] Parakilas Tr., *supra* note 81, at Q1188.

[97] *Id*.

[98] *See id.*; *see also* P. Lewis, *supra* note 93; D. Seetharaman & K. Grind, *Facebook's Lax Data Policies Led to Cambridge Analytica Crisis*, THE WALL ST. J. (Mar. 20, 2018), *available at*: https://www.wsj.com/articles/facebooks-lax-data-policies-led-to-cambridge-analytica-crisis-1521590720.

the impression that the Board and Facebook's officers had turned a blind eye to avoid finding out that truth.[99] According to him***, it was "known and understood" by senior management "that there was risk with respect to the way that Facebook Platform was handling data"***[100] ***but "it was a risk that they were willing to take."***[101]

c. Jan Koum Leaves Facebook Because Of Its Failures To Safeguard User Privacy

270. On April 30, 2018, former Facebook director Koum announced his departure from the Company via a post on the Facebook platform. Koum was a founder of the messaging app "WhatsApp," which he sold to Facebook in 2014. Koum is known for his deep concern regarding user privacy, as he grew up in the Soviet Union during the 1980s—when the Russian state conducted pervasive surveillance on its populace.

271. According to an anonymous Facebook executive, as reported in *The New York Times* on April 30, 2018, Koum had grown increasingly concerned about Facebook's disregard for user privacy and lack of control over personal user information in recent years. Koum was "perturbed by the amount of information

[99] Parakilas Tr., *supra* note 81, at Q1223.

[100] *Id.*at Q1196.

[101] *Id.* at Q1215.

that Facebook collected on people and had wanted stronger protections for that data."

272. Koum's departure came mere weeks after Facebook's sale of its users' personal information allowed Cambridge Analytica to harvest the information of at least 87 million Facebook users. Koum had reportedly become "tired of fighting back against ***pressure from the board*** . . . to allow advertisements on WhatsApp" and Facebook's data and privacy policies. ***Koum left because "he felt the [C]ompany's board simply paid lip service to privacy and security concerns he raised*** . . . ." Concurrently, Brian Acton, who co-founded WhatsApp with Koum, wrote that it was time to delete Facebook after the Cambridge Analytica revelations.

273. Koum also observed that Facebook had stripped privacy protections from WhatsApp since its acquisition of the company. In 2016, after Facebook had acquired WhatsApp, the app revealed it would start disclosing the phone numbers and analytics data of its users to Facebook. One year later, the European Commission fined Facebook approximately $122 million for misleading it by falsely claiming that it was impossible to combine user data collected by Facebook and WhatsApp.

d. Desmond-Hellmann, Chenault And Zients Leave Because The Board Ignores Their Feedback And Concerns

274. On October 30, 2019, Facebook announced that Susan Desmond-Hellmann, who had served as Facebook's lead independent director since June 2015, was leaving the Board. Despite her stated reasons for leaving, *The Wall Street Journal* reported that "Ms. Desmond-Hellmann conveyed to some people that she left Facebook in part because she didn't think the board was operating properly, and that Facebook management wasn't considering board feedback, a person familiar with the matter said."

275. In March 2020, Chenault and Zients both announced they were leaving the Board. *The Wall Street Journal* reported that Chenault had grown disillusioned since he joined the Board in February 2018. Chenault's suggestion to create an outside advisory group that would study Facebook's problems and deliver reports to the board directly, circumventing Zuckerberg, was "opposed" by others on the Board and "the idea sank." Chenault was frustrated with Zuckerberg that Facebook was not taking more responsibility for its role in elections.

276. *The Wall Street Journal* also reported that Zients was generally aligned with Chenault. Chenault and Zients had spearheaded a group of independent directors who last year started holding separate meetings in 2019. Yet they reportedly, and justifiably, were worried their perspectives were being dismissed as Facebook faced regulatory woes. Chenault and Zients were also both unhappy for months with executive management, how the company handled misinformation, and that their stated concerns to the Board received only silent treatment.

277. In addition to defections from senior management and Board members owing to fundamental concerns about the Company's ethos and direction, morale among rank-and-file employees who remained with Facebook plummeted in the wake of the Cambridge Analytica scandal. According to an internal Facebook employee survey in late 2018, 70% of employees were proud to work at Facebook—down from 87% just one year earlier. The same survey showed near 20-point drops in employees' optimism about Facebook's future, and in their belief that Facebook was making the world better, with just barely more than half of employees holding those beliefs in October 2018. Facebook also became much less attractive to job seekers, with job acceptance rates among software engineer candidates falling from nearly 90% in late 2016 to almost 50% in early 2019, and acceptance rates among new graduates falling from 85% in 2017–18 to between 35%–55% as of December 2019.

M. Facebook Incurs Historic Fines As A Result Of Its Misconduct

1. *The UK Information Commissioner's Office Issues The Maximum Possible Penalty Due To Facebook's Lack Of Transparency And Harvesting Of User Data*

278. On July 11, 2018, the UK Information Commissioner's Office (previously defined as the "ICO") imposed the maximum penalty possible at the time—£500,000—on Facebook under existing UK data protection law available before the EU General Data Protection Regulation ("GDPR") had come into effect. The ICO made the following statement regarding the reasoning for the imposition of this fine:

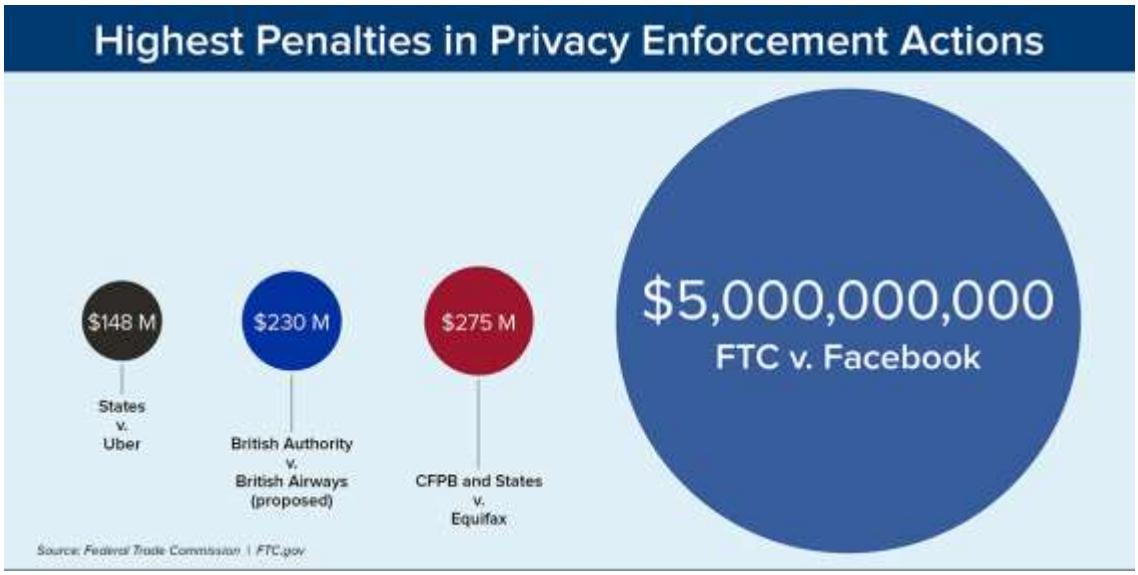
> ***We fined Facebook because it allowed applications and application developers to harvest the personal information of its customers who had not given their informed consent—think of friends, and friends of friends***—and then Facebook failed to keep the information safe. . . . It is not a case of no harm, no foul. Companies are responsible for proactively protecting personal information and that's been the case in the UK for thirty years. . . . Facebook broke data protection law, and it is disingenuous for Facebook to compare that to email forwarding, because that is not what it is about; it is about the release of users' profile information without their knowledge and consent.

279. Elizabeth Denham, the ICO's UK Information Commissioner ("Denham"), stated that the ICO "found [Facebook's] business practices and the way applications interact with data on the platform to have contravened data protection law. That is a big statement and a big finding." Denham also stated that, based upon her interactions with Facebook executives, Facebook did not view prior rulings from

federal privacy commissioners in Canada and Ireland to be anything more than advice. Finally, Denham stated, "***unless there is a legal order compelling a change in their business model and their practice, they are not going to do it***."

2. *The FTC Fines Facebook A Record $5 Billion For Its Privacy Breaches*

280. On July 24, 2019, the FTC, working with the DOJ's Civil Division Consumer Protection Branch, announced that it had concluded its investigation into Facebook's privacy practices. The FTC concluded that Facebook violated the 2012 Consent Order by deceiving users about their ability to control the privacy of their personal information. As a result of Facebook's violation of the 2012 Consent Order, Facebook agreed to institute reforms and paid a record-breaking ***$5 billion penalty***, a penalty 20 times greater than the largest privacy or data security penalty imposed worldwide, and one of the largest penalties ever assessed by the U.S. government for any violation:



281. In announcing the fine, FTC Chairman, Joe Simons, stated:

> ***Despite repeated promises to its billions of users worldwide that they could control how their personal information is shared, Facebook undermined consumers' choices. The magnitude of the $5 billion penalty and sweeping conduct relief are unprecedented in the history of the FTC. The relief is designed not only to punish future violations but, more importantly, to change Facebook's entire privacy culture*** to decrease the likelihood of continued violations. The Commission takes consumer privacy seriously, and will enforce FTC orders to the fullest extent of the law.

282. In announcing the Settlement Order, the FTC also alleged that Facebook had violated the 2012 Consent Order. Specifically, the FTC made the following statements regarding Facebook's violations of the 2012 Consent Order:

> ***3. Alleged Violations Of The 2012 Consent Order***
>
> The settlement stems from alleged violations of the FTC's 2012 [Consent Order] with Facebook. Among other things, the [Consent Order] prohibited Facebook from making misrepresentations about the privacy or security of consumers' personal information, and the extent to which it shares personal information, such as names and dates of birth, with third parties. It also

required Facebook to maintain a reasonable privacy program that safeguards the privacy and confidentiality of user information.

The FTC alleges that Facebook violated the [Consent Order] by deceiving its users when the company shared the data of users' Facebook friends with third-party app developers, even when those friends had set more restrictive privacy settings.

In May 2012, Facebook added a disclosure to its central "Privacy Settings" page that information shared with a user's Facebook friends could also be shared with the apps used by those friends. The FTC alleges that four months after the [Consent Order] was finalized in August 2012, Facebook removed this disclosure from the central "Privacy Settings" page, even though it was still sharing data from an app user's Facebook friends with third-party developers.

Additionally, ***Facebook launched various services such as "Privacy Shortcuts" in late 2012 and "Privacy Checkup" in 2014 that claimed to help users better manage their privacy settings. These services, however, allegedly failed to disclose that even when users chose the most restrictive sharing settings, Facebook could still share user information with the apps of the user's Facebook friends—unless they also went to the "Apps Settings Page" and opted out of such sharing***. The FTC alleges the company did not disclose anywhere on the Privacy Settings page or the "About" section of the profile page that Facebook could still share information with third-party developers on the Facebook platform about an app users Facebook friends.

Facebook announced in April 2014 that it would stop allowing third-party developers to collect data about the friends of app users ("affected friend data"). Despite this promise, the company separately told developers that they could collect this data until April 2015 if they already had an existing app on the platform. The FTC alleges that Facebook waited until at least June 2018 to stop sharing user information with third-party apps used by their Facebook friends.

In addition, the complaint alleges that Facebook improperly policed app developers on its platform. ***The FTC alleges that, as a general practice, Facebook did not screen the developers or their apps before granting them access to vast amounts of user data. Instead, Facebook allegedly only required developers to agree to Facebook's policies and terms when they***

> ***registered their app with the Facebook Platform***. The company claimed to rely on administering consequences for policy violations that subsequently came to its attention after developers had already received data about Facebook users. The complaint alleges, however, that ***Facebook did not enforce such policies consistently and often based enforcement of its policies on whether Facebook benefited financially from its arrangements with the developer, and that this practice violated the [Consent Order]'s requirement to maintain a reasonable privacy program***.
>
> The FTC also alleges that Facebook misrepresented users' ability to control the use of facial recognition technology with their accounts. According to the complaint, Facebook's data policy, updated in April 2018, was deceptive to tens of millions of users who have Facebook's facial recognition setting called "Tag Suggestions" because that setting was turned on by default, and the updated data policy suggested that users would need to opt-in to having facial recognition enabled for their accounts.
>
> In addition to these violations of its [Consent Order], the FTC alleges that Facebook violated the FTC Act's prohibition against deceptive practices when it told users it would collect their phone numbers to enable a security feature, but did not disclose that it also used those numbers for advertising purposes.

283. In addition, the DOJ, working with the FTC, filed its own complaint against Facebook (attached hereto as Exhibit C), alleging that the Company repeatedly used deceptive disclosures and settings to undermine users' privacy preferences, also in violation of the 2012 Consent Order. The DOJ alleged that, beginning as early as 2010 and continuing through at least June 2018, that Facebook subverted users' privacy choices to serve its own business interests, by, *inter alia*: (i) allowing Platform Applications to see all of the personal user information of a given user's "friends"; (ii) removing opt-out disclaimers alerting Facebook users that their settings would allow Platform Applications to maintain access to personal user

information; (iii) entering into whitelisting agreements with certain partners through at least June 2018; (iv) failing to maintain a reasonable privacy program that safeguarded the privacy, confidentiality, and integrity of user information, as required by part iv of the 2012 Consent Order; (v) failing to vet third parties and their Platform Applications before granting them access to personal user information; (vi) failing to enforce Facebook's own existing policies, terms, and conditions, and instead selectively enforcing the agreements depending on financial benefit to Facebook; and (vii) inducing users to provide their phone numbers under the guise of a two-factor security authentication measure, when Facebook actually shared users' phone numbers for its own financial benefit in advertising.

284. These tactics also allowed Facebook to share users' personal information with third-party Platform Applications that were downloaded by the user's Facebook "friends." The FTC additionally alleged that many users were unaware that Facebook was sharing such information, and therefore did not take the steps needed to opt-out of sharing.

285. As the DOJ's complaint notes, "***Facebook knew or should have known that its conduct violated the [Consent] Order because it was engaging in the very same conduct that the Commission alleged was deceptive in Count One of the original Complaint that led to the [Consent] Order.***"

286. Facebook and the FTC also stipulated to an order on July 24, 2019 imposing additional restrictions on Facebook's business operations for an additional 20 years (the "Settlement Order). The Settlement Order became effective on July 24, 2019, the day it was posted to the FTC's website, and imposed the following further conditions on the Company, over and above the requirements of the 2012 Consent Order, for a period of twenty years, where a time period is applicable:

i. Prohibition Against Misrepresentations. Facebook was ordered not to misrepresent, in any manner, the extent to which it maintains the privacy of any personal user information, including: (a) its collection, use, or disclosure; (b) the extent to which a consumer can control the privacy of his or her personal user information maintained by Facebook and the steps a consumer must take to implement such controls; (c) the extent to which Facebook makes or has made personal user information accessible to third parties; (d) the steps Facebook takes or has taken to verify the privacy or security protections that any third party provides; (e) the extent to which Facebook makes or has made personal user information accessible to any third party following the deletion or termination of a Facebook user's account; and (f) the extent to which Facebook is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy or

security program sponsored by a government or self-regulatory or standard-setting organization.

ii. Changes to Sharing of Nonpublic User Information. Facebook was further ordered, prior to sharing any personal user information materially exceeding the restrictions imposed by a user's privacy settings, to: (a) clearly and conspicuously disclose in a standalone notice the categories of information to be disclosed to third parties, the identity of the third parties, and that such sharing exceeds the restrictions imposed by the privacy settings of the user; and (b) obtain the user's affirmative express consent.

iii. Deletion of Information. Facebook was ordered to ensure that access to personal user information would be eliminated as to any third party within thirty days from the time a Facebook user deleted such information or deleted or terminated his or her account. Facebook was further ordered to ensure that it implemented procedures to delete personal user information from Facebook servers, or de-identified such information such that it would no longer be associated with the user's account or device, within 120 days from the time that the user deleted the information or his or her account.

iv. Limitations on the Use or Sharing of Telephone Numbers Specifically Provided to Enable Account Security Features. Facebook was required to refrain from using, for the purpose of serving advertisements or

for sharing with third parties, any telephone number that Facebook identified as connected to a specific user when that user gave such information to Facebook for the purpose of maintaining safeguards to protect against unauthorized access (*i.e.*, two-factor authentication, password recovery, and login alerts).

v. Covered Information and User Password Security. Facebook was further ordered to implement and maintain a comprehensive information security program designed to protect the security of personal user information. Facebook was ordered to maintain safeguards appropriate to its size and complexity, the nature and scope of Facebook's activities, and the sensitivity of the personal user information, with further specific guidelines for user passwords.

vi. Facial Recognition Templates. Facebook was further ordered not to create any new facial recognition templates, and to delete any existing facial recognition templates within 90 days from the effective date of the Settlement Order, unless Facebook clearly and conspicuously discloses how Facebook plans to use the facial recognition template and obtains the user's affirmative express consent.

vii. Mandated Privacy Program. Facebook was further required to establish and implement, and thereafter maintain, a comprehensive privacy

program to protect the privacy, confidentiality, and integrity of personal user information collected, used or shared by Facebook. The privacy program included specific record keeping, compliance officer, internal controls, and risk reviews be periodically conducted, alongside the imposition of additional safeguards and privacy training. Facebook was required to establish this program within 180 days of the effective date of the Settlement Order.

viii. Independent Privacy Program Assessments. Facebook was further required to conduct independent biennial assessments of its privacy program. Facebook was required to provide the privacy assessments to the appropriate officials at the FTC for further review.

ix. Covered Incident Reports. Facebook was further required to submit a report to the FTC within 30 days any time information about 500 Facebook users or more was likely to have been accessed, collected, used, or shared by a third party in violation of Facebook's terms of service.

x. Mandated Independent Privacy Committee and Other Governance Matters. Facebook was further required to create and maintain an Independent Privacy Committee within 120 days of the entry of the Order. Facebook was further required to take further efforts to ensure the independence of the Company's Board of Directors.

xi. Certifications. Facebook was further required to certify, at the end of each full fiscal quarter, that Facebook was in compliance with certain terms of the Settlement Order.

xii. Order Acknowledgments. Facebook was further required to acknowledge receipt of the Settlement Order, and provide a copy of the Settlement Order to all principals, officers, directors, and further employees with managerial responsibilities relating to the Settlement Order, for a period of five years after entry of the Settlement Order.

xiii. Compliance Reporting. Facebook was further required to make timely submissions to the FTC of compliance reports with points of contact for the FTC to communicate with Facebook and information ensuring its compliance with the Settlement Order.

xiv. Recordkeeping. The Settlement Order further required Facebook to keep records regarding (a) all widely-disseminated statements the Company made regarding Facebook's privacy, security and confidentiality measures taken with respect to personal user information; (b) records sufficient to identify all types of personal user information Facebook provides or makes available to third parties subject to its mandated privacy program in subsection vii.; (c) all consumer complaints directed at Facebook or forwarded to Facebook by a third party relating to conduct prohibited by

the Settlement Order and any responses to such complaints; (d) any documents prepared by or on behalf of Facebook that contradict, qualify, or call into question Facebook's compliance with the Settlement Order; and (e) each materially different document relating to Facebook's attempt to obtain the consent of users as mandated in subsection ii, along with documents and information sufficient to show each user's consent, and documents sufficient to demonstrate, on an aggregate basis, the number of users for whom each such privacy setting was in effect at any time Facebook has attempted to obtain, and/or was required to obtain, such consent; (f) all materials relied upon to prepare the assessments required under the 2012 Consent Order; and (g) all records necessary to demonstrate full compliance with each part of the 2012 Consent Order.

xv. Compliance Monitoring. Facebook was further required to submit additional compliance reports or other requested information; appear for depositions; and produce documents for inspection and copying, within 14 days of receipt of a written request from the FTC.

287. Facebook waived all rights to appeal or otherwise challenge or contest the validity of the Settlement Order. On April 24, 2020, the U.S. District Court for the District of Columbia approved the settlement.

4. *The SEC Fines Facebook For Misleading Shareholders About The Risk Of Misuse Of User Data*

288. Facebook also incurred damages due to its materially false and misleading disclosures regarding its wide-ranging privacy violations. On July 24, 2019, the SEC announced through a press release that it had charged Facebook for making misleading disclosures regarding risks with Facebook user data. Specifically, the SEC stated that, "[f]or more than two years, Facebook's public disclosures presented the risk of misuse of user data as merely hypothetical, when Facebook knew that a third-party developer, Cambridge Analytica, had actually misused Facebook user data."[102]

289. According to the SEC's complaint, in 2015, Facebook discovered that Cambridge Analytica had obtained vast amounts of personal user information, including names, genders, locations, birthdays, interests, and more, which it used in its political advertising activities. The SEC's complaint further alleged that Facebook did not correct existing disclosures regarding data sharing for more than two years, but instead continued to tell investors that "our users' data may be improperly accessed, used or disclosed." (emphasis in SEC press release).

[102] SEC Complaint, *supra* note 7, at ¶ 1.

290. The SEC also alleged that Facebook reinforced the false impression that its users' data had not been shared for nefarious purposes when it told news reporters who were investigating Cambridge Analytica's use of Facebook personal user information that it had discovered no evidence of wrongdoing. Facebook only disclosed the incident in March 2018, after journalists had already released the information to the public.

291. The SEC further alleged that Facebook had no specific policies or procedures in place to ensure that the Company made accurate disclosures in Facebook's public filings. The SEC chastised Facebook for failing to have procedures in place to make accurate disclosures about material business risks.

292. In addition, the SEC found Facebook's public statements that Facebook merely faced a hypothetical risk of third parties misusing user data when Facebook knew that such misuse was in fact occurring. Specifically, the SEC alleged that "[s]ince the time of its initial public offering in 2012, Facebook has warned investors about the potential for misuse of its users' data by developers and the possible consequent financial effect on the Company's business."[103]

[103] SEC Complaint, *supra* note 7, at ¶ 37.

293. In Facebook's Form 10-Q filed on October 30, 2014, signed by Non-Party Executives Wehner and Athwal, Facebook cautioned that "Improper access to or disclosure of user information, or violation of our terms of service or policies, could harm our reputation and adversely affect our business."[104] In the same Form 10-Q, Facebook advised that if developers "fail to comply with our terms and policies . . . our users' data may be improperly accessed or disclosed."[105] The Form 10-Q acknowledged that such circumstances "could have a material and adverse effect on our business, reputation, or financial results."[106]

294. In Facebook's 2015 Annual Report on Form 10-K filed with the SEC on January 28, 2016 ("2015 Form 10-K"), only weeks after the Company had confirmed that Kogan had improperly transferred personality scores derived from Facebook user data to Cambridge Analytica in violation of its Platform Policy, Facebook stated that, "[a]ny 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

[104] SEC Complaint, *supra* note 7, at ¶ 37.

[105] *Id*.

[106] *Id*.

competitive position."[107] The 2015 Form 10-K further asserted 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."[108]

295. In the Form 10-K for the fiscal years ended December 31, 2015, December 31, 2016, and December 31, 2017, and six quarterly reports on Form 10-Q for each fiscal quarter in 2016 and 2017, Facebook included a risk factor that "misleadingly suggested that the Company faced merely the risk of such misuse and any harm to its business that might flow from such an incident. This hypothetical phrasing, repeated in each of its periodic filings during the Relevant Period, created the false impression that Facebook had not suffered a significant episode of misuse of user data by a developer."[109]

296. And the Risk Factor disclosures were incorporated by reference into Facebook's registration statements on Forms S-8 filed with the SEC on May 21, 2012 and February 1, 2013.[110] These statements registered sales of shares of Facebook common stock under the Company's employee and officer equity

[107] *Id*. at ¶ 38.

[108] *Id*.

[109] *See e.g., id* at ¶ 39.

[110] *Id*. at ¶ 45.

incentive plans, and incorporated future periodic reports filed with the SEC, including those filed during the Relevant Period.[111]

297. Yet, according to the SEC, many of these statements were known to be materially false and misleading at the time it was uttered. Specifically,

- "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 [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";[112]

- "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;"[113] and

- "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."[114]

---

[111] *Id*. Defendants Zuckerberg, Andreessen, Bowles, Hastings and Thiel signed the May 21, 2012 Form S-8, and Defendants Zuckerberg, Andreessen, Bowles, Hastings, Sandberg and Thiel signed the February 1, 2013 Form S-8.

[112] *Id*. at ¶ 6.

[113] *Id*. at ¶ 39.

[114] *Id*. at ¶ 44.

298. Defendants Zuckerberg, Andreessen, Bowles, Desmond-Hellmann, Hastings, Koum, Sandberg, and Thiel signed the 2015-2017 Form 10-Ks referenced above. Defendant Zuckerberg signed the Form 10-Q for the period ended March 31, 2017.

299. In addition to finding the Company's public statements were materially false and misleading, the SEC charged that Facebook's processes and procedures were inadequate. Specifically, the SEC alleged, *inter alia*, that:

- "The Company's processes and procedures around the drafting of its periodic reports on Forms 10-K and 10-Q, including but not limited to its Risk Factor disclosures, failed to bring [Kogan's] sale of data from tens of millions of Facebook users to Cambridge [Analytica] to the attention of the individuals with primary responsibility for drafting and approving those reports. Although protecting user data is critical to Facebook's business, and Facebook had identified the potential for improper access to and misuse of user data as a significant risk, Facebook did not maintain disclosure controls and procedures designed to analyze or assess incidents involving misuse of user data for potential disclosure in the [C]ompany's periodic filings."[115]

- "During the relevant period, Facebook identified trends and events for possible disclosure through a series of quarterly meetings to prepare for the [C]ompany's earnings announcements. This process relied on the employees and managers who attended these meetings to identify issues that might need to be disclosed. Although several employees in Facebook's legal, policy, and communications groups who attended these meetings during the relevant period were aware

[115] SEC Complaint, *supra* note 7, at ¶ 40.

of [Kogan's] improper transfer of data to Cambridge [Analytica], that incident was never discussed. Facebook also did not share information regarding the incident with its independent auditors and outside disclosure counsel in order to assess the [C]ompany's disclosure obligations."[116]; and

- "Facebook had no specific mechanism to summarize or report violations of its Platform Policy to employees responsible for ensuring the accuracy of Facebook's filings with the [SEC]. For example, the Facebook employees responsible for monitoring violations of the [C]ompany's Platform Policy were not provided with the draft disclosures pertaining to the misuse of user data. As a result, Facebook senior management and relevant legal staff did not assess the scope, business impact, or legal implications of [Kogan's] improper transfer of data to Cambridge [Analytica], including whether or how it should have been disclosed in Facebook's public filings or whether it rendered, or would render, any statements made by the [C]ompany in its public filings misleading."[117]

300. Facebook paid a $100 million fine to settle the SEC's charges.

5. *Individual Defendants' User Privacy Violations Caused Numerous Other State And Foreign Regulatory Actions*

301. In February 2016, a German court fined Facebook €100,000 for failing to comply with a 2012 order related to its policies on data usage.[118]

---

[116] *Id.* at ¶ 41.

[117] *Id.* at ¶¶ 42–43.

[118] Reuters Staff, *German Court Fines Facebook $109,000 in Dispute Over IP License Clause*, REUTERS (Feb. 29, 2016), *available at*: https://www.reuters.com/article/us-facebook-germany/german-court-fines-facebook-109000-in-dispute-over-ip-license-clause-idUSKCN0W21W4.

302. In May 2017, France's privacy regulator fined Facebook €150,000 for misusing user data for targeted advertising and illegally tracking what users do on and off the site via cookies.[119]

303. In May 2017, the EU's antitrust regulator fined Facebook €110,000,000 after it changed its privacy policy in contradiction to the pledge it made to segregate WhatsApp data from other Facebook platforms to secure approval of the merger of WhatsApp and Facebook in 2014.[120]

304. In September 2017, the same EU regulator fined Facebook €1.2 million for failing to obtain proper consent to collect and store sensitive personal data, including information on gender, religion, and internet use.[121]

---

[119] Samuel Gibbs, *Facebook Facing Privacy Actions Across Europe as France Fines Firm €150k*, THE GUARDIAN (May 16, 2017), *available at*: https://www.theguardian.com/technology/2017/may/16/facebook-facing-privacy-actions-across-europe-as-france-fines-firm-150k.

[120] Reuters Staff, *EU Fines Facebook 110 Million Euros Over WhatsApp Deal*, REUTERS (May 18, 2017), *available at*: https://www.reuters.com/article/us-eu-facebook-antitrust/eu-fines-facebook-110-million-euros-over-whatsapp-deal-idUSKCN18E0LA.

[121] Natasha Lomas, *Facebook Fined €1.2 Million for Privacy Violations in Spain*, TECHCRUNCH (Sept. 11, 2017), *available at*: https://techcrunch.com/2017/09/11/facebook-fined-e1-2m-for-privacy-violations-in-spain/.

305. In March 2018, Spain's data protection watchdog fined Facebook and WhatsApp a total of €600,000 for processing user data without people's consent.[122]

306. On March 26, 2018, Pennsylvania Attorney General, Josh Shapiro ("PA AG"), backed by a coalition of 37 other State Attorneys General sent a letter to Defendant Zuckerberg demanding answers about the Company's business practices and privacy protections.[123] Attorney General Shapiro stated: "[b]usinesses like Facebook must comply with the law when it comes to how they use their customers' personal data . . . State Attorneys General have an important role to play in holding them accountable . . . ."[124]

307. On March 20, 2018, a committee in the British Parliament sent a letter to Zuckerberg asking him to appear before the panel to answer questions related to

---

[122] Michaela Ross, *Facebook, WhatsApp Fined by Spain for Failure to Obtain Consent*, BLOOMBERG LAW (Mar. 16, 2018), *available at*: https://news.bloomberglaw.com/ business-and-practice/facebook-whatsapp-fined-by-spain-for-failure-to-obtain-consent/.

[123] CBS News, *State Attorneys General Send Letter to Zuckerberg Over Data Scandal*, CBS NEWS (Mar. 26, 2018), *available at*: https://www.cbsnews.com/news/cambridge-analytica-state-attorneys-general-send-letter-to-facebook-ceo-mark-zuckerberg/.

[124] *Id.*

Cambridge Analytica.[125] "The committee has repeatedly asked Facebook about how companies acquire and hold on to user data from their site, and in particular about whether data had been taken without their consent," wrote Damian Collins, chairman of the British committee.[126] "Your officials' answers have consistently understated this risk and have been misleading to the committee."[127]

308. A few weeks later, the President of the EU Parliament also requested Zuckerberg appear to testify.[128]

309. On July 10, 2018, the ICO fined Facebook the highest allowable fine of £500,000 over breaches of the U.K. Data Protection Act in connection with the Cambridge Analytica scandal.[129] ICO found that Facebook contravened the law by "failing to safeguard people's information" and "failed to be transparent about how people's data was harvested by others" and for "lack of transparency and security

---

[125] Letter from Damiam Collins, Parliament Member of the U.K., to Mark Zuckerberg, (Mar. 20, 2018), *available at*: https://www.parliament.uk/globalassets/documents/commons-committees/culture-media-and-sport/180320-Chair-to-Mark-Zuckerberg-re-oral-evidence.pdf.

[126] *Id*

[127] *Id*.

[128] Tony Romm, *Facebook CEO Mark Zuckerberg Faces Another Request to Testify—in Europe*, THE WASH. POST (Apr. 12, 2018), *available at*: https://www.washington post.com/news/the-switch/wp/2018/04/12/facebook-ceo-mark-zuckerberg-faces-another-request-to-testify-in-europe/.

[129] U.K. Disinformation Report, *supra* note 4, at ¶ 115.

issues relating to the harvesting of data" in contravention of the Data Protection Act of 1998.[130] In particular, the ICO fined Facebook:

> because it allowed applications and application developers to harvest the personal information of its customers who had not given their informed consent—think of friends, and friends of friends—and then Facebook failed to keep the information safe . . . It is not a case of no harm, no foul. Companies are responsible for proactively protecting personal information and that's been the case in the UK for thirty years . . . Facebook broke data protection law, and it is disingenuous for Facebook to compare that to email forwarding, because that is not what it is about; it is about the release of users' profile information without their knowledge and consent.[131]

310. The UK Information Commissioner, Elizabeth Denham, told the Digital Committee that the ICO found that Facebook's "business practices and the way applications interact with data on the platform to have contravened data protection law. This is a big statement and a big finding."[132] Nevertheless, Denham

[130] *Id*.

[131] *Id*. at ¶ 57.

[132] *Id*. at ¶ 58.

believed that Facebook thought that the ICO's finding, or the ruling of the federal privacy commissioner in Canada was merely advice.[133]

311. In response to this fine, Erin Egan, Facebook's Chief Privacy Officer, stated: Facebook "should have done more to investigate claims about Cambridge Analytica and take action in 2015."[134]

312. The Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia have said that Facebook violated national and local laws in allowing third-parties access to private user information through "superficial and ineffective safeguards and consent mechanisms."[135] The Canadian regulators plan to take the company to a Canadian federal court.[136] The court, which focuses on regulatory issues and lawsuits against the government, may impose

---

[133] *Id.*

[134] Emma Woollacott, *Facebook Find $645,150 Over Cambridge Analytica Scandal—And is Told it's Getting off Lightly*, FORBES (Oct 25, 2018), *available at*: https://www.forbes.com/sites/emmawoollacott/2018/10/25/facebook-fined-645150-over-cambridge-analytica-scandal-and-is-told-its-getting-off-lightly/?sh=4936d99f2c34.

[135] Tiffany Hsu & Ian Auster, *Canada Says Facebook Broke Privacy Laws With 'Superficial' Safeguards*, N.Y. TIMES (Apr. 25, 2019), *available at*: https://www.nytimes.com/2019/04/25/technology/facebook-canada-privacy.html.

[136] *Id.*

fines.[137] The Canadian investigation began after the news broke regarding Cambridge Analytica.[138] The Canadian regulators believe that the unauthorized access by Cambridge Analytica could have been avoided or alleviated if Facebook had followed recommendations it issued in 2009 after a similar investigation by the Canadian Federal Privacy Commissioner.[139] Canadian officials said Facebook refused to allow audits of its privacy procedures.[140]

313. Daniel Therrien, privacy commissioner of Canada, has stated that "[t]he stark contradiction between Facebook's public promises to mend its ways on privacy and its refusal to address the serious problems we've identified—or even acknowledge that it broke the law—is extremely concerning."[141] British Columbia's Information and Privacy Commissioner, Michael McEvoy concurred, stating that "Facebook has spent more than a decade expressing contrition for its actions and

---

[137] Cecilia Kang & Adam Satariano, *Regulators Around the World are Circling Facebook*, N.Y. TIMES (Apr. 25, 2019), *available at*: https://www.nytimes.com/2019/04/25/technology/facebook-regulation-ftc-fine.html.

[138] *Id*.

[139] *Id*.

[140] Hsu & Auster, *supra* note 135.

[141] Natasha Lomas, *Facebook Broke Canadian Privacy Law, Joint Probe Finds*, TECHCRUNCH (Apr. 25, 2019), *available at*: https://techcrunch.com/2019/04/25/facebook-broke-canadian-privacy-law-joint-probe-finds/.

avowing its commitment to people's privacy. But when it comes to taking concrete actions needed to fix transgressions, they demonstrate disregard."[142]

314. Governments in Australia, India, New Zealand and Singapore have passed or are considering new restrictions on social media.[143]

315. The California Attorney General continues to investigate Facebook more than two years after opening its probe following the wake of the Cambridge Analytica scandal.[144] The probe was first revealed in November 2019 when the Attorney General sued Facebook in Superior Court in San Francisco, alleging the company failed to comply with two prior subpoenas and refused to search the e-mail records of Defendant Zuckerberg and Defendant Sandberg.[145] The Attorney General sent a third subpoena to Facebook in February 2020.[146] More recently, Facebook has begun to comply with the records and witnesses requests such that the California Attorney General petitioned the court to close the subpoena enforcement action.[147]

---

[142] Id.

[143] *Id.*

[144] Mike Swift, *Facebook Hit with Additional Subpoena in California Privacy Probe*, MLEX (Aug. 19, 2020) a*vailable at*: https://mlexmarketinsight.com/news-hub/editors-picks/area-of-expertise/data-privacy-and-security/facebook-hit-with-additional-subpoena-in-california-privacy-probe.

[145] *Id.*

[146] *Id.*

[147] *Id.*

316. Similarly, Facebook and the Massachusetts Attorney General have been embroiled in discovery fights concerning access to records sought by Attorney General Healey in connection with her probe of Facebook's data-sharing practices.[148] That dispute reached the Massachusetts Supreme Court, resulting in a March 24, 2021 opinion: *Attorney General v. Facebook, Inc.*, 164 N.E.3d 873 (Mass. 2021) (affirming in part the trial court's decision on issues of attorney-client privilege, and reversing and remanding on work product issues).[149]

317. Facebook is also currently in the midst of discovery, following the filing of a lawsuit by the Washington D.C. Attorney General for allegedly "fail[ing] to protect the privacy of its users and deceived them about who had access to their data and how it was used."[150]

318. In Ireland, home to Facebook's European headquarters, the company is facing several investigations into whether it is complying with European data

---

[148] *Id.*

[149] *Id.*

[150] Press Release, *AG Racine Sues Facebook for Failing to Protect Millions of Users' Data*, OFFICE OF THE A.G. FOR THE D.C. (Dec. 19, 2018), *available at*: https://oag.dc.gov/release/ag-racine-sues-facebook-failing-protect-millions.

protection laws.[151] The Irish Data Protection Commission recently started a fresh inquiry into Facebook's exposing of user passwords.[152] Under European privacy law, Facebook could be fined up to 4 percent of global revenue, or $2.23 billion.[153]

N. Facebook Fails To Reform Its Illicit Business Practices

319. Facebook's failure to protect its users' personal information continued well into 2019, and it is still unclear whether Facebook has or will bring itself into compliance with the 2012 Consent Order and the new FTC settlement approved on April 24, 2020.

320. On July 26, 2019, *The Hill* reported that an independent audit conducted by PricewaterhouseCoopers LLP ("PwC") between 2017 and February 2019 found that ***Facebook did not effectively implement privacy safeguards that were required under the 2012 Consent Order***, according to documents it had obtained. PwC found that Facebook, among other things, did not have controls in place to properly authorize to the sharing of personal user information amongst the developers of its

---

[151] Jack Power, *Data Protection Commissioner to Investigate Facebook Over Password Storage*, THE IRISH TIMES (Apr. 25, 2019), *available at*: https://www.irishtimes.com/business/technology/data-protection-commissioner-to-investigate-facebook-over-password-storage-1.3871585.

[152] *Id*.

[153] Sam Schechner, *EU Nears Decisions in Facebook Privacy Cases*, WALL ST. J. (Aug. 12, 2019), *available at*: https://www.wsj.com/articles/eu-nears-decisions-in-facebook-privacy-cases-11565602202.

Platform Applications and had not implemented an appropriate procedure to adequately prevent, detect and respond to privacy breaches. As the PwC report stated:

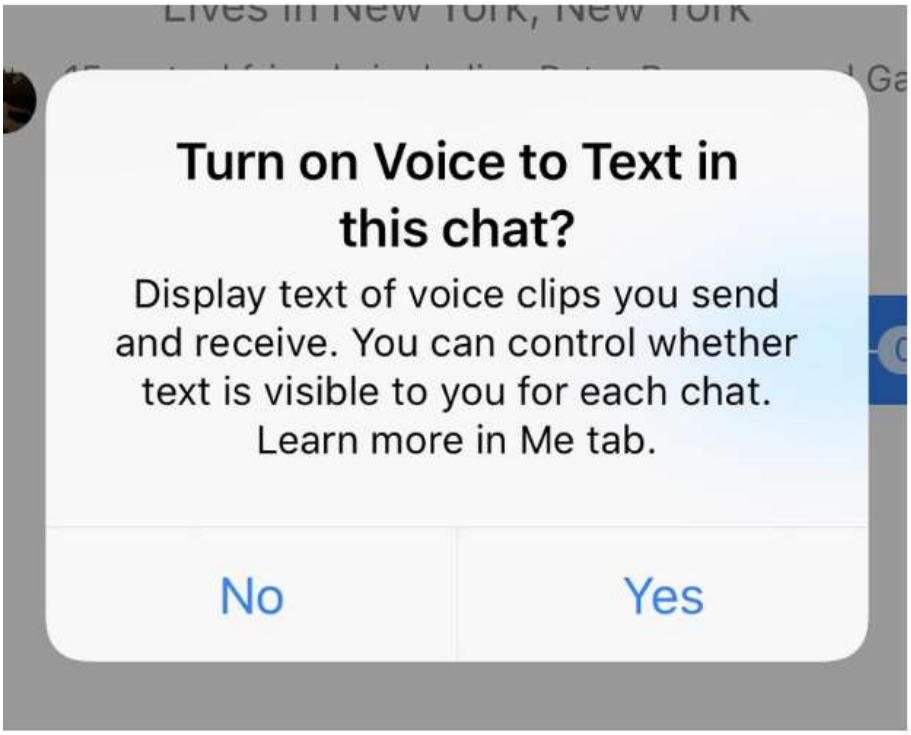
> ***Management's control was not appropriately designed and implemented to address intake, detection, handling, response, remediation, and reporting (as applicable) for all privacy incidents (e.g., misuse of user data by service providers or other third party misuse)."***

321. ***PwC further noted that although it had been unable to complete the investigation, it had still done enough to conclude "that Facebook's privacy controls were not operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information." The firm's investigation was submitted to Facebook on June 6, 2019, and the terms and reasons for why PwC's engagement was ended before it could finish its report were not known***. Facebook and PwC declined to comment. There is no evidence that this assessment was ever reviewed by the Board in the 220 Documents produced to Plaintiffs.

322. On August 13, 2019, *Bloomberg News* reported that Facebook had hired outside contractors to transcribe the audio files of users of Facebook services. Facebook gave these outside contractors the audio files, but no information about where the audio was recorded or how it was otherwise obtained. The contractors stated that the audio files contained Facebook users' private conversations, including sometimes vulgar content. Facebook confirmed that it had been transcribing users'

audio, but it gave no explanation as to why such an invasive practice was started, and stated it would no longer do so after the news was widely disseminated.

323. In response to the reporting, during the week of August 15, 2019, Facebook claimed that Facebook users chose the option to have their voice chats transcribed by outside contractors somewhere in Facebook Messenger's app. However, the Messenger permissions dialogue that, according to Facebook, was the means by which users gave such permission contains no mention of other persons ever being allowed to listen to or review their private conversations:



Even in a separate information page in the Messenger app, dedicated to explaining Voice to Text services, Facebook simply stated, "[v]oice to Text uses machine

learning," and "[t]he more you use this feature, the more Voice to Text can help you." Completely absent from these disclosures was any disclosure that the "machine learning" involved human review and transcription of audio logs.

324. On August 21, 2019, *CNBC* reported that Facebook was walking back prior promises from Zuckerberg to allow users to "flush their history whenever they want." Instead of allowing users to delete their account and all relevant data, Facebook stated that it would merely "disconnect" the Facebook account, allowing Facebook to ***retain*** a record of all of a user's interactions with the Facebook platform, and maintain this information on Facebook's servers for an unspecified period of time. Analysts quoted in the article additionally noted that Facebook would ***also*** still be able to track and retain data about a user's ***future*** interactions with Facebook, even after disconnecting an account, including information recording every time a user opens an app, adds an item to a shopping cart, searches for an item or makes a purchase. The analysts also noted that Facebook's default procedure would be to continue collecting information, as Facebook required users to "opt out" of further information sharing after deleting an account, so that the likelihood of users actually activating the "opt-out" mechanism was very low.

325. Further, as late as September 20, 2019, *CNBC* reported that Facebook had allowed personal user information to be shared, without user consent, with "***tens of thousands of apps***." At this late date, the Company stated that it was belatedly

suspending these Platform Applications, ***which involved 400 companies***, from the Facebook platform. ***Facebook also stated that some of its partners had continued to "inappropriately shar[e] data obtained from us, making data publicly available without protecting people's identity*** or [doing] something else that was in clear violation of our policies." Facebook did not comment on how the Company had continued to allow personal user information to be illicitly shared with tens of thousands of apps, nor how such sharing could be explained in the context of its own obligations to protect personal user information. Instead, Facebook merely stated that the belated suspensions were the result of an internal investigation.

326. Despite its public statements that it would immediately suspend these Platform Applications, Facebook once again did not live up to its promises in the months leading into 2020. As *CNBC* reported on November 5, 2019, as many as 100 companies were still continuing to "improperly" access personal user information, including names and profile pictures of users and certain "groups" of which they were members. Additionally, during the prior 60 days, Facebook had allowed 11 of its partners to access this type of personal user information. In its public statements, Facebook failed to disclose how many users were affected, and stated that, "[a]lthough we've seen no evidence of abuse, we will ask them to delete any member data they may have retained and we will conduct audits to confirm that it has been deleted."

327. Additionally, on November 19, 2019, U.S. Senators Josh Hawley and Chris Coons wrote a letter to Zuckerberg regarding Facebook's practice of continuing to track user location data, even for Facebook users who had chosen to restrict such information from the Company. The Senators also asked the Company to respond to specific questions about, *inter alia*, its data collection practices with respect to users' location information. These questions were prompted by a recent Facebook blog post that indicated that, even if users "opted out" of allowing Facebook to collect their location data, the Company would still track users' locations (a) through "check-ins" on the Facebook app (even if a user is not actually using the Facebook app) and (b) by deducing a user's location by snooping on information regarding a user's internet connection.

328. As the Senators stated in their November 19, 2019 letter to Facebook:

> If a user has decided to limit Facebook's access to his or her location, Facebook should respect these privacy choices. ***The language in the blog post, however, indicates that Facebook may continue to collect location data despite user preferences, even if the user is not engaging with the app, and Facebook is simply deducing the user's location from information about his or her internet connection. Given that most mobile devices are connected to the internet nearly all the time, whether through a cellular network or a Wi-Fi connection, this practice would allow Facebook to collect user location data almost constantly, irrespective of the user's privacy preferences. Users who have selected a restrictive Location Services option could reasonably be under the misimpression that their selection limits all of Facebook's efforts to extract location information***.

In sum, as reflected by the Senators' November 2019 letter, Facebook simply continues to find new ways to provide its users with merely the ***illusion*** of choice with respect to protecting their personal information while actively collecting it—in this instance, as to their location data from their mobile devices—on a continuous basis at virtually all times.

O. Facebook's Impaired Corporate Governance Function

329. In addition to the control allegations made *supra* §VI, which prevent the Board from exercising effective and independent oversight, Facebook's governance function suffers from severe internal control deficiencies that have prevented the Board from taking the remedial efforts necessary to stop a business plan premised on the widespread illegal distribution of personal user information.

1. *The Board's Duties And Presumption Of Director Knowledge Of The Company's Core Business Plans*

330. The Board was under an affirmative obligation to monitor Facebook's controls and business practices concerning personal user information and prevent further dissemination of personal user information to third parties under the 2012 Consent Order.[154] All current and former directors were under this same obligation

[154] The Audit & Risk Oversight Committee charter reaffirms many of these obligations, including, "[t]he Committee will review with management, at least annually, (a) the Company's privacy program, (b) the Company's compliance with its [C]onsent [O]rder with the U.S. Federal Trade Commission, as well as the

because the 2012 Consent Order specified that every current and future director was to be provided with a copy of the Order, which imposed the obligations for a period of 20 years.

331. Moreover, Facebook continually violated the 2012 Consent Order, from its inception, through business plans central to the Company's function, including plans involving the core functioning of the Facebook platform and the deals made with every one of Facebook's business partners that interacted with the Facebook platform. In sum, a director could not have been unaware of Facebook's violations of the 2012 Consent Order unless they were simply unaware of the Company's core business plans. This complete dereliction of duty by any director who might protest a lack of knowledge of the ongoing violations of the 2012 Consent Order constitutes a separate and independent violation of each such director's fiduciary obligations of loyalty and due care.

General Data Protection Regulation and other applicable privacy and data use laws, and (c) the Company's major privacy and data use risk exposures and the steps the Company has taken to monitor or mitigate such exposures, including the Company's procedures and any related policies with respect to risk assessment and risk management." FB220-00020763. The Audit & Risk Oversight Committee Committee was further required to provide "reports to the full board of directors regarding" the matters set forth in their charter, including compliance with the 2012 Consent Order. FB220-00025802.

332. Because directors are presumed to carry out their fiduciary obligations in good faith, it is reasonable to infer that the Director Defendants and Former Director Defendants ***were in fact aware*** that the Company's core business plans, virtually from the date the 2012 Consent Order took effect, through various iterations until as late as 2019, were in violation of the 2012 Consent Order—and yet these serious and ongoing violations of the 2012 Consent Order were never honestly addressed, let alone remedied, by Facebook or its Board.

333. Under Delaware law, when a subject matter is essential and "mission-critical," the Board is obligated to make a good faith effort to put in place a reasonable system of monitoring and reporting about the corporation's central compliance risks. This was and is especially the case for Facebook, where the 2012 Consent Order imposed on Facebook an affirmative obligation to establish a comprehensive privacy program and submit itself to biennial third-party audits.

334. The Director Defendants' failures to institute proper internal controls, and their resulting failure to restrain Facebook's illicit business conduct, have therefore been inexcusable. The Director Defendants' and Facebook's, failure to act evinces a complete and total failure of corporate governance under any circumstances—but their failures, which effectively allowed, *inter alia*, Cambridge Analytica to obtain the personal user information of at least ***87 million users*** for

nefarious purposes, can only be described as egregious in light of the 2012 Consent Order.

335. Of course, for those directors that were also members of management, their culpability is particularly acute. For example, as e-mails produced to Plaintiffs in the Section 220 Action demonstrate, Sandberg [redacted] In one May 2017 email, Sandberg [redacted] FB220-0021580 at FB220-0021581-2.

336. In sum, during the course of this epic corporate governance failure, the Director Defendants were well aware of (or at best recklessly disregarded) the massive risks that Facebook's illegal course of conduct posed to the Company, given (a) the steady drumbeat of numerous red flags that marched past each Director Defendant warning that user privacy and data sharing liability issues plagued the Company and were not being resolved; (b) their knowledge or reckless indifference

to Facebook's adoption of a business strategy that was based on massive data sharing; and (c) the 2012 Consent Order.

2. *The Company's Books And Records Confirm The Board's Apathy, Inaction And Breaches Of Fiduciary Duty*

337. As confirmed by Plaintiffs' review of the 220 Documents obtained from Facebook, from June 26, 2013, the date of Facebook's implementation of its v.3 of the Facebook Platform, through roughly the end of December 2017, before the Cambridge Analytica scandal became front page news, Facebook's Board provided virtually no oversight into whether the Company had sufficient policies in place to protect the privacy of its users' personal information, while Facebook's core business plans were implemented and violated the 2012 Consent Order. While the Board received [redacted], the 220 Documents provide no evidence of any Board efforts or actions to change Facebook's policies or practices concerning the handling and protection of its users' personal information. Similarly, the 220 Documents provide no evidence that the Board engaged in any meaningful inquiry into, or oversight over, Facebook's practices with respect to ensuring that Facebook complied with its legal obligations under the 2012 Consent Order, dealt candidly with regulatory inquiries, or appropriately limited the corporation's massive exposure to legal liability.

3. *The Board's Failure To Review The Biennial Assessments Of Facebook's Compliance With The 2012 Consent Order*

338. Under Section V of the 2012 Consent Order, Facebook was required to obtain "biennial assessments and reports" concerning Facebook's privacy controls and its compliance with the 2012 Consent Order's minimum privacy requirements. Facebook retained PwC to prepare such reports (hereafter, "PwC Biennial Reports"). Four such reports are known to have been duly commissioned, covering the periods of (1) August 2012 to February 2013 (an initial "stub" period, the "2013 Biennial PwC Report"); (2) February 2013 through January 2015 (the "2015 Biennial PwC Report"); (3) February 2015 through January 2017 (the "2017 Biennial PwC Report"); and (4) February 2017 through February 2019 (the "2019 Biennial PwC Report").

339. Only [redacted], was referenced in the Board materials produced to Plaintiffs. As discussed below, according to the Board minutes of the Audit Committee meeting of May 17, 2019, the Audit Committee was given [redacted], and advised that [redacted] FB220-00025082.

340. However, with regard to the Board's review prior to year-end 2017, what is most noteworthy is that ***none*** of the minutes or board presentations produced by Facebook discuss ***any*** of the assessments, other than the [redacted] Given that the Court ordered the production of all Audit Documents in the Section 220 Action (including all audits performed on behalf of Facebook concerning its compliance with data privacy policies and/or the 2012 Consent Order from January 2013 to the present), it is reasonable to infer from the absence of evidence of any other discussions regarding PwC Biennial Reports that the [redacted] was the ***only*** such report whose findings (preliminary or otherwise) were actually reviewed by the Audit & Risk Oversight Committee. In addition, there is no evidence from the Audit Documents produced that the Audit & Risk Oversight Committee ever reported even this limited review of the [redacted] to the full Board.

341. According to Facebook's privilege log provided in the Section 220 Action, on June 10, 2015, the Audit Committee received an "update" concerning [redacted] However, there is no evidence that the update concerns work on any PwC Biennial Report. Nor is there any document in Facebook's production that suggests that the Audit Committee members were given a copy of a Biennial PwC Report covering the period (from February 2013 through January 2015, or less probably, the report

covering February 2015 through January 2017). Having been identified as privileged, this update presumably related to legal concerns—but the absence of any document reflecting Audit or Board action taken to review or change the Company's business practices concerning matters involving a close nexus between "Facebook's privacy program" and the "FTC Consent [Order]" only further strengthens the inference of total Board inaction, even in the face of attorney concerns about related legal liabilities.

342. Moreover, Facebook has not produced any materials concerning the three prior PwC Biennial Reports (collectively covering the period of August 2012 through January 2017) that evidence any Board or Audit Committee level supervision and oversight of Facebook's privacy program. Rather, the available evidence indicates that the directors allowed the Company's privacy program to be run, and overseen, solely by a select cadre of senior executives (including the Chief Privacy Officer of Products) who reported directly to either Zuckerberg or Sandberg. This abdication of active board oversight responsibility is a classic case of allowing the foxes to manage and oversee the henhouse.

343. Nor would Board reliance on the PwC Biennial Reports have been an adequate substitute for Board leadership with respect to legal compliance, even if the Board had given the PwC Biennial Reports any close attention. The 2012 Consent Order required, *inter alia*, "regular testing or monitoring of the

effectiveness" of the controls and procedures that Facebook was obligated to establish to protect personal user information (including express user consent requirements). Given (a) management's ability to control the information presented to PwC; (b) the fact that PwC conducted its assessments only every other year; (c) the obvious conflicts between Facebook's post-2012 Consent Order core business plans to increasingly monetize personal user information; and (d) the 2012 Consent Order's paramount object of protecting user privacy; no Board acting in good faith would have relied solely on PwC to assure ongoing compliance (especially so without any scrutiny of PwC's work). Additionally, a Board cannot rely on the assurances of reports they have not reviewed.

344. Based on the available record, moreover, the Board apparently has not even bothered to review how the prior PwC Biennial Reports were satisfied that Facebook's "Data Use Policy . . . [adequately] informs users about how information is disclosed to applications created by developers when a user connects to those applications," (2015 Biennial PwC Report); or "Facebook's Platform privacy settings and Granular Data Permissions ('GDP') allows users to control the transfer of covered information from Facebook to third-party applications," 2017 PwC Biennial Report. This abdication of oversight occurred at a period when, *inter alia*, Facebook was actually sharing massive amounts of personal user data, ***as well as the***

personal data of those users' friends, with third parties, without users' knowledge or consent. *See e.g.* ¶¶ 6, 10, 15, 22, 97, 100, 106, 131, 186.

4. *The Evidence Concerning The Board's Review Of Annual "SOC" Reports Only Confirms The Directors' Failure To Ensure Compliance With The 2012 Consent Order's Obligations For The Protection Of Personal User Information*

345. A January 11, 2016 Audit Committee presentation included a review of [redacted] FB220-00001015 at FB220-00001020. The presentation also apprised the Audit Committee of the [redacted][155] FB220-00001027. The Atlas SOC reports considered matters relating to [redacted] Custom Audiences SOC2 considered matters relating to [redacted] FB220-00001399, 1048-49.

[155] Although the parties and the Court have referred to these engagements as "audits," technically they appear to have been "attestations" rather than "audits." Consistent with past usage, however, this complaint will refer to them as "audits," and refer to the resulting E&Y work product as a "Report."

346. According to February 10, 2016 Audit Committee presentation materials, for which no meeting minutes were produced, the Audit Committee (which would have at that time included Defendants Bowles, Andreessen, and Desmond-Hellmann) received, but did not discuss, a [redacted] that would include an "Atlas SOC1" report (which was not produced to Plaintiffs) and a "Custom Audiences SOC2" report. FB220-00001067. The Company also had E&Y conduct Atlas SOC2 and SOC3 Reports, and Custom Audiences SOC2 and SOC3 Reports, all for the period January 1, 2015 through December 31, 2015.

347. ***None of these Reports reviewed, considered or provided any insight into Facebook's reciprocal sharing of personal user information with Platform Applications, whitelisting agreements, the monetization of personal user information, or any of the other misconduct described herein. Additionally, none examined Facebook's obligations or compliance under the 2012 Consent Order***. ***Instead, these SOC reports solely concerned*** [redacted] ***, and did not examine controls with respect to the data of the Company's users***. For example, this focus was explained in a chart from an Audit Committee meeting presentation dated

January 11, 2016 (FB220-00001015) discussing the [redacted]

FB220-00001027. Facebook also produced Custom Audience SOC2 and Custom Audience SOC3 Reports covering 2016 and 2017, and four SOC2 and SOC3 "Workplace" [156] Reports for 2016 and 2017, but none of these reports reviewed, considered or provided any insight into any of those topics, either.

348. The structure of all of the Atlas, Custom Audiences and Workplace SOC Reports was fundamentally the same: namely, they contained [redacted]

[156] As stated in the 2016 Workplace SOC2 Report, [redacted] FB220-000044398.

[redacted][157] More specifically:

(a) the "Opinion" portion of each SOC2 report expressed E&Y's opinion that [redacted] AICPA Trust Services Principles §100 (***the "Applicable TSP Criteria"***)][158] [redacted]

[157] The SOC3 reports do not have [redacted] but instead describe [redacted] They are otherwise the same in format.

[158] The long-form title of the AICPA's TSP §100 is "Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy."

[redacted] [*See, e.g.* FB220-00004049 to 4051]; and

(b) the "Opinion" portion of each SOC3 report expressed E&Y's opinion that, [redacted] [*See, e.g.*, FB220-00004140-41].[159]

349. While couched in terms of finding satisfactory privacy controls, a faithful director exercising his or her fiduciary duties in good faith would know that

[159] The Company also produced a 2017 SOC3 Report for Custom Audience, styled as a "Type II Report," which states more briefly, [redacted] FB220-00004747. The SOC3 Type II reported [redacted]

the SOC Reports said nothing about Facebook's compliance with the 2012 Consent Order, and actually raised far more questions than they answered about Facebook's compliance with its confidentiality obligations to its individual users.[160]

350. For example, all of the SOC2 and SOC3 Reports (for 2015, 2016 and 2017, the last year for which they were produced) refer to Facebook's [redacted]

[redacted]

It then [redacted]

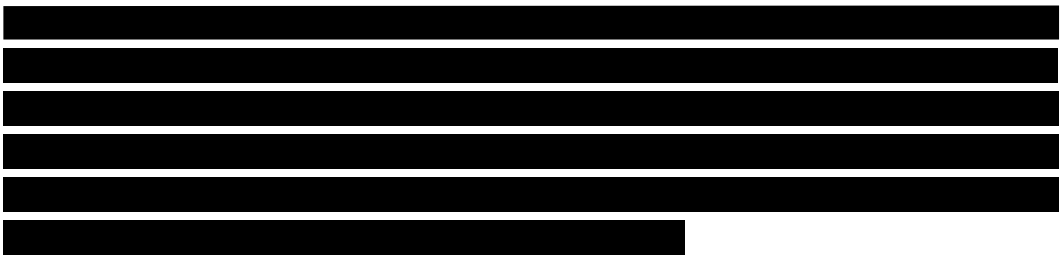
See, e.g., FB220-00004157; FB220-00004512 at 4531-32.

[160] As an example, even the term "user" in the context of the SOC Reports does not refer to an individual user with an account on the Facebook platform. In the SOC Reports, "users" generally refers to third party "users" of the relevant Facebook system (e.g., advertisers who "used" Facebook's Custom Audiences System).

351. However, none of the SOC Reports ever explained how personal user information covered by the 2012 Consent Order—notably information that required express and informed user consent before Facebook could share it—was classified under this four-category scheme. Moreover, the summary of the limited testing that E&Y did to find reasonable assurance that Facebook appropriately protected "Private," "Confidential" and/or "Regulated" categories simply confirms that E&Y did ***not*** test whether a Facebook user's personal data (let alone the user's friends' data) was being ***shared*** with third parties without the user's consent. Instead, E&Y made clear that it only [redacted] *See* FB220-00004133. E&Y's testing of [redacted] said ***nothing*** as to whether Facebook was complying with the 2012 Consent Order's requirement that users give their clear and informed consent ***before*** ***Facebook could make the user's personal***

data <u>available</u> to a third party in the first place.[161] There is no basis in the materials produced to suggest that any Director ever sought to explore this gaping hole in E&Y's testing of Facebook's "Security and Confidentiality" controls for the Company's Custom Audience, Atlas and Workplace systems.

352. There was also nothing in any of the SOC Reports that would suggest that the Audit Committee or the Board had ***any*** role in supervising or reviewing any confidentiality or privacy matters, let alone any role in ensuring compliance with the 2012 Consent Order. Instead, the SOC2 reports recite only that:



FB220-00004058. By contrast, Board oversight is nowhere mentioned, or even hinted at.[162]

[161] *See In re Facebook, Inc. Section 220 Litig.*, 2019 WL 2320842, at *14 n.147 (Del. Ch. May 31, 2019) (the "May 2019 Order") (noting that the Consent Order "explicitly require[d] Facebook and its representatives to . . . implement procedures reasonably designed to ensure that covered information cannot be ***accessed*** by any third party from servers under [Facebook's] control").

[162] *See id.* at *3 ("The implementation of the Consent Decree was to be monitored at the Board level by Facebook's Audit Committee.").

353. Perhaps most egregious, however, is the inference that can be drawn from the SOC Reports and the sparse contents of Facebook's books and records as to the Board's failure to set up any meaningful ***internal audit*** controls to insure that senior management was in fact complying with the 2012 Consent Order and any other applicable regulatory restrictions on giving third parties access to personal user data (or to users' friends' data).

354. Specifically, the SOC Atlas, SOC Custom Audience and SOC Workplace Reports (all prepared by E&Y) all contain the following statement:

[redacted]

See, e.g., FB220-00004148 (2015 Custom Audience SOC3 Report); FB220-00004175 (2016 Atlas SOC2 Report). However, the Section 220 Documents produced by Facebook contained ***no copies*** of [redacted] ***no copies*** of [redacted] and ***no copies*** of any [redacted] that went to the Board level and tested Facebook's obligations under the 2012 Consent Order or examined Facebook's core business practices to discover the misconduct described *supra* §§IV.A–F.

355. This absence from the Section 220 Documents of any evidence of a functioning Board-level review of Facebook's controls with respect to user data must be considered in light of this Court's Order directing Facebook to provide "Audit Documents," which the Court defined as including "[the SOC2/3] audits performed on behalf of the Company, and any other formal internal audits performed regarding compliance with Facebook formal data privacy policies and procedures or with the Consent Decree." May 2019 Order at 52.

356. Facebook's failure to produce such documents establishes the reasonable inference that no such [redacted] or [redacted] exist. A further reasonable inference is that the Board, since January 2013 (the defined scope of "Audit Documents" under the May 2019 Order, *see id.* at 55), continued on for a period of almost six years without seeing any such internal compliance reports, without ever raising this as an issue with management, and without otherwise acting to install a functioning internal governance regime. The only reporting provided to the Board included, at best: (a) [redacted] consisting of [redacted]; and (b) periodic [redacted] limited to [redacted]

[redacted] that fail to describe such changes in any detail.

357. Perhaps most damning, one can equally infer that, ***never having seen such reports, the Board similarly knew (or recklessly disregarded) that Facebook was not conducting any regular internal audits or preparing any regular reports to test Facebook's business operations concerning***: (a) FTC-related compliance; (b) the effective operation of controls to mitigate risks identified by the 2012 Consent Order; or (c) any [redacted] prepared by Facebook's Internal Audit Department. In short, not only did the Board conspicuously fail to monitor management's performance under the 2012 Consent Order, it also knowingly failed to empower and enable the firm's Internal Audit Department to act as a meaningful, day-to-day internal "watchdog" over the powerful senior management "foxes" who were allowed to guard the henhouse.

358. The SOC3 Atlas review for 2016 covered only [redacted] While the [redacted] It is thus not clear from the SOC3 Atlas review which category Facebook's management attributed personal user information to, but what is clear is

that these classifications were only used to examine data sharing with Facebook's advertising partners.

5. *The Audit Committee's Involvement In Approving Misleading Changes To SEC Disclosures, And The Directors' Knowledge That Facebook's Core Business Practices Were Attracting Increasing Regulatory Attention*

359. The Directors Defendants' lack of oversight throughout the 2013-2017 period was especially egregious for those who were members of the Audit Committee, which included Bowles (2013-2017), Andreessen (2013-2017), Thiel (2013), and Desmond-Hellmann (2014-2017), because they reviewed and approved the SEC filings that contained the privacy disclosures found to be false and misleading by the SEC on July 24, 2019, that (1) misleadingly indicated that Facebook only faced a hypothetical risk that user data could be misused; and (2) actively concealed the nature of the data misuse. These misleading disclosures included:

a. From a 2013 Form 10-K, filed with the SEC on January 31, 2014, for the fiscal year ended December 31, 2013, discussing how "[i]mproper access to or disclosure of user information . . . ***could*** harm our reputation and adversely affect our business." FB220-00000401;

b. From the 2013 10-K referenced above, changing the disclosure that Facebook's [redacted]

[redacted] to how the "Data Use Policy ***governs the collection and use of information we receive in connection with our services***." *Id*.;

c. From a Form 10-Q for the third quarter of 2015, filed with the SEC on November 5, 2015, [redacted] that improper access to or disclosure of user data "***may*** . . . result in financial harm to us." FB220-00000998;

d. From a Form 10-Q for the second quarter of 2017, filed with the SEC on July 27, 2017, modifying the disclosure [redacted] and replacing that phrase with "***shared between countries or regions in which we operate***." FB220-00001468; and

e. From the 2Q 2017 Form 10-Q referenced above, [redacted] read that Facebook's business would be impacted adversely "if we ae prohibited from sharing [***personal***] data among our products and services." *Id*.

360. Yet despite having actual knowledge of—or having inexplicably failed to adequately inform themselves of—the extreme risks that Facebook was exposed

to by allowing thousands of third parties practically unlimited access to personal user information, the Audit Committee did little more than make cosmetic edits to Facebook's SEC filings rather than conduct any actual oversight of the accuracy of their privacy disclosures.

361. For example, in connection with a presentation to the Audit Committee on January 28, 2014, the Audit Committee reviewed [redacted] The Company's risk disclosures included information about the [redacted] but did not disclose that Facebook was willfully entering into and maintaining whitelisting and reciprocity arrangements with its business partners to generate, ***and share***, as much personal user information as possible.

362. The Audit Committee approved changes to the language for the Company's [redacted] at its January 28, 2014 meeting. The original language had stated: "Our Data Use Policy governs the collection and use of ***information that users share*** using our services, including information we receive in connection with our services." At this meeting, the Audit Committee approved a change to delete [redacted] so that the disclosure

read: "Our Data Use Policy governs the collection and use of information we receive in connection with our services." FB220-00000362 at FB220-00000401. In light of the Audit Committee's knowledge of the 2012 Consent Order and the increasing regulatory scrutiny regarding privacy, the Audit Committee's elimination of [redacted] reflected the Audit Committee's culpable knowledge, or reckless disregard, of the fact that Facebook's data sharing policies were inconsistent with the 2012 Consent Order and the requirements for Company disclosures thereunder.

363. A [redacted] presentation from management to the Audit Committee dated February 12, 2014 states: [redacted] FB220-00000282 at FB220-00000299. The presentation describes [redacted] FB220-00000301. The presentation further stated that the Audit Committee [redacted] *Id*. The Audit Committee was also told that

[redacted] and that [redacted] FB220-00000314.

364. Yet, the Audit Committee did not have any policies or reporting procedures in place to confirm or ensure that the sharing of personal user information—which the Company was actively engaged in on a massive scale and had already "authorized" as part of Facebook's core business plan—was done only after "obtain[ing] the user's affirmative express consent" (*see* 2012 Consent Order at §II.B) and otherwise in accord with all of the requirements the 2012 Consent Order. In short, by focusing solely on "unauthorized" sharing of personal information, the Audit Committee failed to install and actively oversee governance procedures to fulfill its legal obligation to ensure that what "Facebook had "authorized" with respect to sharing personal user information was in fact consistent with its users' privacy settings and otherwise in compliance with the 2012 Consent Order. The Audit Committee thus failed in its duty to monitor whether, and ensure that, the Company's privacy practices were at all times consistent with the requirements of the 2012 Consent Order.

365. Also in this February 12, 2014 presentation, the Audit Committee was made aware that [redacted]

[redacted] FB220-00000311. The Audit Committee was also informed of a [redacted] FB220-00000312. The Audit Committee was also told that [redacted] FB220-00000315.

366. At the same time, as of the February 12, 2014 presentation (which was roughly one and a half years after the 2012 Consent Order became final), the Audit Committee knew that Facebook's compliance efforts were woefully inadequate, because the same presentation advised them that Facebook had [redacted] FB220-00000313. Facebook at all relevant times has had at least ***hundreds of millions*** of active users, with over 2.5 ***billion*** monthly active users as of December 2019, ***tens of thousands*** of employees (nearly 45,000 today), and annual revenues measured in the ***billions*** of dollars. To allow Facebook to delay until late 2013 before it [redacted] was a glaring red flag, and further evidences the Director Defendants' willful or reckless disregard for whether the Company operated within the bounds of the law. This is especially so given the 2012 Consent Order's express directive that Facebook implement a "comprehensive privacy program . . . contain[ing] controls and procedures

appropriate to [Facebook]'s size and complexity, [and] the nature and scope of [Facebook]'s activities."

367. In Board materials for the February 13, 2014 Board meeting (FB220-00000001), the Board was informed of how [redacted] *See* FB220-00000125. The same materials further stated that, [redacted] *Id*. Given that the Board was on notice by 2014 that [redacted], the failure of the Board to take forceful steps to ensure that Facebook's fundamental business model was in full compliance with both U.S. and foreign law and regulations was shocking—and particularly so given their actual knowledge that the Company had already been targeted by the FTC, subjected to a 2012 Consent Order, and was operating in violation of that. Again, the Board's meeting minutes indicate that the

Board took no action in response to this information, and it proposed no reforms or other changes to the Company's business model.

368. In the same materials, the Board was also informed that [redacted] a *Id*. Thus, the Board was also informed that the [redacted], despite the Company's public statements to the contrary. Again, the minutes indicate that the Board took no action in response to this information, and it proposed no reforms or other changes to the Company's business model.

369. A presentation for the Board meeting of August 21, 2014 (FB220-00000457) put the Board on further notice that Facebook lacked proper controls to protect its users' privacy, ***as it*** [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

FB220-00000545-46.

370. Thus, even with the Board's knowledge of the 2012 Consent Order, increasing regulatory scrutiny, and of [redacted], the Board sat idly by as Facebook adopted changes to its Data Use Policy that management itself described as [redacted] and allowed for Facebook to continue to engage in the information sharing practices made illegal under the 2012 Consent Order. The Board also stood by idly as Facebook attempted to manipulate [redacted], without conducting any analysis on whether such efforts (even if "successful") would still cause the Company to operate below the minimum standards of data privacy protection that Facebook's was required to comply with under the 2012 Consent Order.

371. A presentation to the Board dated December 4, 2014 (FB220-0000580) further alerted the Board to ongoing privacy issues:

[redacted]

[redacted]

FB220-000000622-23 (emphasis added except in paragraph headers, where emphasis was in original).

372. In a February 11, 2015 Audit Committee presentation (FB220-00000625), the Audit Committee was again expressly advised of [redacted] FB220-00000659. The Audit Committee was also told about [redacted] *Id*.

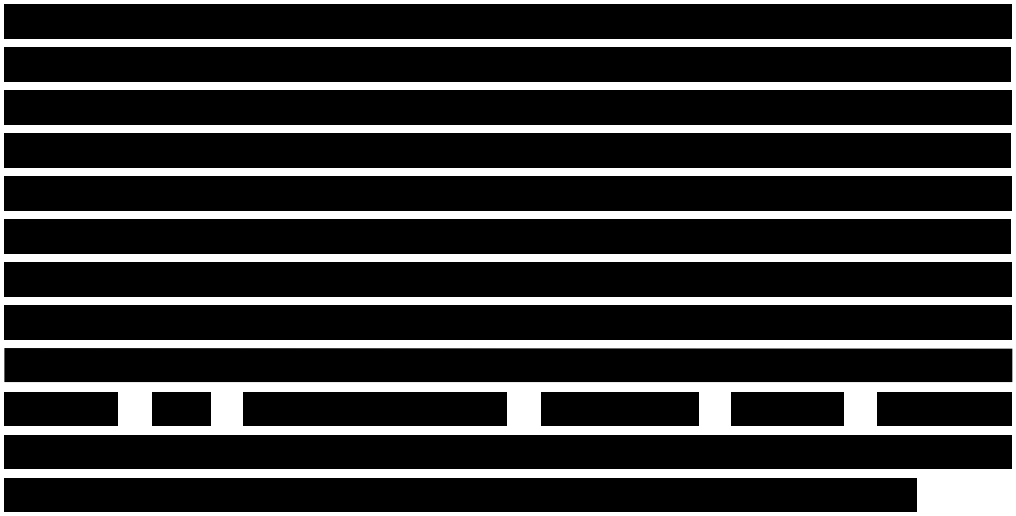
373. A February 12, 2015 Board presentation (FB220-00000762) further alerted the Board to [redacted]

[redacted]

- [redacted]

- [redacted]

- [redacted]



FB220-00000859-60 (emphasis added in body; emphasis in headers in original).

374. In sum, in February 2015, the Board was again informed about [redacted]—and was again advised that Facebook would [redacted] Once again, however, the Board sat idly by and failed to investigate or reform Facebook's business practices, despite the obvious risk that the Company's efforts to promote [redacted] privacy provisions (which were described as [redacted] would do nothing to bring the Company into compliance with its obligations under the 2012 Consent Order, and would instead likely create only a

pretext for Facebook to continue (if not expand) its rampant violations of the 2012 Consent Order.

375. Further Section 220 Documents reviewed by Plaintiffs confirm that the Board continued to breach its fiduciary duties in failing to institute and maintain a working governance function for Facebook through 2015 and beyond.

376. For example, based on presentation materials for an October 20, 2015 Audit Committee meeting (FB220-00000682), the Audit Committee reviewed a draft Form 10-Q for the third quarter of 2015, which included [redacted] FB220-000000862 at FB220-0000998. Thus, these Individual Defendants were expressly advised and knew or recklessly disregarded that Facebook's unfettered sharing of personal user information presented a risk of material financial harm to the Company. However, notwithstanding that the Audit Committee knew or at best recklessly disregarded in October 2015 that the Company's core business [redacted], there is no evidence in the Company's books and records that the Audit Committee took any steps to investigate or otherwise act on the resulting risk of serious financial harm to Facebook.

377. On December 11, 2015, *The Guardian* published an article, "Ted Cruz using firm that harvested data on millions of unwitting Facebook users." This article

partially revealed Cambridge Analytica's use of "psychological data," which it had created through access to Facebook users' (and users' friends') personal information. As alleged *supra* ¶¶191–95, Facebook was contemporaneously aware of this harvesting having occurred. However, no materials were produced showing any Audit Committee or Board discussion of this article or Cambridge Analytica's collection and use of the personal data of "millions of unwitting Facebook users," even though *The Guardian* reported that users' data was being harvested without their consent. Indeed, most of the data was collected from users' friends who had never even heard of the application used to collect Facebook user information, making the Board's failure to prevent such an occurrence, and subsequent failure to investigate the conduct to ensure no similar violations had occurred or could occur, a transparent violation of Facebook's obligations under the 2012 Consent Order.

378. Board minutes for a meeting on December 8, 2016 (FB220-00001162) included notes that the Board had previously received [redacted] FB220-00001174. However, the requirements of the 2012 Consent Order were nowhere discussed by the Board. Instead, the update simply refers to information on [redacted] FB220-00001185 (emphasis in original).

379. These [redacted] as Facebook characterized them, included [redacted] *Id*. The Board minutes also reflect that the Board was aware that [redacted] in Europe had begun regarding [redacted] *Id.* The Board was thus on notice of the data privacy problems that Facebook's business practices implicated, yet it continued to fail to examine (let alone ensure) Facebook's compliance with its obligations under the 2012 Consent Order. Instead, as reflected in the Board minutes, management and the Board internally cast regulatory attempts to ensure consumer privacy was protected as [redacted] Given the Board's awareness that Facebook's business model required the widespread sharing of personal user information with third parties, and that further regulatory scrutiny posed a threat to that plan, the Board's failure to act and ensure compliance with the 2012 Consent Order was egregious.

380. Presentation materials for a February 15, 2017 Audit Committee meeting (FB220-00001344) included [redacted] Those materials advised the Audit Committee of [redacted]

[redacted] FB220-00001373. The Audit Committee was also told that going forward, there would be [redacted] FB220-00001374. Once again, however, there is no evidence in the Company's books and records that the Audit Committee did anything in response to these materials to bring the Company's practices into compliance with the 2012 Consent Order, even though it was now undeniably on notice that the Company was [redacted] FB220-00001373.

381. The Board received a similar update in presentation materials dated February 16, 2017. FB220-000011188. However, the accompanying Board meeting minutes for a Board meeting held on February 16, 2017 were entirely redacted, indicating that the Board did not review or discuss the responsive topics covered in the presentation materials. FB220-00001291. The materials covered the results of an [redacted] which would have notified the Board of the dire risks to the Company should Facebook not be a good steward of its users' personal information. However, the presentation failed to address Facebook's data sharing with Platform Applications, whitelisting agreements, data reciprocity, or other misconduct described herein, and failed to examine Facebook's obligations or compliance under the 2012 Consent Order, so it would have been of little use had

the Board actually reviewed and discussed it. The assessment also would have informed the Board that the protection of personal user information was critical to the Company, but the threat was posed as an external risk, and Facebook's business practices were never examined.[163]

382. The February 16, 2017 Board presentation also included a report on [redacted] that included [redacted] FB220-00001269 (emphasis in original). These [redacted] in Facebook's words, included a [redacted] (emphasis removed), [redacted] and [redacted] *Id*. Facebook's obligations and compliance under the 2012 Consent Order were nowhere discussed in this

[163] For example, the report stated that, [redacted] FB220-0001221.

presentation. And despite this additional regulatory scrutiny that the Board knew, based on this presentation, impacted Facebook's fundamental business model, the Board condoned the Company's practices because there is no evidence in the documents produced that the Board sought to change or reform Facebook's data sharing with Platform Applications, whitelisting agreements, data reciprocity, or other misconduct described herein.

383. The Board received a [redacted] presentation dated June 1, 2017. FB220-00024498. The accompanying Board meeting minutes were not produced, indicating that the Board did not discuss the presentation materials. The Board was provided [redacted] as part of a [redacted] section of the presentation. FB220-00024510. Despite being given [redacted], and thus being reminded that Facebook was required to obtain affirmative consent from users before sharing their personal user information, the Board took no action to investigate or reform the Company's business practices. Instead, the Board stood idly by while Facebook characterized regulatory concerns regarding the Company's treatment of user privacy as [redacted] FB220-00001287 (emphasis in original).

384. Instead of taking Facebook's problematic practices seriously, as would be required in the face of correspondence from the FTC concerning the 2012 Consent

Order, in addition to the numerous regulatory inquiries building against the Company regarding its treatment of personal user information and data privacy practices, the Board failed to discuss the 2012 Consent Order at all, and took no action in response to either examine the Company's business practices in the context of the 2012 Consent Order or bring Facebook into compliance. Instead, it received information of [redacted] while allowing regulatory and legislative initiatives to be [redacted] by management. FB220-00001287.

385. The Audit Committee presentation of July 25, 2017 (FB220-00001442) showed that the Audit Committee knew about [redacted] In a draft Form 10-Q for the second quarter of 2017, the Audit Committee approved the modification of the language: [redacted] FB220-00001468. Thus, the Audit Committee actively concealed the fact that Facebook shared personal user information with partners and to countries outside of the United States, disguising the fact that the information at issue being shared between countries was personal user information

386. The Audit Committee similarly allowed Facebook's risk disclosure to remove the word [redacted] from [redacted] so that the Form 10-Q further concealed that Facebook shared personal user information in violation of the 2012 Consent Order. The Form 10-Q was changed to read that [redacted] *Id*. Moreover, as alleged in the SEC Complaint, these disclosures were misleading to the extent that they indicated that Facebook only faced a hypothetical risk that user data could be misused, when in fact executives at the highest levels in the Company actively promoted a business plan that depended on the misuse of user data through constant, illicit sharing with third parties.

387. The Audit Committee presentation of September 6, 2017 (FB220-00001483) included draft May 31, 2017 Audit Committee minutes (FB220-00001535), which included a presentation by [redacted] of [redacted] FB220-00001537. The Audit Committee minutes are surprisingly silent regarding the interactions described between Stamos, Zuckerberg and Sandberg at and surrounding this meeting, detailed *supra* §IV.L.2. Given the sparse

detail regarding [redacted] presentation in the materials produced to Plaintiffs, and the detailed circumstances concerning Stamos' inability to present his full views to the Audit Committee as detailed *supra* §IV.L.2, it is reasonable to infer that the Audit Committee was on notice that Facebook had severe internal control problems regarding data security risks related to its products, and was further aware that Facebook's management, led by Zuckerberg and Sandberg, were attempting to stifle or outright destroy Board oversight into these issues.

388. The December 6, 2017 Audit Committee meeting materials also include draft September 6, 2017 Audit Committee meeting minutes, which are entirely redacted for responsiveness. It is thus reasonable to infer that the Audit Committee did not have any further relevant discussions during that meeting, and that significant information concerning Facebook's business practices were being withheld from the Audit Committee.

389. Through a December 6, 2017 Audit Committee meeting presentation (FB220-00001607), the Audit Committee was again informed of the [redacted], including, the [redacted] FB220-00001629. Nowhere during the meeting did the Audit Committee

address Facebook's own data sharing with Platform Applications, whitelisting agreements, data reciprocity, or other misconduct described herein, and nowhere did the Audit Committee examine Facebook's obligations or compliance under the 2012 Consent Order.

390. In addition, according to Facebook's privilege log, at a December 6, 2017 meeting, the Audit Committee received a report from [redacted] Thus, the Audit Committee was aware that Facebook had voluntarily shared personal user information in a manner that allowed Cambridge Analytica to harvest and analyze the personal user information of at least 87 million Facebook users. This knowledge was imparted to the Audit Committee months before the data breach was reported in the news. And yet, even armed with the knowledge that Facebook's practices had actually caused tremendous harm to its users, and would cause tremendous harm to the Company should the truth be exposed, the Audit Committee chose to do nothing in response. For example, the Audit Committee did nothing to ensure that this information was disclosed to the Board or to the public. Nor did the Audit Committee propose any reforms to Facebook's data sharing with Platform Applications, whitelisting agreements, data reciprocity, or other misconduct described herein. At an even more basic level, the Audit Committee failed to examine Facebook's obligations or compliance under the 2012 Consent Order,

despite knowledge that the Company had failed to adequately protect its users' personal information, as required under that 2012 Consent Order.

P. The Board Fails To Reform Facebook's Illegal Business Practices In The Wake Of Cambridge Analytica

1. *The Board Knows Facebook Continues To Share Vast Amounts Of Personal Information In Contravention Of The 2012 Consent Order*

391. Even after the Cambridge Analytica scandal broke out in full force, the Board limited itself to cosmetic changes, while Zuckerberg and Sandberg focused on a PR response.

392. *The New York Times* and *The Guardian* simultaneously published reports of the Cambridge Analytica scandal on March 17, 2018. The scandal had severe immediate effects, including a $36 billion wipeout of market capitalization the next day for Facebook.

393. The Audit Committee met five days later, on March 22, 2018. The members who attended the Audit Committee meeting were Andreessen, Bowles, and Desmond-Hellmann. Other directors in attendance were Chenault, Hastings, Sandberg, and Zuckerberg. The Audit Committee discussed [redacted] and [redacted]

[redacted]

FB220-00024676 at FB220-00024677.

394. The Committee also discussed [redacted] including [redacted] and [redacted] *Id*. For the reasons discussed above, these audits were fundamentally flawed. These audits also failed to address Facebook's own misconduct in the matter, including the fact that its fundamental business model included granting developers access to user data without affirmative user consent, in violation of the 2012 Consent Order.

395. Moreover, the Audit Committee also discussed [redacted] and [redacted] *Id*. Thus, the Audit Committee's only response to Cambridge Analytica was to [redacted]

[redacted] The Audit Committee thereby condoned an illegal business plan, rather than confront Zuckerberg and bring about actual accountability.

396. The final item in the March 22, 2018 Audit Committee meeting minutes acknowledged that [redacted]

[redacted]

FB220-00024676 at FB220-00024678.

397. On March 26, 2018, the FTC confirmed it was investigating whether the Cambridge Analytica incident breached the 2012 Consent Order.

398. The Board met on March 28, 2018. FB220-00024669. All of the then-directors attended the meeting: Andreessen, Bowles, Chenault, Desmond-Hellmann, Hastings, Koum, Thiel, Sandberg, and Zuckerberg. The Board was apprised of [redacted]

399. The March 28, 2018 minutes indicate that the Board then received [redacted] and [redacted] The Board was thus aware of the [redacted] was having on Facebook's goodwill, financials, and stock price.

400. After discussing the [redacted], the Board then received and discussed an update from [redacted]. The update showed that the Board had [redacted] (and, it is reasonable to infer, how those [redacted]:

[redacted]

FB220-00024669 at FB220-00024670.

401. At the same meeting, the Board was also informed that the Company had [redacted]. The Board discussed the [redacted] and [redacted]

402. Afterwards, the Board discussed [redacted] and [redacted] The review did not include any investigation of Facebook's own data sharing practices, despite the Board's receipt in the same meeting of information about [redacted], which would have included information about the [redacted] The investigation instead was geared to cast blame on third parties, without seriously considering the Company's own business practices.

403. The Board then discussed [redacted] This investigation, too, failed to address the fundamental issues inherent in the Company's business model, spearheaded by Zuckerberg and Sandberg.

404. Thus, in the immediate aftermath of Cambridge Analytica, as the March 28, 2018 meeting minutes disclose, the Board's focus remained on [redacted] The Board had just received a [redacted] that Facebook allowed for the sharing of vast amounts of personal user information without consent, including sharing the personal information of 87 million users when no more than 270,000 could have possibly consented to that sharing through Kogan's app. Instead of investigating the extent to which Cambridge Analytica was merely the natural consequence of a business plan predicated on "full reciprocity," the Board was satisfied with the plan to merely investigate "misuse" as the fault of Facebook's developer partners.

2. *The Board's Oversight Failures Are Revealed Through Internal Investigation, And Responded With Cosmetic Changes*

405. The Audit Committee again met on April 26, 2018, with Andreessen, Bowles, and Desmond-Hellman attending. FB220-00024674. The discussions

included [redacted] and [redacted] FB220-00024674 at FB220-00024675. It is thus reasonable to infer that, before April 26, 2018, Facebook did not have functioning oversight relating to privacy and data use, because [redacted] In addition, such [redacted], rather than addressing Facebook's fundamental breach of its obligations under the 2012 Consent Order.

406. According to a presentation to the Board dated May 31, 2018, (for which the accompanying minutes were not produced) the Board was asked—now more than two months after the Cambridge Analytica scandal broke—to [redacted] FB220-00024685 at FB220-00024694.

407. An [redacted] dated May 30, 2018 (FB220-00024788) was also presented to the Board. One item describes the [redacted]

[redacted] Thus, the Board was reminded within two months of the Cambridge Analytica scandal that the [redacted] Despite these serious red flags, the Board's response was to promote only cosmetic changes.

408. The first item for the May 31, 2018 presentation to the Board was an [redacted] The [redacted] included a [redacted] The only concrete action item from this meeting were [redacted] In the face of intensifying governmental investigations into unprecedented consumer privacy violations, the Audit Committee's response to its first [redacted] following public knowledge of Cambridge Analytica was not a wide-ranging internal investigation or corporate governance reforms, but a cosmetic change to [redacted]

409. The draft [redacted] also made only cosmetic changes to the [redacted] FB220-00024685 at FB220-00024739-45. The [redacted]

[redacted] However, the responsibilities of the Audit Committee [redacted] which did not change.

410. The presentation also showed that the Board [redacted] which actually loosened the Company's corporate governance. For example, the Board changed [redacted] The Board also [redacted] Thus, at a point when Zuckerberg was under increasing public and regulatory scrutiny for his failing leadership and outsized influence compared to his ownership stake in the Company, the Board actually proposed to ***reduce*** its oversight of his performance. The Board also proposed other cosmetic changes such as changing [redacted] and changing the [redacted]

411. The superficial changes to the [redacted] did nothing to ensure oversight over Facebook's sharing of personal user

information. Previously, [redacted] The changes in the [redacted] merely provided [redacted]

412. Despite the fact that the 2012 Consent Order put the Board on notice for ***six years*** before the Cambridge Analytica scandal that the Board and the Audit Committee needed to establish effective governance over Facebook's sharing of personal information, the Audit Committee failed to even discuss with management items such as privacy, data use, compliance with the 2012 Consent Order, or cybersecurity until this point. Moreover, these additional items were merely cosmetic changes, as the [redacted] these items. At a time when Management had shown itself to be completely incapable of ensuring that the Company was in compliance with its legal obligations, the Audit Committee decided

to continue to rely on management through [redacted] rather than ensure that independent mechanisms were in place to bring the Company into compliance.

413. At the May 31, 2018 meeting, the Board also reviewed [redacted] including a [redacted] Yet, other than the cosmetic changes to the [redacted], the Board failed to [redacted]

414. After these initial meetings, the Board and the Audit Committee held meetings on the same pre-existing schedule as previous years. Despite the drumbeat of regulatory inquiries, news coverage and ongoing misuse of personal user information, waving red flags that the Company's business model violated the 2012 Consent Order, the Board and Audit Committee contented themselves with cosmetic

changes to their purviews while continuing to allow management to control the flow of information regarding legal compliance, privacy, and security risks. The Board thereby continued to bless Facebook's illicit business model.

415. The Audit & Risk Oversight Committee next met on July 24, 2018, with members Andreessen, Bowles, Chenault, and Zients in attendance, as well as Board director Desmond-Hellmann observing. FB220-00024680. Only a [redacted] and no other discussion ensued regarding broader issues concerning user privacy and the handling of personal user information. The Committee did separately discuss [redacted] and [redacted] Despite having this discussion, the Committee remained unconcerned about the Company's fundamental business model of granting access to user data without users' consent. Instead, the Company's lone [redacted] highlighting how the Board was focused on containing the damage from a public relations standpoint rather than engaging in fundamental reform.

3. *The Board's Complete Abdication Of Its Duties Results In Regulatory Action Being Taken Against The Company*

416. The Board next met on September 6, 2018, with all directors present: Andreessen, Bowles, Chenault, Desmond-Hellmann, Hastings, Sandberg, Thiel,

Zients, and Zuckerberg. FB220-00025084. Bowles, [redacted] However, despite the fact that the [redacted] the September 2018 Board minutes do not indicate that Bowles gave ***any*** report regarding user privacy, or the fact that sharing data with developers without user consent violated the 2012 Consent Order.

417. Also at this meeting, the Board received a [redacted] But even in the face of [redacted], the Board still offered no changes in the Company's policies to protect user information and did not question why the Company's fundamental business model included sharing data with developers without user consent.

418. A December 5, 2018 Audit & Risk Oversight Committee meeting agenda was produced (though the accompanying minutes were not). FB220-00024926. ***The Committee was given notice that*** [redacted]

[redacted] FB220-00024926 at FB220-00024928.

419. Despite these [redacted] which provided mounting evidence that management was responsible for a nearly decade-long illicit business plan, the Audit & Risk Oversight Committee showed no will to effect any substantive policy changes. Instead, the only action taken was more of the same: [redacted] FB220-00024926 at FB220-00024930-1.

420. Any doubt about the SEC's intent to prosecute Facebook's violations of the 2012 Consent Order were laid to rest on February 6, 2019, when the FTC sent [redacted] a preliminary complaint and proposed consent order, alleging violations of the 2012 Consent Order and naming both Facebook and Defendant Zuckerberg as defendants.[164] According to that version of the 2019 FTC Complaint, Defendant Zuckerberg was named because [redacted]

[164] *See generally* FB220-00016035.

[redacted] and [redacted] [redacted][165]

421. The next meeting of the Audit & Risk Oversight Committee was on February 13, 2019. FB220-00025065. Committee members Andreessen, Bowles, Chenault, and Zients attended, as well as director Desmond-Hellmann. By this point, the Chair had rotated from Bowles to Zients, who had been appointed in May 2018. The committee focused on [redacted] In addition, the committee received a [redacted] Any steps the Company may have taken to [redacted] were not described with any detail in the minutes. The Committee also [redacted]

422. The February 13, 2019 Audit & Risk Oversight Committee meeting continued to indicate, [redacted]

[165] FB220-00016039 at 16073.

[redacted] that no concrete action would be taken to ensure that the Company had ceased its illicit business practices and was in compliance with the 2012 Consent Order. The minutes contain no discussion of the Company having valid defenses to the FTC's financial penalty, implicitly admitting that the Company's fundamental business model violated the 2012 Consent Order, and so focused on [redacted] Yet the Committee did not inquire further into Facebook's sharing of personal information without consent, condoning this business model without reform and seeking only minor therapeutic changes, if any.

423. The full Board met on March 19, 2019, to discuss [redacted] FB220-00025593. All directors were present: Andreessen, Bowles, Chenault, Desmond-Hellmann, Hastings, Thiel, Zients, and Zuckerberg. The Board received [redacted] FB220-00025593 at FB220-00025594. At the conclusion of the meeting [redacted]

[redacted] FB220-00025593 at FB220-00025595. Thus, despite being on clear notice that [redacted] ***the Board's primary concern was protecting Zuckerberg from personal liability***.

424. On March 26, 2019, the full Board met again, with Bowles absent, and Andreessen, Chenault, Desmond-Hellmann, Hastings, Thiel, Zients, and Zuckerberg present. FB220-00025597. The meeting was to discuss the [redacted] The Board was informed that [redacted] The Board was also apprised of [redacted] The Board [redacted]

[redacted]

$3 billion was over 30 times the Company's maximum liability under the terms of the 2012 Consent Order.

425. On March 26, 2019, [redacted][166] Zuckerberg's [redacted] clear priority to benefit himself at the expense of the Company. The Director Defendants were therefore disloyal to the Company in failing to conduct any serious investigation to find the culpable executives responsible for Facebook's illegal business plans, and in further failing to ensure that a truly independent body was able to negotiate and settle the FTC's enforcement action against the Company outside of Zuckerberg's personal concerns.

426. The Special Committee was not truly independent because, as alleged *infra* ¶¶428-58, it repeatedly allowed Defendant Zuckerberg to taint the discussion

[166] *See generally* FB220-00027656.

and impute his influence on the Special Committee by allowing him to participate in meetings and [redacted]

427. The full Board met again on March 30, 2019, with directors Andreessen, Bowles, Desmond-Hallman, Sandberg, Thiel, Zients, and Zuckerberg in attendance, and Hastings absent. FB220-00025602. The meeting was devoted to the [redacted], where the Board heard again that the [redacted] The minutes note that [redacted]

4. *The Board's Fealty To Zuckerberg Clouds The Company's Response To The FTC's Settlement Demands*

428. At the March 30, 2019 meeting, the Board was informed that the [redacted]

[redacted] The [redacted] The Board then held a discussion on [redacted] ***The Board therefore did not seriously discuss privacy oversight as an option during FTC settlement negotiations until it knew this oversight could be used to prevent Zuckerberg from being held personally liable for the infringements identified by the FTC***.

429. Finally, at the March 30, 2019 meeting, Desmond-Hellmann [redacted]

430. The Special Committee held its first meeting on April 5, 2019, where directors Andreessen, Chenault, Zients, Desmond-Hellmann, and Bowles (the latter two attending by invitation and the former three constituting the Committee) received an [redacted]

[redacted] FB220-00025565.

431. The Special Committee met again on April 7, 2019, again with Andreessen, Chenault, Zients, Bowles, and Desmond-Hellmann in attendance. FB220-00025567. The meeting focused on [redacted] ***The Board heard that the*** [redacted] FB220-00025567 at FB220-00025568.

432. The Special Committee met the next day, on April 8, 2019, including attendees Andreessen, Chenault, and Zients. FB220-00025570. Desmond-Hellmann and Bowles did not attend. ***After having just heard about the*** [redacted]**,** ***however, the Special Committee allowed Zuckerberg to attend this meeting, and failed to hold an executive session where actions beneficial to the Company could be discussed independently from Zuckerberg***. Chenault then informed the Special Committee that they would discuss [redacted]

[redacted]

433. The Special Committee met again the next day, on April 9, 2019. FB220-00025573. Andreessen, Chenault, Zients and Bowles attended, as well as Zuckerberg and Sandberg. The Special Committee was informed [redacted]

[redacted] and the meeting appeared to close with no further discussion.

434. On April 10, 2019, the Special Committee again met, with Andreessen, Chenault, Zients, Bowles, and Desmond-Hellmann in attendance. FB220-00025576. Zuckerberg and Sandberg also attended. [redacted] informed the Special Committee that [redacted] This was the report prepared by PwC discussed *supra* ¶¶320–21, finding, *inter alia*, that Facebook's privacy controls were not operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information.

435. Additionally, at the April 10, 2019 meeting of the Special Committee, the Special Committee was informed [redacted] The Special Committee was also informed that ***the*** [redacted]

[redacted]

436. The Special Committee next met on April 11, 2019. FB220-00025579. Andreessen, Chenault, Zients, Bowles, and Desmond-Hellmann attended. Zuckerberg and Sandberg also attended. [redacted] informed the Special Committee that [redacted]

437. On April 15, 2019, the Special Committee again met, with Andreessen, Chenault, and Zients attending. FB220-00025582. The meeting was in between a Board meeting on April 15, 2019. [redacted] The Special Committee also resolved and [redacted] FB220-00025582 at FB220-

00025583. The Special Committee again met on April 25, 2019, with Andreessen, Chenault, Zients, Bowles, and Hastings in attendance, and with Zuckerberg and Sandberg also in attendance. FB220-00025588. The meeting's purpose was to discuss a [redacted] presentation distributed beforehand. In the presentation, [redacted]

438. The Special Committee then listened to [redacted] and it discussed [redacted] ***discussed with the Special Committee that*** [redacted] FB220-00025588 at FB220-00025590. The Special Committee requested the [redacted] The Special Committee also discussed, after Zuckerberg and Sandberg left, [redacted]

[redacted]

439. The next meeting of the Audit Committee, on April 23, 2019 was attended by Committee members Andreessen, Bowles, Chenault, and Zients. FB220-00025077. No other directors were present. The Committee [redacted] The Committee knew that [redacted] The Committee also received [redacted] (emphasis in original).

440. Furthermore, the Committee received an update [redacted] ***The Committee also discussed*** [redacted] ***They further discussed*** [redacted] It is reasonable to infer that the prior

SOC reports were not sufficiently capturing the Company's privacy violations given the foregoing, so that the foregoing indicates that future SOC reports would need to be expanded and/or modified to actually capture whether the Company complied with its purported privacy controls. Finally, the Committee heard a presentation on [redacted] and discussed [redacted]

441. Despite the focus on the FTC's investigation and settlement terms, the Audit Committee still did not appear to question the basic business model of the Company, which entailed sharing user data with developers without the users' consent, even though the minutes indicate that [redacted]

442. The accompanying Committee presentation noted that [redacted] FB220-00025008 at FB220-00025012. ***The Committee estimated that*** [redacted] ***The presentation also noted,*** [redacted] However, the Committee presentation did not indicate the Committee was considering any

reforms, but rather it [redacted]

443. The Audit & Risk Oversight Committee met again on May 17, 2019, as negotiations with the FTC reached the end stage. FB220-00025082. Committee members Andreessen, Bowles, Chenault, and Zients attended, along with directors Desmond-Hellmann and Thiel. The committee discussed [redacted] The assessment, referenced *supra* ¶¶320–21, found that Facebook's privacy controls were not effective, and more specifically, that management's control was not appropriately designed and implemented to address intake, detection, handling, response, remediation, and reporting for all privacy incidents. There is no indication that the Audit & Risk Oversight Committee actually reviewed either draft or final versions of the 2019 PwC Assessment. Instead, the committee heard a [redacted] FB220-00025082 at FB220-00025083. The directors then discussed [redacted]

444. At the May 17, 2019 meeting, the Audit & Risk Oversight Committee also discussed [redacted] as well as [redacted] Thus, the minutes reflect, as they did in the April 2019 minutes, that the Committee was on notice that the Company's platform and data use practices violated the 2012 Consent Order.

445. On May 30, 2019, the full Board met. FB220-00025614. The directors present were Alford, Andreessen, Desmond-Hellmann, Sandberg, Zients, and Zuckerberg. Chenault and Thiel were absent. The Board received and discussed [redacted] The Board also received and discussed [redacted] The Board also received an update of [redacted]

446. Furthermore, at the May 30, 2019 meeting, ***the Board heard from*** [redacted] FB220-00025614 at FB220-00025618. One of the executives then [redacted] ***The Board, having had at least several months to absorb the gravity of the Company's nearly decades-long privacy violations, the FTC's insistence on*** [redacted]***, and the FTC's earlier insistence of*** [redacted]***, allowed Zuckerberg to staff, craft and oversee the implementation of the Company's supposed privacy programs***.

447. In the accompanying Board materials dated May 30, 2019, the agenda noted that the [redacted] FB220-000025174. The agenda also noted that the [redacted] the day before. However, in the May 30, 2019 Board minutes provided to Plaintiffs, the entirety of the presentation from Audit & Risk Oversight Committee to the Board was redacted for responsiveness, indicating that these issues were not put before the Board. FB220-00025614 at FB220-00025615. The Board therefore knew that the Audit & Risk Oversight Committee

had discussed developments for both the ongoing SEC and FTC inquiries into the Company's privacy practices, as well as the adverse 2017-2019 PwC privacy assessment, but failed to discuss or inquire into these issues.

448. The Board at the May 30, 2019 meeting also received an update from [redacted], which summarized the [redacted] The [redacted]

449. A later, June 10, 2019 presentation from the Compensation & Governance Committee indicated that the Compensation & Governance Committee [redacted] FB220-00027011 at FB220-000270033. However, to date, the Board has yet to [redacted] This reticence to implement the corporate governance reforms requested by the FTC is both unsurprising and inexcusable at this late date.

450. The same June 10, 2019 presentation indicates that [redacted] However, the changes again are cosmetic and do nothing to rectify the Company's oversight failures, due in large part to a lack of independence from Zuckerberg. The

Compensation, Nominating & Governance Committee was given the power to recommend nominees to the Board. However, Zuckerberg retained through his absolute voting power the ability to veto any candidate, effectively allowing him to choose who the Company's directors will be. In addition, as of May 11, 2020, the three members of the Compensation, Nominating & Governance Committee are Andreessen and Thiel, the longest-serving directors, who were both early investors in Facebook, and Houston, Zuckerberg's close friend that he nominated to the Board, and these directors have the most personal and professional ties to Zuckerberg.

451. In effect, Zuckerberg retains his control over nominations as well as the power of the veto, because he has the absolute voting power to veto any candidate, as well as the two directors with the closest personal and professional ties to him serving as the sole Board members able to nominate future candidates.

452. On June 12, 2019, the Special Committee met to [redacted] with Andreessen, Chenault and Zients in attendance. FB220-00027245. The substantive discussion was redacted for privilege, and the Special Committee concluded that it [redacted]

453. On June 12, 2019, the full Board met, with Alford absent and Andreessen, Chenault, Desmond-Hellmann, Sandberg, Thiel, Zients, and Zuckerberg present. FB220-00027291. The meeting was to discuss the [redacted] The Board was informed that in addition to the issues that had been previously discussed, the [redacted] The Board was also apprised of [redacted] that the FTC proposed settlement be approved, and the Board voted in favor unanimously.

454. Even in approving the Settlement, the Board was apprised of a red flag, because it found out that yet another area of the Company's business—regarding its facial recognition technology—violated the 2012 Consent Order, and it was an issue that was flagged very recently. Yet in the almost one year since the FTC Settlement, the Board has shown no appetite to examine the Company's illegal business model of sharing data with developers without user consent, reform the governance structures allowing such rampant illicit activity to persist, nor to establish independent oversight regarding the same. Instead, as of May 11, 2020, Facebook has yet to implement the new Privacy Committee contemplated by the Settlement.

455. A July 23, 2019 Audit & Risk Oversight Committee presentation discussed the [redacted] FB220-00026953. It also notes that [redacted] ***Facebook also acknowledged*** [redacted]

456. Moreover, the while the FTC ultimately approved the settlement it was not without criticism of Facebook's unqualified, uninformed and zealous defense of Zuckerberg. For example, two of the five FTC Commissioners—specifically,

Commissioners Chopra and Slaughter—to dissent from the settlement and publicly criticized the 2019 Consent Order.[167]

457. Specifically, Commissioner Chopra:

- Lamented the "unusual legal shield" the settlement gave Defendant Zuckerberg, noting the "deeply problematic" "blanket release" for all claims that the FTC might have otherwise been able to bring against Facebook's officers and directors for conduct prior to June 12, 2019.[168]

- Explained that "when individuals make calculated decision to break or ignore the law, they—and not just their firm or shareholders—should be held liable. To instead expressly shield individuals from accountability is dubious as a matter of policy and precedent."[169]

- Noted that the "grant of broad immunity is highly unusual" and "is a departure from FTC precedent and established guidelines. Americans should ask why Mark Zuckerberg, Sheryl Sandberg, and other executives are being given this treatment, while leaders of small firms routinely face investigations, hearings, and charges."[170]

---

[167] *See* Rebecca Kelly Slaughter, *Dissenting Statement of Commissioner Rebecca Kelly Slaughter, In the Matter of FTC vs. Facebook, Office of the Commissioner*, F.T.C. (July 24, 2019) ("Slaughter Dissent"), *available at*: https://www.ftc.gov/system/files/documents/public_statements/1536918/182_3109_slaughter_statement_on_facebook_7-24-19.pdf; Rohit Chopra, *Dissenting Statement of Commissioner Rohit Chopra, In the Matter of FTC vs. Facebook, Office of the Commissioner*, F.T.C. (July 24, 2019) ("Chopra Dissent"), *available at*: https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

[168] Chopra Dissent, *supra* note 167, at 18.

[169] *Id*. at 19.

[170] *Id*.

- Noted that "the law imposes affirmative obligations on officers and directors whose firms are under order, uncovering their role in potential violations is critical to any investigation. It is especially critical to this investigation, which involved a firm that is tightly controlled by its founder, CEO, and Chairman, Mark Zuckerberg. Given the structure of his ownership and his special voting rights, it is hard to imagine that any of the core decisions at issue were made without his input. Whether Zuckerberg took all reasonable steps to ensure compliance with the 2012 [Consent Order] is an essential determination we should evaluate carefully before pursuing any resolution, including, for example, by thoroughly reviewing documents in his custody and examining him under oath."[171]; and

- Emphasized that, despite the unusual circumstances surrounding the FTC's investigation of Facebook and Zuckerberg, there was "already sufficient evidence, including through public statements, to support a charge against Mark Zuckerberg for violating the 2012 [Consent Order] . . . [T]he Commission had enough evidence to take . . . Zuckerberg to trial."[172]

458. Commissioner Slaughter echoed many of these concerns, noting:

- The "extremely compelling evidence of a series of significant, substantial [violations of the 2012 Consent Order] and law violations," including "sufficient evidence to name Mr. Zuckerberg in a lawsuit."[173]

- That she would "have preferred to name Mr. Zuckerberg in the complaint and in the [2019 Consent Order]." She

[171] *Id*. at 11–12.

[172] *Id*. at 12–13, 12 n.36

[173] Slaughter Dissent, *supra* note 167, at 6.

> "disagree[d] with the decision to omit him now, and [] strenuously objected to the choice to release him and all other executives from any potential liability for their roles to date." She further was "concerned that a release of this scope [was] unjustified by [the FTC's] investigation and unsupported by either precedent or sound public policy."[174]

5. *Zuckerberg And Sandberg Conduct A PR Campaign Outside Of The Board's Purview, Further Undermining The Company's Compliance Function*

459. Compounding the foregoing severe governance deficiencies, the Board was further prevented from effectively overseeing the Company because Zuckerberg and Sandberg were not forthcoming with relevant information to the Board. Outside of formal minutes, e-mail updates to the Board were limited to discussions of [redacted], while Zuckerberg and Sandberg conducted their own public disclosure campaigns with virtually no oversight.

460. Shortly before the full Board met regarding Cambridge Analytica, Sandberg was personally and solely directing, [redacted] and seeking to [redacted] FB220-00018381.

461. In the immediate aftermath of Cambridge Analytica, Sandberg and her staff made sure to update the Board on news coverage, with Facebook's internal summaries to color their views.

---

[174] *Id*. at 14.

a. On April 5, 2018, Elliot Schrage e-mailed the Board (Andreessen, Thiel, Koum, Hastings, Desmond-Hellmann, Bowles, Sandberg and Zuckerberg) to tell them about [redacted] thus trying to keep the Board focused on the [redacted] rather than broad misuse of user data. FB220-00010833. On the same day, Schrage also sent the Board another report with an [redacted] FB220-00010145.

b. On April 8, 2018, Schrage sent the Board an update on a CNBC story about [redacted] FB220-00010093. However, Schrage's focus showed that he wanted the Board to think of the problem as one limited to rogue developers rather than question the fundamental business model of Facebook.

c. On April 9, 2018, Sandberg sent a [redacted] to the Board, noting [redacted] FB220-00018973.

462. Despite how ill-informed the Board was by Zuckerberg and Sandberg, some of the directors were still alarmed by the information they did receive. For

example, on March 30, 2018, Chenault sent an e-mail to Sandberg regarding [redacted] [redacted] FB220-00021693. He wrote:

> Sheryl,
>
> [redacted]
>
> [redacted]
>
> [redacted]
>
> [redacted] Ken.

FB220-00021693 at FB220-00021694-95.

463. Sandberg responded that [redacted] *Id*. at FB220-00021694. Chenault responds, [redacted] *Id*. Sandberg responds, [redacted] *Id*. at FB220-00021693. Chenault was [redacted] Sandberg, however, and responded, [redacted] *Id*.

464. Despite Chenault's [redacted] there are no further emails in the documents produced to Plaintiffs discussing the issue further with Zuckerberg or Sandberg.

465. Meanwhile, veteran directors with longer ties to Sandberg and Zuckerberg expressed sympathy, especially to Sandberg. Bowles, for example, appeared to forward [redacted] to Sandberg. In one exchange, an acquaintance told Bowles he [redacted]

[redacted] FB220-00009908.

466. Also, in the immediate aftermath of Cambridge Analytica, Bowles [redacted] an April 8, 2018 e-mail from Sandberg to Bowles expressed, [redacted] FB220-00014366.

467. Hastings, in text messages with Sandberg in November 2018, told her, [redacted] FB220-00024497. He also complained, [redacted] *Id*.

468. At the same time, ***Sandberg and Zuckerberg were aware that the practices Facebook engaged in violated the 2012 Consent Order. In a*** [redacted] ***she flagged a*** [redacted] FB220-00018210 at FB220-00018227. And in response to charges that Facebook ad targeting is discriminatory, she flagged, [redacted]

[redacted] *Id*. at FB220-00018217. In August 2018 correspondence regarding [redacted] Zuckerberg observed, [redacted] FB220-00022954.

469. Sandberg and Zuckerberg continued to be more concerned with their image rather than ensuring that Facebook's business practices were within the bounds of the law. For instance, in an April 14, 2018 e-mail, Sandberg [redacted] FB220-00016338.

470. Zuckerberg and Sandberg also flagged that he wanted to avoid as much self-finger-pointing as possible. Regarding a [redacted], Sandberg noted, [redacted] FB220-00010582. She noted, [redacted] *Id*.

471. And in December 2018, regarding [redacted]

Zuckerberg noted to Nick Clegg, [redacted] FB220-00003836.

472. ***Sandberg also offered to*** [redacted] FB220-00012972.

473. Zuckerberg especially wanted to avoid having to [redacted] In March 28, 2018 correspondence regarding [redacted] Sandberg reported to Christopher Cox, Facebook's Chief Product Officer, that [redacted] FB220-00018378 at FB220-00018378-9.

474. Sandberg's team considered it to be a victory when they got the [redacted] FB220-000008135.

475. Moreover, Zuckerberg tried to limit damage in testimony he gave. For instance, in June 2018, he asked his policy team (with Sandberg copied), [redacted]

[redacted] FB220-00017761. Joel Kaplan, Facebook's lobbying chief, responded, [redacted] *Id.*

476. Sandberg and Zuckerberg's public relations push was so intense that less than a month after the Cambridge Analytica scandal broke, a Facebook employee told Sandberg and other executives or branding employees, [redacted] FB220-00018529. She further noted, [redacted] *Id.*

477. In a June 24, 2018 e-mail, Sandberg reported to a cohort of officers and Zuckerberg, ***but not to the Board***, [redacted] FB220-00021107. She observed that ***with respect to*** [redacted]

[redacted] *Id*. at FB220-00021109.

478. ***Sandberg also*** [redacted] and moreover, [redacted] *Id*.

479. In December 2018, the pace of privacy scandals was so overwhelming that [redacted] a *Business Insider* article stating, [redacted] FB220-00003142. The article is entitled, "Facebook's big new problem: it's so mired in grubby privacy scandals, people confuse legit data deals with bad breaches." *Id*. One Facebook

employee, Carolyn Everson, replied, [redacted] *Id*.

480. Sandberg also kept herself apprised of the business impact of the Cambridge Analytica scandal, monitoring Facebook deactivation and deletions, and commenting on how [redacted] FB220-00018495. Schrage noted to Sandberg and her team members [redacted] FB220-00016336.

481. Sandberg and Zuckerberg, as part of Facebook's leadership team, also received a briefing in mid-April, [redacted] FB220-00010765. The report noted, [redacted] *Id*.

482. Zuckerberg also maintained interest in the business impact and the impact on stock price. In evaluating the FTC settlement offer in the wake of news of a potential $3–$5 billion settlement with the FTC, ***Zuckerberg and Sandberg received a debrief*** [redacted] FB220-00016402.

V. INSIDER TRADING ALLEGATIONS

483. Instead of providing the market with correct information, as they were obligated to do under their duties as fiduciaries of the Company, the Insider Trading Defendants used their knowledge of Facebook's material, non-public information to

sell their personal holdings[175] while they knew the Company's stock was artificially inflated during the Relevant Period (June 26, 2013 through July 23, 2019). As officers and directors of Facebook, the Insider Trading Defendants were privy to material, non-public information about the true state of Facebook's business and operations.

A. Mark Zuckerberg

484. While Defendant Zuckerberg was in possession of adverse material non-public information about the true state of Facebook's business and operations, including Facebook's misrepresentations as to its users' purported ability to control the sharing of their personal information and the Company's non-compliance with the FTC Consent Order, entities affiliated with and controlled by Zuckerberg sold more than ***84.9 million shares*** of Facebook stock during the Relevant Period for proceeds of more than ***$9.6 billion*.** On December 26, 2013, Zuckerberg sold 41.35

[175] Senior executives and certain directors at Facebook received of Reserve Stock Units ("RSUs"), which were convertible 1:1 into Facebook Series B stock, and which in turn were convertible 1:1 into Facebook Series A stock. Series B and RSU holdings were reported in Forms 4 as derivatives of the common equity, Series A. The calculations of the percentages of stock sold during the Class Period take into account holdings and dispositions of Series A stock, plus the amount of Series B stock and RSUs that remained unconverted at the end of the last Form 4 for each officer or director.

million shares of stock in a secondary offering for total proceeds of $2.276 billion. Afterwards, he sold no more shares until August 2016.

485. By then, 99% of Zuckerberg's stock holdings—more than 418 million shares—had been placed in the Chan Zuckerberg Initiative, LLC ("CZI"), later renamed CZI Holdings LLC, which was created in December 2015. Although purportedly established for charitable purposes, CZI was structured as a limited liability company, enabling it to avoid having to distribute 5% annually of the value of its endowment for charitable purposes, as is typically required for a nonprofit. Also, the LLC structure allows Zuckerberg to control the voting of and the disposition of any shares held by the entity, and to use the entity to make political donations—all without the disclosure required for a nonprofit. In essence, Zuckerberg "remains completely free to do as he wishes" with the entity and its stock holdings.

486. As stated in Facebook's December 1, 2015 Form 8-K, when Zuckerberg created CZI, he "plan[ned] to sell or gift no more than $1 billion of Facebook stock each year for the next three years" and "intends to retain his majority voting position in our stock for the foreseeable future." But after Zuckerberg learned of Cambridge Analytica's massive extraction of Facebook user data, he and the entities controlled by him significantly accelerated his sales of Facebook shares, selling 18,755,276 shares for proceeds of $2,828,482,748 during the August 17,

2016 to March 16, 2018 period (just before *The New York Times* published its exposé revealing that Cambridge Analytica had extracted Facebook user data), and selling another 23,469,497 shares for proceeds of $4,334,752,914 between March 19 and August 30, 2018. Zuckerberg and his controlled-entities thereafter sold a further 1,296,322 shares for $230,456,530 between April 3 and April 18, 2019.

487. Overall, during the Relevant Period, Zuckerberg and entities he controls sold 84,971,095 shares of Facebook stock, for total proceeds of ***$9,670,019,692***. Although Zuckerberg continued to control more than 376 million shares, the vast dollar amount of his sales and their timing make them highly suspicious.

B. Sheryl Sandberg

488. Defendant Sandberg also sold massive amounts of Facebook stock during the Relevant Period while in possession of material adverse information concerning the company. From July 10, 2013 to July 10, 2019, Sandberg sold 18,107,425 of the shares that she owned either directly or were held in family trusts, reaping proceeds of more than ***$1.6 billion***. These sales represented 73.85% of Sandberg's total beneficially owned Facebook stockholdings during the Relevant Period. Facebook also "withheld" another 476,906 shares (with a value of $77,196,800) to pay withholding taxes for Sandberg's benefit. Sandberg also gifted 400,000 shares to an unnamed entity or person, transferred a further 1,804,200 shares

to an unspecified entity "for estate planning purposes," and conveyed 2,011,700 shares to the "Sheryl Sandberg & David Goldberg Family Fund, a donor advised fund."

489. The stock sales and transfers made by Zuckerberg and Sandberg around the time when the Cambridge Analytica scandal broke received notice in the press. For example, as *CNBC* reported on March 18, 2018: "During the months preceding Facebook's disclosure of the Cambridge Analytica security breach, [Facebook] executives [were] selling shares like crazy." *CNBC* also reported two days later, that, "[i]n the two weeks before Facebook's recent struggles, Zuckerberg sold 1.14 million shares as part of regularly scheduled programs. ***That was the most insider selling for any public company, going back as far as three months*** . . . ." Although it was reported that Zuckerberg sold more stock "than any insider at any other company" during the three-month period prior to the disclosure of the data security, *CNBC* also noted on March 18, 2018 that "Sandberg sold over $300 million [in 2017], which pales in comparison to her colleagues, but is still is unusually large among officers of top tech companies." The article added: "Facebook is facing real problems. ***Instead of giving answers to those problems, top execs are selling, spinning and staying silent***."[176]

176 *Id.*

C. Jan Koum

490. Defendant Jan Koum, the founder and CEO of WhatsApp before its sale to Facebook, served as a Facebook director from October 2014 until May 2018. According to press reports, Koum resigned as a Facebook director because he clashed with Zuckerberg and others over Facebook's strategy and Facebook's attempts to use its personal data and weaken its encryption. Nonetheless, while having these concerns and with the benefit of his access to material adverse inside information about the Company, Defendant Koum and a family trust that he controlled sold huge amounts of Facebook common stock. For example, between November 16, 2015 and May 16, 2018, trusts controlled by Koum sold 60,458,555 shares, for total proceeds of ***almost $8 billion ($7,928,739,230)***. Among these sales were the following: between April 28, 2017 and April 30, 2018 (when Koum's plan to resign was publicly disclosed) Koum's trusts sold 15,436,644 shares for total proceeds of ***over $2.55 billion*** ($2,554,457,484). Koum's trusts made further sales of another 1,253,111 shares on May 16, 2018 for more than ***$229 million***. Overall, Koum sold 62.74% of his trust's stock holdings during the Relevant period, while he was aware of Facebook's financial exploitation of its users' personal information for profit.

D. Marc Andreessen

491. Defendant Marc Andreessen has been a Facebook director throughout the Relevant Period. From November 8, 2013, through November 9, 2017, Andreessen, the "Andreessen 1996 Living Trust," and various investment LLCs in which Andreessen was a managing member sold 6,484,996 shares of Facebook stock for total proceeds of ***over $454 million***. Overall, Andreessen and his affiliated entities sold approximately 63% of their stockholdings during the Relevant Period—and his affiliated LLCs also distributed more than 3.3 million shares to their investors (net of distributions to other entities affiliated with Andreessen). These sales were unusually large and suspicious in their timing. For instance, over the course of just four days—November 9 to November 12, 2015—Andreessen sold over $63.5 million worth of Facebook common stock alone.

E. Peter Thiel

492. Defendant Peter Thiel has been a Facebook director throughout the Relevant Period. Throughout the Relevant Period, Thiel, through a limited liability company that he beneficially owned, and certain investment funds that he managed, collectively sold 3,048,650 shares of Facebook stock for proceeds of over ***$308.6 million***. Overall, Thiel and his controlled entities sold 97.56% of his Facebook stock holdings during the Relevant Period. Thiel's transactions were unusually large and suspect in their timing, including large sales of the majority of his holdings on

August 13, 2015 (over $100 million in sales), May 4, 2016 (over $101 million in sales), and November 21, 2017 (over $28 million in sales), each made while he was in possession of material nonpublic information concerning the Company's lack of protection for user information.

F. David Fischer

493. Defendant David Fischer served as Facebook's Vice President of Business & Marketing Partnerships and in April 2019 became Facebook's Chief Revenue Officer. During the Relevant Period, Fischer sold 1,884,025 shares of Facebook stock for total proceeds of ***over $174 million***. These sales represented about 84% of Fischer's entire stock holdings during the Relevant Period. Facebook withheld a further 288,188 shares (valued at over $48 million) in payment of withholding taxes for Fischer's benefit. Fischer's sales were suspicious in their timing and amount. For instance, Fischer sold 50,533 shares of Facebook stock on August 14, 2017, constituting $8,588,083 and 40% of his holdings at the time. Fischer again sold 61,103 shares of Facebook stock on August 31, 2018, constituting $10,766,947 and 62% of his then current holdings. These large sales were unusually large, atypical, and suspicious in their timing as they occurred shortly after *The New York Times* revealed that Cambridge Analytica had extracted Facebook user data and public scrutiny on the Company's data practices increased. In all, Fischer sold roughly 84.4% of his stock during the Relevant Period.

G. Michael Schroepfer

494. Defendant Schroepfer served as Facebook's Chief Technology Officer throughout the Relevant Period. During the Relevant Period, he and family trusts controlled by him sold 4,393,665 shares of Facebook stock for proceeds of ***over $425.9 million***. These shares represented 55.75% of his total beneficially owned stock holdings during the Relevant Period. Schroepfer also gifted a further 1,375,406 shares, and Facebook "withheld" a further 690,220 shares (valued at over $113 million) in payment of withholding taxes for Schroepfer's benefit.

H. David Wehner

495. Defendant Wehner served as Facebook's CFO beginning June 1, 2014. From August 15, 2014 through the end of the Relevant Period, Wehner sold a total of 475,622 shares for proceeds of over ***$63 million***. These shares represented approximately 69% of his total stock holdings, those of his wife and those of a personal trust during the Relevant Period. Wehner also transferred 45,894 shares in transactions that were exempt from reporting requirements under Section 16 of the Securities Exchange Act of 1934. In addition, Facebook "withheld" 194,814 shares (valued at over $32.5 million) in payment of withholding taxes for Wehner's benefit.

496. In sum, in breach of their fiduciary duties, and while in possession of material adverse information, the Insider Trading Defendants collectively sold the

staggering total of ***over $20.6 billion*** worth of Facebook stock at artificially inflated prices.

VI. CONTROL ALLEGATIONS

A. Zuckerberg Has Majority Voting Control Of Facebook Despite Holding A Minority Economic Interest

497. Since the Company's initial public offering ("IPO") in 2012, Zuckerberg has maintained control of the Company by means of Facebook's dual-class stock structure. Facebook's Class A Stock is entitled to one vote per share while Facebook's Class B common stock ("Class B Stock"), is entitled to ten votes per share. The Class B Stock is thus able to exert outsized influence when both classes of stock vote together as they are generally required to, under Section 3.2 of Facebook's Restated Certificate of Incorporation, including in elections of directors.

498. After the IPO, Zuckerberg held 57.6% of Facebook's voting control. Specifically, Zuckerberg held (i) 503,601,850 shares of Class B Stock, representing 32.2% of the outstanding Class B Stock and 30.9% of the voting power outstanding, (ii) irrevocable proxies for 7,125,242 shares of Class A Stock and (iii) 432,682,785 shares of Class B Stock, which added an additional 27.6% to Zuckerberg's voting power.

499. As described in Facebook's Registration Statement filed as part of its IPO:

> ***Our CEO has control over key decision making as a result of his control of a majority of our voting stock.***
>
> As a result of voting agreements with certain stockholders, together with the shares he holds, ***Mark Zuckerberg, our founder, Chairman, and CEO, will be able to exercise voting rights with respect to an aggregate of 879,062,051 shares of common stock, which will represent approximately 55.8% of the voting power of our outstanding capital stock following our initial public offering. As a result, Mr. Zuckerberg has the ability to control the outcome of matters submitted to our stockholders for approval, including the election of directors*** and any merger, consolidation, or sale of all or substantially all of our assets. This concentrated control could delay, defer, or prevent a change of control, merger, consolidation, or sale of all or substantially all of our assets that our other stockholders support, or conversely this concentrated control could result in the consummation of such a transaction that our other stockholders do not support. . . . In addition, ***Mr. Zuckerberg has the ability to control the management and major strategic investments of our company as a result of his position as our CEO and his ability to control the election or replacement of our directors***. . . . As a stockholder, even a controlling stockholder, Mr. Zuckerberg is entitled to vote his shares, and shares over which he has voting control as a result of voting agreements, in his own interests, which may not always be in the interests of our stockholders generally.

500. After the IPO, Facebook stock traded on NASDAQ. Before the IPO, however, Facebook's Board had employed the Company's status as a controlled company (*i.e.*, one with a controlling stockholder) to excuse its compliance with certain NASDAQ requirements, namely the requirement for a majority-independent board and an independent director-nomination process. While Facebook claims that its Board is majority-independent, as described below, that is not the case.

501. Facebook's 2020 Proxy Statement reiterates his control over Facebook insofar as it states:

> Because Mr. Zuckerberg controls a majority of our outstanding voting power, we are a "controlled company" under the corporate governance rules of the NASDAQ Stock Market LLC (NASDAQ). Therefore, we are not required to have a majority of our board of directors be independent, nor are we required to have a compensation committee or an independent nominating function. In light of our status as a controlled company, our board of directors has determined not to have an independent nominating function and to have the full board of directors be directly responsible for nominating members of our board.[177]

502. Indeed, Zuckerberg has historically prioritized maintaining his control of the Company and advancing his own personal interests over those of the Company. Zuckerberg has explained that "hav[ing] voting control of the company, [is] something I focused on early on. And it was important because, without that, there were several points where I would've been fired."[178]

---

[177] Facebook Inc., Form DEF14A, at 14 (Definitive Proxy Statement) (April 10, 2020), *available at:* https://www.sec.gov/Archives/edgar/data/0001326801/000132680120000037/facebook2020definitiveprox.htm.

[178] Casey Newton, *Read The Full Transcript Of Mark Zuckerberg's Leaked Internal Facebook Meetings*, THE VERGE (Oct. 1, 2019), *available at*: https://www.theverge.com/2019/10/1/20892354/mark-zuckerberg-full-transcript-leaked-facebook-meetings.

B. The Failed Reclassification

503. Although Zuckerberg had voting control after the IPO, it was widely anticipated that Zuckerberg's control would diminish to the point he no longer had a majority vote. In 2010, Zuckerberg had signed the Giving Pledge, declaring he would give away at least half of his wealth during his lifetime or in his will. Zuckerberg intended to begin his giving early, with the pledge letter from Zuckerberg and his wife stating "[w]e believe passionately that people should not wait to give back."

504. But Zuckerberg's plan to sell his Facebook holdings came with the concomitant problem of selling his control. By 2015, after sales of Class B stock by Zuckerberg and others, Zuckerberg held 53.8% of Facebook's voting power. Zuckerberg asked Facebook's legal department about this and learned that he could only sell $3-$4 billion in his stock before losing majority voting control.

505. On June 9, 2015, Zuckerberg sent an e-mail to the Board, stating:

> I am planning on significantly ramping up my personal philanthropy soon, and leading up to that I will begin selling some of my stock. This is relevant for our corporate governance because these sales will reduce my voting percentage over time. Given my desire to increase my philanthropy, I would like to begin a discussion with the board as to what my stock sales may mean for Facebook and how we can best position the company for continued success. I look forward to discussing this in greater detail.

506. Zuckerberg made his formal proposal to the Board during an August 20, 2015 meeting, proposing that Facebook issue to its existing stockholders new non-voting stock (the "Reclassification"). In response the Board established a special committee, comprised of Desmond-Hellmann, Andreessen and Bowles.

507. The special committee for the Reclassification was a sham from the start. For example, the special committee was required to prepare a formal charter delineating its duties and responsibilities but it never did.[179] The special committee also selected and hired legal and financial advisers without ever having met them.[180] According to the special committee's lead banker, they were hired "in the second inning," after the transaction was already well under way.[181] Meanwhile, another financial advisor later hired by the special committee had previously served as Defendant Zuckerberg's ***personal*** financial adviser on the very same transaction.[182] That financial advisor then used work product created by private counsel to Defendant Zuckerberg to prepare its analysis and recommendation.[183]

---

[179] *Facebook Class C Shares Litigation*, *supra* note 10, at 5.

[180] *Id*. at 5–6.

[181] *Id*. at 6.

[182] *Id*.

[183] *Id.*

508. Given that background, it was clear from the outset that the special committee always anticipated that reclassification would take place.[184] Deliberations were focused "less on whether to pursue a reclassification or propose an alternative and more on the details of the reclassification that Zuckerberg wanted."[185] Indeed, after Defendant Zuckerberg rejected two of the special committee's proposed concessions, the special committee did not ask any further questions "about the concessions that Zuckerberg had rejected; it simply accepted Zuckerberg's position."[186] The special committee was so dysfunctional that it did not even seek to negotiate or demand money, or some differential distribution for minority shareholders, in return for giving up concessions or otherwise handing Defendant Zuckerberg lifetime control of Facebook.[187] According to Defendant Desmond-Hellmann, the reason for this behavior was because "the [c]ommittee believed that it had no real ability to say 'no' to Zuckerberg."[188]

509. Meanwhile, throughout the process, Defendant Andreessen acted as a mole for Defendant Zuckerberg, providing him private details about the committee's

---

[184] *Id*. at 5.

[185] *Id*.

[186] *Id*. at 7.

[187] *Id*. at 8.

[188] *Id*. at 13-14, 16.

discussions, "coach[ing]" him on how to address the committee, and "repeatedly reassure[ing] [him] . . . that the Committee would ultimately agree to the reclassification."[189] And then when special committee met to vote on whether to recommend the reclassification to the full Board, Defendants Zuckerberg and Thiel were allowed to attend.[190]

510. Although the special committee was still considering Zuckerberg's proposal, on November 30, 2015, Zuckerberg and his wife publicly posted a letter to their newborn daughter, wherein they stated they will donate 99% of their Facebook shares, valued at $45 billion, away during their lifetimes. Zuckerberg seemed to have no doubt that the Reclassification would be approved by the Board.

511. On April 14, 2016, the Board approved the Reclassification requested by Zuckerberg. Under the terms approved by the Board, a new class of non-voting

---

[189] *Id.* at 31. *See also id.* at 9–10 (discussing "Andreessen Back-Channels Information To Zuckerberg," including how Defendant Andreessen told Defendant Zuckerberg that "senior staff thinks this is a big mistake" and that they "wish you would stop but don't want to challenge you."). *See ZeniMax Media Inc. et. al. v. Oculus VR Inc et. al.*, 3:14-cv-01849-K, Exhibit 2 to Plaintiff's Motion To Compel, at 2 (N. D. Tex. Dec. 27, 2016) (Dkt. # 824-2) (filing Class C share text messages and special committee meeting board minutes as exhibits in a case concerning allegations that Oculus infringed on ZeniMax's intellectual property, wherein in the messages, Andreessen wrote Zuckerberg on February 11, 2016 that "Between us—re special board session [ ] new share class will happen . . . .") (hereinafter "ZeniMax").

[190] *Facebook Class C Shares Litigation*, *supra* note 10, at 10.

common stock, the Class C stock, was authorized, with two Class C shares to be issued as a dividend for each Class A and Class B share. According to the Company, the Reclassification was "designed to create a capital structure that will, among other things, allow us to remain focused on Mr. Zuckerberg's long-term vision for our company and encourage Mr. Zuckerberg to remain in an active leadership role at Facebook."

512. The certificate amendment to approve the Class C shares was expected to be approved by Zuckerberg, as Facebook's controlling stockholder, at its annual meeting on June 20, 2016. On June 21, 2016, Facebook announced that the Reclassification had been approved by stockholders, with 5.1 billion votes in favor, 1.5 billion votes against, and 1.2 billion votes abstaining. Not counting Zuckerberg's votes, there were only 453 million votes in favor of the Recapitalization, and 1.5 billion votes against.

513. The Reclassification was put on hold after numerous stockholders filed lawsuits to block it. Ultimately, the Company abandoned it on the eve of trial.

C. Zuckerberg Controls The Stockholder Vote

514. As Facebook described Zuckerberg in its proxy statement filed with the SEC on April 12, 2019 (the "2019 Proxy"), "he is synonymous with Facebook." The 2019 Proxy further noted that Zuckerberg's role put him in a "unique" position due

to the "high-profile nature of being our founder, CEO, Chairman, and controlling stockholder."

515. According to Facebook's proxy statement filed with the SEC on April 10, 2020 (the "2020 Proxy"), as of March 31, 2020, Zuckerberg held 53.1% of Facebook's voting power (57.9% including shares for which he holds a proxy), despite holding only 12.9% of its stock. Only one other stockholder holds over 5% voting power (Eduardo Saverin at 6.8%), and large investment houses such as The Vanguard Group and BlackRock each hold less than 3% of Company voting power.

516. At Facebook's 2019 annual meeting, stockholders proposed changing the voting structure of Facebook stock to one share, one vote, noting that the Council for Institutional Investors and The International Corporate Governance Network have recommended a seven-year phase-out of dual class share offerings. Similar proposals had been made each year from 2014 through 2018.

517. In response, the Board stated: "Our board of directors believes that our capital structure contributes to our stability and insulates our board of directors and management from short-term pressures, which allows them to focus on our mission and long-term success." The proposal did not pass, but when the number of Zuckerberg-controlled votes is removed (assuming he voted against the proposal), the proposal was approved, garnering 82.4% of the votes cast.

Results of 2019 Stockholder Proposal Regarding Change in Stockholder Voting Structure, Without Zuckerberg Vote

Number of Votes		Percentage of Votes	
For	Against	For	Against
1,392,113,978	297,004,975	82.4%	17.6%

518. Also in 2019, four public pension funds and Trillium Asset Management proposed separating the role of the Chairman of the Board and CEO. New York City Comptroller Scott Singer, who manages one of the pension funds that sponsored the proposal, stated:

> Facebook plays an outsized role in our society and our economy. They have a social and financial responsibility to be transparent—that's why we're demanding independence and accountability in the company's boardroom.
>
> We need Facebook's insular boardroom to make a serious commitment to addressing real risks—reputational, regulatory, and the risk to our democracy—that impact the company, its shareowners, and ultimately the hard-earned pensions of thousands of New York City workers. An independent board chair is essential to moving Facebook forward from this mess, and to reestablish trust with Americans and investors alike.

519. While the proposal failed overall, a majority (67.4%) of Facebook's unaffiliated stockholders (*e.g.*, non-Zuckerberg-controlled votes) voted for the proposal.

Results of 2019 Stockholder Proposal Regarding an Independent Chair, Without Zuckerberg Vote

Number of Votes		Percentage of Votes	
For	Against	For	Against
1,139,241,589	550,953,033	67.4%	32.6%

520. Another 2019 stockholder proposal sought a requirement that there be a majority vote for uncontested director elections. As the stockholders proposing majority voting for uncontested director elections noted:

> Facebook operates essentially as a dictatorship. Mark Zuckerberg controls a majority of the votes using a multi-class share structure with unequal voting rights. Shareholders cannot call special meetings and have no right to act by written consent. A supermajority vote is required to amend certain bylaws. Our Board is locked into an out-dated governance structure that reduces board accountability to shareholders.

521. The proposal to require a majority vote for election of directors received similar support as the proposals for separating Chairman and CEO and to give all shares one vote, but this is not evidence of invariably obstinate minority stockholders. Stockholders roundly rejected other proposals regarding other matters, such as diversity.

522. The results of the 2019 stockholder meeting demonstrate Zuckerberg's dominance. Only 16.5% of non-Zuckerberg controlled voting power (the votes of shares he does not own directly or have proxy voting power over) voted to put Zuckerberg on the board of directors, yet he was reelected.

523. This was not the first time Zuckerberg failed to garner a majority of stockholder approval for his reelection to the Board. At the 2018 shareholder meeting, a majority of the minority shareholders (including all shares held by the

pension funds above) voted against the re-election of Defendant Zuckerberg and Defendant Sandberg. Yet both maintained their positions.

D. Zuckerberg Controls The Board Of Directors

524. Zuckerberg is the Chairman of the Board, presiding over all Board meetings. Unlike many companies, during the majority of the Relevant Period, Facebook's Board did not have a nominating committee, but instead ostensibly delegated director nominations to the whole Board. Zuckerberg controlled all director nominations and the stockholder vote on these nominations. This did not change despite the newly created Compensation, Nominating & Governance Committee, which Facebook was required to form as part of the 2019 Consent Order. Zuckerberg's control of the stockholder vote has resulted in a Board that is just a formality, as each director can be removed by Zuckerberg at his pleasure. As a result, and as alleged herein, any director who disagrees with Zuckerberg is forced to resign or decline further tenure at the Company.

1. *Zuckerberg Unilaterally Decided Facebook Would Acquire Instagram And Oculus*

525. In 2012, shortly before its IPO, Facebook acquired Instagram for $1 billion. But the acquisition was negotiated and agreed to by Zuckerberg almost

alone, with no Board involvement, in three days.[191] "By the time Facebook's board was brought in, the deal was all but done. The Board . . . '[w]as told, not consulted.'"[192] And while the Board technically had a vote on the acquisition, it was "largely symbolic."[193] Director Defendants Andreessen, Bowles, Hastings and Thiel were among the members of the Board that rubber-stamped Facebook's acquisition of Instagram.

526. The purchase of Instagram was not the only time Defendant Zuckerberg insisted the Board rubber-stamp a billion-dollar acquisition that he alone negotiated.[194] Defendant Zuckerberg similarly negotiated Facebook's purchase of Oculus VR for $3 billion by himself,[195] over the course of five days, and again sealed the deal at a private dinner with only him and Brendan Iribe present, the CEO and

---

[191] Shayndi Raice, Spencer E. Ante & Emily Glazer, *In Facebook Deal, Board Was All But Out of Picture*, WALL ST. J. (Apr. 18, 2012), *available at*: https://www.wsj.com/articles/SB10001424052702304818404577350191931921290#:~:text=INSTADEAL%3A%20Facebook%20CEO%20Mark%20Zuckerberg,days%20with%20Instagram's%20Kevin%20Systrom.&text=By%20the%20time%20Facebook's%20board,Was%20told%2C%20not%20consulted.%22.

[192] *Id*.

[193] *Id*.

[194] At the time, the Board was substantially the same as the Demand Board and included Defendants Andreessen, Bowles, Desmond-Hellmann, Hastings, and Thiel.

[195] *Zenimax*, Dkt. 927 at 14:22–15:3 (Zuckerberg testifies at trial that he purchased Oculus for "2 billion . . . had an additional $700 million plus earnouts in ongoing compensation . . . [that totaled] more than $3 billion").

co-founder of Oculus.[196] According to Defendant Zuckerberg's own testimony, the only person at Facebook with whom he spoke about the deal—prior to reaching the agreement in principal—was Defendant Andreessen.[197] Defendant Zuckerberg spoke with Defendant Andreessen even though he knew that Defendant Andreessen was conflicted—he appeared on both sides of transaction—and therefore could not vote to approve the deal.[198] But that did not stop Defendant Zuckerberg from pursuing this conversation "in [Defendant Andreessen's] capacity as a director of Facebook."[199] Defendant Zuckerberg later testified that he only decided to go through with the deal after Defendant Andreessen did not express "any concerns."[200]

527. The morning after his discussion with Defendant Andreessen, a Friday, Defendant Zuckerberg told his lawyers to immediately start due diligence, as he expected to finalize the deal by Monday.[201] Defendant Zuckerberg gave this instruction even though it was already apparent that things Oculus had told Facebook

---

[196] Max Chafkin, *Why Facebook's $2 Billion Bet on Oculus Rift Might One Day Connect Everyone on Earth*, VANITY FAIR (Sept. 8, 2015), *available at*: https://www.vanityfair.com/news/2015/09/oculus-rift-mark-zuckerberg-cover-story-palmer-luckey.

[197] *Zenimax*, Dkt. 927 at 59:5-68:1-5.

[198] *Id*. at 59:5-68:1-5.

[199] *Id*. at 62:21-25.

[200] *Id*. at 63:2-21.

[201] *Id*. at 65:12-66:18.

"were simply not true."[202] Defendant Zuckerberg later acknowledged that Oculus "misrepresented some things to us that would have led us to offer a lower price than we might have."[203] But, at the time, Defendant Zuckerberg callously dismissed these concerns and insisted on moving forward on his stated timetable.[204]

528. The Board, meanwhile, was first informed of the transaction on Sunday night and immediately rubber-stamped the deal.[205] The deal was finalized the following Tuesday, or one day later than Defendant Zuckerberg had previously demanded.[206] The Board's approval of the deal was particularly striking because Defendant Zuckerberg had even told the Board that Facebook's "top deal guy [was] telling [him] on the day [they're] doing diligence [that] there is a risk in doing this over a weekend without digging into their agreements and their IP."[207]

529. After the deal was finalized and announced, but before closing, ZeniMax sued Oculus for misappropriation of intellectual property, and copyright

---

[202] *Id.* at 71:22-72:5.

[203] *Id*. at 68:1-5.

[204] *Id*. at 68:7-12, 68:14-19.

[205] *Id*. at 64:14-20.

[206] *Id*. at 66:14-16.

[207] *Id*. at 69:23-70:1 (Defendant Zuckerberg testified, "I'm sure that was part of the discussion.").

and trademark infringement.[208] Following closing, ZeniMax amended the lawsuit to add Facebook as a defendant.[209] The case went to a jury trial, and the jury returned a $500 million verdict against Facebook and Oculus.[210]

530. Defendant Zuckerberg's brazen attitude of moving fast and breaking things, coupled with the Board's submissiveness to his whims and desires, caused the Company to overpay for Oculus and then pay a judgment of half a billion dollars on behalf of Oculus for IP misappropriation. The Board, meanwhile, could have prevented this harm if it had stood up to Defendant Zuckerberg and withheld its vote until due diligence was completed properly. But the Board failed to do this because its members cannot say no to Defendant Zuckerberg.

---

[208] *Zenimax*, Dkt. 928 at 97:6-25; *see also Zenimax*, at Dkt. 38.

[209] *Zenimax*, at Dkt. 38.

[210] J. Krochtengel, *Oculus, Execs Must Pay $500M for Software Infringement*, LAW360 (Feb. 1, 2017), *available at*: https://www.law360.com/articles/886093. The Final Judgment entered in the case was $304 million, which Facebook stated it would appeal. D. Simpson, *ZeniMax's IP Verdict Against Oculus Cut by $250M*, LAW360 (June 27, 2018), *available at*: https://www.law360.com/articles/1058278. The case subsequently settled. *See* Nicole Tanner, *ZeniMax and Facebook Settle Oculus VR Suit*, GEEKWIRE (Dec. 12, 2018), *available at*: https://www.geekwire.com/2018/ zenimax-facebook-settle-oculus-vr-suit/.

2. *Zuckerberg Ousts Anyone Who Defies His Authority*

531. Any director who disagrees with Zuckerberg is forced to leave the Board. High-level employees who disagree with Zuckerberg similarly have nowhere to go but out.

532. Jan Koum, a founder of the messaging app WhatsApp, joined Facebook's Board in 2014 after selling WhatsApp to Facebook. In 2018, Koum left the Board without publicly providing a reason besides "it's time to move on."

533. WhatsApp's other co-founder, Brian Acton, had already left Facebook after receiving pressure from Zuckerberg and Sandberg to monetize WhatsApp. In an interview with *Forbes*, Acton summed up his response to the pressure as "[i]t was like, okay, well, you want to do these things I don't want to do," resulting in him leaving Facebook and forgoing stock grants worth $850 million. Eventually Acton publicly supported the #DeleteFacebook movement.

534. Later, in 2018, Instagram's co-founders, Kevin Systrom and Mike Krieger, left Facebook, reportedly after clashing with Zuckerberg and other members of Facebook management over the direction of Instagram.

535. In April 2019, Facebook announced Hastings and Bowles were leaving the Board and Alford, who had been the Chief Financial Officer of the Chan Zuckerberg Initiative, was joining the Board.

536. It was widely reported that Hastings and Bowles had clashed with Facebook's management. As discussed more fully *supra* ¶¶246–54, Bowles, in connection with his responsibilities as Chairman of the Audit Committee, had met with Alex Stamos, Facebook's chief information security officer, and Colin Stretch, Facebook's general counsel, in or around September 2017. Zuckerberg and Sandberg had asked the pair to brief the Audit Committee on Russian use of Facebook to influence the 2016 presidential election. According to *The New York Times*, Bowles was furious about being informed of the matter so late.

> The disclosures set off Mr. Bowles, who after years in Washington could anticipate how lawmakers might react. He grilled the two men, occasionally cursing, on how Facebook had allowed itself to become a tool for Russian interference. He demanded to know why it had taken so long to uncover the activity, and why Facebook directors were only now being told.
>
> When the full board gathered later that day at a room at the company's headquarters reserved for sensitive meetings, Mr. Bowles pelted questions at Facebook's founder and second-in-command. Ms. Sandberg, visibly unsettled, apologized. Mr. Zuckerberg, stone-faced, whirred through technical fixes, said three people who attended or were briefed on the proceedings.

537. As reported by *The New York Times*, this led to Sandberg confronting Stamos the next day, yelling at him "[y]ou threw us under the bus!"

538. On October 30, 2019, Facebook announced that Desmond-Hellmann, who had served as Facebook's lead independent director since June 2015, was leaving the Board. Facebook quoted Desmond-Hellmann, stating that her departure

was due to "increasing demands from my CEO role, my extended family, and my own health."

539. In February 2020, Dropbox Inc. CEO, Drew Houston joined the Board. Far from adding a steady independent voice, Houston is described by *The Wall Street Journal* as "a friend of Mr. Zuckerberg's who has appeared with him at social events."

540. Shortly thereafter, in March 2020, Chenault and Zients both announced they were leaving the Board. According to *The Wall Street Journal*, Chenault and Zients were generally aligned in their thinking, and Chenault was frustrated with Zuckerberg's failure to take Chenault's advice. Specifically, Chenault is reported to have pushed the Company to take more responsibility for its role in elections. Chenault and Zients' departure is disconcerting, as they are the two directors who received the most votes at the 2019 stockholders' meeting.

541. On April 28, 2020, *The Wall Street Journal* reported further on Facebook's Board turnover, in an article entitled, "Mark Zuckerberg Asserts Control of Facebook, Pushing Aside Dissenters." The article describes an alarming power grab from Zuckerberg as longstanding advisers and independent voices are stripped of authority, resign, or otherwise distance themselves from the Company. As the article states, in relevant part:

Within months, Facebook announced the departure of two directors, and added a longtime friend of Mr. Zuckerberg's to the board. The moves were the culmination of the chief executive's campaign over the past two years to consolidate decision-making at the company he co-founded 16 years ago.

* * *

In February, Mr. Zuckerberg brought on more boardroom support, adding longtime friend Drew Houston, the 37-year-old CEO of cloud-software company Dropbox Inc. The previous spring, he had added Peggy Alford, a PayPal Holdings Inc. executive who had worked for him as finance chief at the Chan Zuckerberg Initiative.

* * *

542. As evidenced by the above, Facebook's profound governance failures have led to a complete breakdown in Board independence, leaving Zuckerberg's consolidation of decision-making power unchecked.

3. *Zuckerberg Unilaterally Replaces The Dissenting Directors*

543. Article VI Section 2 of Facebook's Certificate of Incorporation allows the Board to increase its size, and Section 2.2 of Facebook's Bylaws allows the Board to fill newly created vacancies.

544. Under Section 1.2 of the Bylaws, Zuckerberg, in his capacity as the Chairman or the CEO, has the right to call special meetings unilaterally "for any purpose . . . at any time[.]"

545. Under Section 1.10 of the Bylaws, Zuckerberg also has the right to take actions by written consent, including electing directors unilaterally. Section 1.10 states:

> [A]ny action . . . permitted to be taken at any annual or special meeting of the stockholders may be taken without a meeting, without prior notice and without a vote, if a consent or consents in writing . . . shall be signed by the holders of outstanding stock having not less than the minimum number of votes that would be necessary to authorize or take such action at which all shares entitled to vote thereon were present and voted.

546. Because Zuckerberg alone holds an absolute majority of the voting power of Facebook, he can take almost any action by written consent. This includes the election of directors, since Zuckerberg's majority control of the voting power can be exercised to override other stockholders' votes, and can veto the actions demanded by any other stockholder.

547. Using these powers, either directly or implicitly through his dominance and control of the Board (and because Zuckerberg can override any Board nomination with which he disagrees through his veto power and has the ability to call special meetings or take actions by written consent), Zuckerberg has recently used his dominance over the Board to cause it to increase its size and add four new directors within months before the annual stockholder meeting, instead of waiting

for the meeting to allow stockholders to vote before the new directors can join the Board.

548. The Company's 2020 Proxy, filed on Form DEF 14A with the SEC on April 10, 2020, implies that Zuckerberg was the impetus for the Board's appointment of at least one and up to all four new directors. The 2020 Proxy states, "Mr. Houston was recommended by our CEO." Zuckerberg, through one of the executives he employs, may also have been involved in nominating Killefer, because the 2020 Proxy also states, "Ms. Killefer was recommended by a member of management," who all ultimately report to Zuckerberg. While the 2020 Proxy states that "Ambassador Kimmitt and Ms. Travis [were] recommended by a non-management director[,]" given the ties among Zuckerberg and almost all the non-management directors, and Zuckerberg's ability to unilaterally block any recommendation, he likely had influence over Kimmitt's and Travis's nomination as well.

549. On February 3, 2020, the Board elected Houston as a director. On March 5, 2020, the Board elected Killefer and Travis as directors, effective March 9, 2020. The Board also appointed Travis to the Audit & Risk Oversight Committee. On March 25, 2020, the Board elected Kimmitt as a director, appointing him to the position of Lead Independent Director.

550. These new directors owe their positions to Zuckerberg, who as the controlling stockholder with dominance and control over the current Board, and with

the express authority to call special meetings at any time and to take actions through written consent, can nominate and remove them (alongside the captive Board members who voted for these new directors) to fill the newly created vacancies.

4. *Zuckerberg Dominates Facebook's Negotiations With The FTC*

551. Just days after news of the Cambridge Analytica scandal broke, and without any investigation, the majority of the Demand Board immediately backed Defendant Zuckerberg and advised the public in an SEC-filings and in media interviews that they supported him (and Defendant Sandberg). In a statement on behalf of the Board, Defendant Desmond-Hellmann pronounced that "Mark and Sheryl know how serious this situation is and are working with the rest of Facebook leadership to build stronger user protections . . . They have built the company and our business and are instrumental to its future."[211]

552. Shortly thereafter, the FTC announced it was opening an investigation to ascertain whether Facebook's conduct had violated the 2012 Consent Order. As the FTC investigation was wrapping up, the FTC sent a preliminary complaint and

[211] *See* Joseph Bernstein & Ryan Mac, *Facebook's Board Said It Supports Zuckerberg And Sandberg In The Cambridge Analytica Crisis*, BUZZFEED NEWS (Mar. 21, 2018) (reporting that Zuckerberg and Sandberg "received a full-throated endorsement" from the Board), *available at*: https://www.buzzfeednews.com/article/josephbernstein/facebook-board-cambridge-analytica.

proposed consent order to [redacted], that named Zuckerberg as a defendant and held him personally responsible for the alleged violations of the 2012 Consent Order[212] because he [redacted] and [redacted][213]

553. But, as detailed herein and in Section V.B, *infra*, the devotion to Defendant Zuckerberg at the expense of the Company was so dispositive that the Board was willing to walk away from ***any*** settlement talks that resulted in Defendant Zuckerberg being held personally liable. The Board ultimately got what it wanted: the FTC agreed to settle the inquiry for $5 billion and Defendant Zuckerberg was not named as a defendant.

554. Reaching that conclusion, however, required numerous Board meetings and discussions between March 2019 and June 2019. The Board even created a Special Committee with its own counsel to [redacted][214] But there is no evidence the Board considered whether it could achieve a better result for the Company and its shareholders if it agreed to hold Defendant Zuckerberg personally liable. Instead,

[212] FB220-00016035.

[213] FB220-00016039 at 16073.

[214] FB220-00025602 at 25604.

there is evidence that the Board authorized the payment of a fine that was 50 times higher than what the Board believed was the Company's maximum liability to protect Defendant Zuckerberg.[215]

555. Further evidence of the Board's unqualified devotion to Defendant Zuckerberg comes from the operation of the Special Committee, which lacked meaningful independence, and which permitted Defendant Zuckerberg to frequently participated in Committee meetings to guide it to adopt his preferred settlement terms. This was allowed despite the obvious conflicts of interest.

556. Defendant Zuckerberg's control over the Special Committee was so complete that it felt it was necessary to resolve that Chenault, the Chair of the Committee, [redacted][216]

[215] David Shepardson, *Facebook To Pay Record $5 Billion U.S. Fine Over Privacy; Faces Antitrust Probe*, REUTERS (July 24, 2019), *available at*: https://www.reuters.com/article/us-facebook-ftc/facebook-to-pay-record-5-billion-u-s-fine-over-privacy-faces-antitrust-probe-idUSKCN1UJ1L9.

[216] FB220-00025582 at 25582-83.

VII. DEMAND FUTILITY AND INDEPENDENCE ALLEGATIONS

557. When this action was initiated on April 25, 2018, Facebook's Board consisted of nine members: Defendants Zuckerberg, Sandberg, Andreessen, Thiel, Hastings, Desmond-Hellmann, Bowles and Koum, together with non-party Chenault (the "Original Demand Board").[217]

558. When Laborers' Local No. 79 initiated its action on May 13, 2020, Facebook's Board consisted of 11 members: Defendants Zuckerberg, Sandberg, Andreessen, Thiel, Alford, Chenault, Houston, Kimmitt, Travis, Zients and Killefer. As of the filing of this Complaint, Facebook's Board consists of 9 members: Defendants Zuckerberg, Sandberg, Andreessen, Thiel, Alford, Houston, Kimmitt, Travis, and Killefer (the "Local 79 Demand Board"). At times herein, the Original Demand Board, the Local 79 Demand Board, and the 2021 Demand Board are collectively referred to as the "Demand Board."

[217] The Original Demand Board is Plaintiffs' operative iteration of the Facebook Board for purposes of satisfying Court of Chancery Rule 23.1's demand futility requirement. Demand futility with respect to the Local 79 Demand Board and the 2021 Demand Board is pled in the alternative. Chenault was new to the Original Board when suit was initiated, and given the timing, he was named as defendant for the Local 79 Demand Board as he became involved in the alleged misconduct.

559. Facebook's current Board consists of the following nine members: Defendants Zuckerberg, Sandberg, Andreessen, Thiel, Alford, Killefer, Houston, Kimmitt and Travis (the "2021 Demand Board").

Original Demand Board	**Local 79 Demand Board**	**2021 Demand Board**
Mark Zuckerberg	Mark Zuckerberg	Mark Zuckerberg
Sheryl Sandberg	Sheryl Sandberg	Sheryl Sandberg
Marc Andreessen	Marc Andreessen	Marc Andreessen
Peter Thiel	Peter Thiel	Peter Thiel
Reed Hastings	Peggy Alford	Peggy Alford
Susan Desmond-Hellmann	Nancy Killefer	Nancy Killefer
Erskine Bowles	Andrew Houston	Andrew Houston
Jan Koum	Robert Kimmitt	Robert Kimmitt
Kenneth Chenault	Tracey Travis	Tracey Travis
	Kenneth Chenault	
	Jeffrey Zients	

560. Demand is futile because a majority of the Demand Board cannot properly exercise its independent and disinterested business judgment in responding to a demand. The majority of the Demand Board: (1) is and were controlled by and/or beholden to Zuckerberg (*see e.g*. ¶¶20, 27-28, 497-556); (2) either caused, was directly involved in, and/or financially benefitted from, the illegal privacy and data sharing abuses that led to the 2012 Consent Order violations (*see e.g.* ¶¶7-10, 493-496, 569, 575, 584, 602, 606, 613, 619, 623, 645); and/or (3) knew of the legal obligations set forth by the 2012 Consent Order (*see e.g*. ¶¶93(vii), 94, 330, 363, 370), took no action to cause the Company to come into compliance with the 2012

Consent Order and either caused the Company to violate the 2012 Consent Order or knowingly took no action to ensure the Company's compliance. *See e.g.*, *supra* §§ IV.O.

A. Mark Zuckerberg

561. At all times Zuckerberg has been a controlling stockholder of Facebook as well as an officer and director of the Company. Zuckerberg faces a substantial threat of liability for the acts and omissions chronicled herein, and he engaged in massive insider sales while in the possession of material undisclosed information concerning Facebook, as described herein.

562. As described *supra* §VI, Zuckerberg has used his domination and control to cause Facebook to commit and suffer from the wrongs described herein. Directors who have sought to challenge Zuckerberg have either resigned or had their voices quashed. Specifically, Defendant Zuckerberg is "interested" in this litigation because he was personally responsible for the decisions that exposed users to misappropriation of their data through various channels. Indeed, Defendant Zuckerberg was one of the principal architects behind granting Whitelisted Developers access to the platform. Defendant Zuckerberg was also closely involved with Defendant Sandberg, Facebook executives Vernal, Lessin and Schroepfer, and other top Facebook executives, regarding "weaponizing" Facebook's Platform by

only enforcing Facebook's Platform Policies against competitors and potential competitors.

563. As described *supra* §VI, Facebook's unique structure and governance history results in a substantial doubt that any Board could impartially consider a demand to institute litigation against Zuckerberg. Zuckerberg dominates and controls the Facebook board, and the Board's persistent disregard of overwhelming stockholder support to curtail Zuckerberg's power and the perquisites Zuckerberg enjoys as a founder and controlling stockholder.

564. As described *supra* §VI, Zuckerberg dominates and controls the Company's operations and unilaterally negotiates acquisitions on the Company's behalf.

565. As described *supra* §VI, Zuckerberg dominated and controlled the Company's settlement negotiations with the FTC.

566. The foregoing makes it unlikely that the Board, no matter how constituted, would commence a suit against Zuckerberg.

B. Sheryl Sandberg

567. "As Facebook's longstanding COO" and a Board member during much of the wrongs set forth herein, Sandberg is not independent of [Defendant]

Zuckerberg.[218] She is the quintessential insider in her role as the right hand of Defendant Zuckerberg, and can be removed by Zuckerberg at any time. Defendant Sandberg was a high-ranking officer and a director during the Relevant Period alleged herein, and thus she faces a substantial threat of liability. Specifically, Defendant Sandberg is "interested" in this litigation because she was personally responsible for the decisions that exposed users to misappropriation of their data through authorized (Whitelisted Agreements) and unauthorized (Cambridge Analytica) channels. Indeed, Defendant Sandberg was one of the principal architects behind granting Whitelisted Developers access to the platform. Defendant Sandberg also had conversations with Defendant Zuckerberg and Facebook executives Vernal, Lessin and Schroepfer, and other top Facebook executives, regarding "weaponizing" Facebook's Platform by only enforcing Facebook's Platform Policies against competitors and potential competitors.[219]

568. Defendant Sandberg also stated that she had been aware of Cambridge Analytica's misconduct since December 2015 but failed to act to ensure the

[218] *Facebook Class C Shares Litigation*, *supra* note 10, at 48.

[219] *See* 643 Summaries, *supra* note 5, at 58 (citing FB-01155760).

misappropriated data was deleted, by for instance, auditing Cambridge Analytica and GSR, and instead simply accepted their word.[220]

569. Sandberg cannot exercise her independent judgment in considering a demand to bring suit against Zuckerberg and Facebook's current and former directors. In 2018, Sandberg received over $19 million in cash and restricted stock in compensation from Facebook. In 2019, she received over $20 million in cash and restricted stock from Facebook. Facebook also provides Sandberg with security services and use of a private aircraft, benefits worth millions of dollars annually. Sandberg also engaged in substantial insider sales while in the possession of material undisclosed information concerning Facebook, as described herein.

C. Marc Andreessen

570. As a member of the Board since June 2008, Andreessen faces a substantial risk of liability for the wrongs set forth herein. Andreessen was fully aware of the conduct that led to the 2019 Consent Order and the $5 billion FTC fine. For instance, at a May 2014 board meeting—three weeks after Defendant Zuckerberg's April 2014 announcement at the F8 conference that third-party

[220] EunKyung Kim, *Sheryl Sandberg on TODAY: Other Facebook Data Breaches 'Possible'*, TODAY.COM (Apr. 6, 2018) (hereinafter "Other Data Breaches Possible"), *available at*: https://www.today.com/news/sheryl-sandberg-today-other-facebook-data-breaches-possible-t126579.

developers would no longer have access to user Friend's data—Defendant Andreessen complained (again) that Facebook needed to make more friends in the developer community,[221] which could be accomplished by Whitelisting more developers. Facebook employees also knew not to bring enforcement action against (and instead "work[] with") companies that were "friends of Mark/Sheryl,"[222] including those companies that Defendant Andreessen invested in, like Circle, and which were known to have accessed Facebook user data.

571. Then, in 2016, Defendant Andreessen met directly with whistleblower Wylie, among other, to help Cambridge Analytica utilize the data it misappropriated from Facebook.[223] Defendant Andreessen and Wyle reportedly stayed in touch until Wylie exposed Cambridge Analytica in 2018.[224]

572. Moreover, in December 2017, Defendant Andreessen attended an Audit Committee meeting that discussed Cambridge Analytica and then stood by while

[221] 643 Summaries. *supra* note 5, at 146 (citing FB-01366319).

[222] 643 Summaries, *supra* note 5, at 110 (citing FB-00194154);

[223] Carole Cadwalladr, *Facebook Faces Fresh Questions Over When it Knew of Data Harvesting*, THE GUARDIAN (Mar. 16, 2019), *available at*: https://www.theguardian.com/technology/2019/mar/16/facebook-fresh-questions-data-harvesting-cambridge-analytica.

[224] *Id*.

Facebook and the Officer Defendants concealed the incident from the public until March of 2018.

573. Defendant Andreessen was also involved in the funding of Palantir, a company co-founded by Defendant Thiel that was implicated by Wylie as working with Cambridge Analytica on the Facebook data. *See* ¶¶225; 594–97.[225]

574. Beyond facing a substantial likelihood of liability, Andreessen cannot exercise independent business judgment when considering a demand to institute litigation against Zuckerberg. Andreessen is the co-founder of Andreessen Horowitz, which, according to his co-founder Benjamin Horowitz, they founded after they "set out to design a venture capital firm that would enable founders to run their own companies." Defendants Andreessen and Zuckerberg have a longstanding personal friendship and business relationship. For example, Zuckerberg confided in Andreessen while seeking business advice. In 2006, Yahoo! offered to buy Facebook for $1 billion. As Andreessen told *The New Yorker*, "Every single person involved in Facebook wanted Mark [Zuckerberg] to take the Yahoo! offer. The

[225] *See also* Wylie Tr., *supra* note 85, at Q1341; Nicholas Confessore & Matthew Rosenberg, *Spy Contractor's Idea Helped Cambridge Analytica Harvest Facebook Data*, N.Y. TIMES (Mar. 27, 2018), *available at*: https://www.nytimes.com/2018/03/27/us/cambridge-analytica-palantir.html#:~:text=As%20a%20start%2Dup%20called,spy%20agencies%20and%20the%20Pentagon.

psychological pressure they put on this twenty-two-year-old was intense. Mark and I really bonded in that period, because I told him, 'Don't sell, don't sell, don't sell!'"

575. Defendant Andreessen has used this relationship (and placement on Facebook's board) to amass billions of dollars in personal wealth. Defendant Andreessen is the co-founder and principal at Andreessen Horowitz, a venture capital firm that provides seed, venture, and growth stage funding to the "best new technology companies," several of which were sold to Facebook at a substantial profit. Defendant Andreessen has admitted the success of the firm has been materially impacted by his relationship with Defendant Zuckerberg and Facebook. In a May 18, 2015 New Yorker article titled "Tomorrow's Advance Man," Defendant Andreessen explained:

> Deal flow is everything. If you're in a second-tier firm, you never get a chance at that great company. Andreessen Horowitz saw its biggest successes after 'logo shopping' to add Facebook to the firm's portfolio in 2010. Within two years of that investment, 'Andreessen Horowitz was the talk of the town.'[226]

576. Two of Andreessen Horowitz's portfolio companies, Instagram and Oculus VR, were purchased by Facebook. Andreessen Horowitz's $250,000 investment in Instagram returned $78 million when Facebook acquired Instagram,

[226] Tad Friend, *Tomorrow's Advanced Man*, THE NEW YORKER (May 11, 2015), *available at*: https://www.newyorker.com/magazine/2015/05/18/tomorrows-advance-man.

an acquisition that was pushed through by Zuckerberg without Board involvement. Defendant Andreessen also profited from Facebook's purchase of Oculus VR—a company that he was able to invest in only because of his relationship with Defendant Zuckerberg. Defendant Andreessen had initially declined to invest in Oculus in its early stages, and later regretted that decision.[227] Defendant Andreessen subsequently sought to invest in Oculus in the fall of 2013, but Oculus's CEO was reluctant to allow the investment until Defendant Zuckerberg convinced him to accept Andreessen Horowitz's offer.[228] Defendant Andreessen then became a director on Oculus's four-member board.[229] Shortly thereafter, Defendant Zuckerberg offered $3 billion to acquire Oculus VR,[230] making Andreessen Horowitz $270 million dollars on their investment.[231] Prior to making that offer, the only person with whom Defendant Zuckerberg consulted was Defendant

[227] *Facebook Class C Shares Litigation*, *supra* note 10, Consolidated Verified Class Action Complaint, at ¶ 82 (June 6, 2016) (Trans. ID 59094969).

[228] *Id*.

[229] *Id*.; *Zenimax*, Dkt. 927 at 52:21-54:17.

[230] *Zenimax*, Dkt. 927 at 14:3-8.

[231] Anita Balakrishnan, *Facebook Tried to do Oculus Due Diligence in a Weekend, Zuckerberg Reveals in Court*, CNBC (Jan 17, 2017), *available at*: https://www.cnbc.com/2017/01/17/facebook-did-oculus-due-diligence-in-a-weekend-zuckerberg-reveals-in-court.html.

Andreessen—who could not vote to approve that transaction on behalf of Facebook due to his material conflict. [232]

577. Andreessen, through his venture fund, also owns more than [redacted] of OfferUp, Inc., [redacted]

578. In litigation over the Reclassification it was revealed that Andreessen, despite being a member of the special committee ostensibly negotiating with Zuckerberg over the terms of the Reclassification, had worked behind the scenes to give Zuckerberg insights into the special committee's deliberative process. Andreessen even coached Zuckerberg on his calls with the special committee. As it related to the Reclassification transaction, a Delaware Court found that Andreessen:

> [C]ould not exercise disinterested and independent judgment regarding a demand. Based on his back-channel communications during the Committee process and self-professed fealty to Zuckerberg, he is not independent of Zuckerberg and he would face a substantial risk of liability on a claim challenging the Reclassification. He would not be entitled to exculpation because he acted disloyally and in bad faith.[233]

579. Then in 2019 Facebook formed another Special Committee to recommend the circumstances under which the Board would consider settling the

[232] *See supra* §VI.D.1.

[233] *Facebook Class C Shares Litigation*, *supra* note 10, at 48.

FTC inquiry. Defendant Andreessen again demonstrated his loyalty to Defendant Zuckerberg by allowing him to attend Special Committee meetings, guide the discussion, and even discern the circumstances under which the Special Committee would recommend settling the FTC inquiry.[234] Defendant Andreessen ultimately recommended Facebook agree to a settlement that was 50 times higher than the Company's calculation of its maximum liability to protect Defendant Zuckerberg from being held personally responsible for the Company's violations of the 2012 Consent Order, thereby again violating his duty of loyalty to the Company.[235]

580. Andreessen's wife, Laura Arrillaga-Andreessen, has advised Zuckerberg and Chan in philanthropy planning. She is a graduate of and lecturer at Stanford University, which has received grants of over [redacted] from the Chan Zuckerberg Initiative.

581. Andreessen also cannot independently and disinterestedly consider a demand against Defendant Thiel, because of their substantial business ties. In addition to their long-standing joint service on the Facebook Board, [redacted]

[234] *See supra* at *supra* §IV.P.4.

[235] *Id*.

[redacted] For his loyal service to Defendant Zuckerberg as a director of Facebook, and as a member of Defendant Zuckerberg's trusted inner-circle, Andreessen (along with Sandberg and Thiel) are among the few who own 10-to-1 vote Class B shares of Facebook.

582. Since 2012, Andreessen has directly or indirectly sold over 8.8 million shares of Facebook common stock valued of ***over half a billion dollars***. Andreessen currently owns 188,048 shares of Class A shares currently valued at over $66 million. As set forth *supra* §V.D, Andreessen also engaged in substantial insider trading during the Relevant Period.

D. Peter Thiel

583. Thiel has served as President of Thiel Capital, an investment firm, since 2011, Thiel is also the co-founder of the venture capital firm Founders Fund and is Facebook's earliest and first outside investor. In 2004, Thiel made a $500,000 angel investment for 10.2% of Facebook's stock, which Thiel later sold for over $1 billion, a significant financial benefit that was tied to his relationship with Zuckerberg and for decades represented a substantial portion of Thiel's wealth.

584. During Thiel's thirteen-year tenure on Facebook's Board, Thiel has served on the Audit Committee until he stepped down on May 15, 2013 and on the Compensation Committee from May 15, 2013 through present. In 2016, the Compensation Committee expanded and renamed the Compensation & Governance

Committee. Then, after the FTC ordered Facebook to appoint an independent nominating committee, the Compensation & Governance Committee was again expanded to become the Compensation, Nominating & Governance Committee, which oversees succession planning and director nominations. Thiel was named Chair of the Compensation, Nominating & Governance Committee and is joined by two Zuckerberg loyalists, Andreessen and Houston.

585. As a member of the Board since April 2005[236], Thiel faces a substantial risk of liability for the wrongs set forth herein. In addition, Defendant Thiel faces substantial liability from this litigation, or otherwise received a material benefit from the alleged misconduct, because he knew (or should have known) about Facebook's illegal data sharing practices through other business ventures. For example,

[236] Facebook Inc., Form DEF14A, at 9 (Definitive Proxy Statement) (April 26, 2013), *available at*: https://www.sec.gov/Archives/edgar/data/1326801/000119312513178090/d493645ddef14a.htm.

Defendant Thiel was also an early investor in Zynga,[237] Lyft,[238] Spotify,[239] all of which were all given special access to Facebook user data without user consent.[240]

586. Thiel cannot exercise independent business judgment when considering a demand to institute litigation against Zuckerberg. Thiel's venture capital fund, The Founders Fund, in its marketing literature boasts that the Founders Fund "had never removed a single founder," while describing other "VCs who kick out or overly control founders in an attempt to impose 'adult supervision.'" Its website notes further that "we have often tried to ensure that founders can continue to run their businesses through voting control mechanisms, as Peter Thiel did with Mark Zuckerberg and Facebook."

---

[237] Matthew Lynley, *Here are Zynga's Minority Investors: Google, Peter Thiel, Softbank and Others*, VENTUREBEAT (July 18, 2011), *available at*: https://venturebeat.com/2011/07/18/zynga-minority-investor/.

[238] Sarah Kessler, *Why It's Almost Impossible to Boycott Peter Thiel*, FAST COMPANY (Oct. 17, 2016), *available at*: https://www.fastcompany.com/3064713/why-its-almost-impossible-to-boycott-peter-thiel.

[239] *Id*.

[240] 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), *available at*: https://www.forbes.com/sites/angelauyeung/2019/11/07/facebook-ceo-mark-zuckerberg-dismissed-tinder-cofounder-as-irrelevant-but-still-let-dating-app-get-special-access-to-users-data/?sh=579d2f9a3ffc.

587. Furthermore, Thiel is loyal to Zuckerberg because Zuckerberg saved Thiel from being ousted from the Board in 2016. In 2016, Thiel came under heavy internal criticism for his support of Donald Trump's campaign. In October 2016, Zuckerberg defended Thiel in an internal memo disclosed by *The Verge*, stating in part, "[w]e care deeply about diversity . . . . We can't create a culture that says it cares about diversity and then excludes almost half the country because they back a political candidate. There are many reasons a person might support Trump[.]"

588. Furthermore, in 2017, Zuckerberg mediated an ongoing conflict between Thiel and Hastings over Thiel's support of Trump, by declining both of their resignations and defending Thiel for adding "ideological diversity" to the Board. Again, in March 2017, Zuckerberg publicly defended Thiel, stating that Facebook was enriched because "[w]e have a board member who is an adviser to the Trump administration, Peter Thiel."

589. People close to Defendants Zuckerberg and Thiel described their relationship as an "alliance" based on a long history of protecting each other's positions and interests.[241] Indeed, Zuckerberg's decision to not oust Thiel for his

[241] Douglas MacMillan, Keach Hagey & Deepa Seetharaman, *Tech Luminary Peter Thiel Parts Ways with Silicon Valley*, WALL ST. J. (Feb. 15, 2018), *available at*: https://www.wsj.com/articles/tech-luminary-peter-thiel-parts-ways-with-silicon-valley-1518696120.

connection with the Cambridge Analytica scandal alone demonstrates that Thiel cannot be impartial to Zuckerberg. Additional examples of such a connection abound.

590. For example, in 2017, when there was public outcry to remove Defendant Thiel from Facebook's Board on account of his affiliation with Trump, Defendant Zuckerberg called the suggestion "crazy" and refused to remove him. Then, in 2018, after the Cambridge Analytica scandal was fully revealed and facing a Board unable or unwilling to carry out their fiduciary duties in good faith, Defendants Bowles and Chenault sought to reform the Company's governance practices by creating an outside advisory group that analyzed a range of problems confronting Facebook and that would deliver reports directly to the Board.[242] The group was never assembled, in part, because it was seen internally as circumventing Defendant Zuckerberg's authority, including opposition from Thiel.[243]

[242] Deepa Seetharaman & E. Glazer, *Mark Zuckerberg Asserts Control of Facebook, Pushing Aside Dissenters*, WALL ST. J. (Apr. 28, 2020) (hereinafter "Zuckerberg Asserts Control"), *available at*: https://www.wsj.com/articles/mark-zuckerberg-asserts-control-of-facebook-pushing-aside-dissenters-11588106984.

[243] Eric Lutz, *Guess Who's Behind Facebook's Political Ad Policy*, VANITY FAIR (Dec. 17, 2019), *available at*: https://www.vanityfair.com/news/2019/12/peter-thiel-behind-facebooks-political-ad-policy; *see also* Zuckerberg Asserts Control, *supra* note 242.

591. Defendant Thiel also protected Defendant Zuckerberg when the Board considered whether to resolve the 2019 FTC Consent Order, voting to approve a settlement that was 50 times higher than the Company's calculation of its maximum liability to ensure Defendant Zuckerberg was not held personally liable.

592. Defendant Thiel also receives "good deal flow" because of his high-profile association with Defendant Zuckerberg and Facebook.[244] For instance, Defendant Thiel's Founders Fund was a Series A investor in Oculus VR,[245] and like Defendant Andreessen, it turned its small investment into millions of dollars when Defendant Zuckerberg acquired Oculus VR. Thiel's Founders Fund was also invested in start-up CTRL-Labs which Facebook purchased in September 2019 for a reported $500 million to a $1 billion.

593. Defendant Thiel also co-founded Palantir, a data processing and analyzation company, in 2003, and has served as the Chairman of the Board of Directors since then. Palantir was directly linked to Cambridge Analytica's misuse of Facebook data by whistleblower Wylie, who produced documents demonstrating that senior Palantir employees aided in the construction of Cambridge Analytica's

---

[244] *Facebook Class C Shares Litigation*, *supra* note 227, Consolidated Verified Class Action Complaint, at ¶ 85.

[245] CBInsights, *Oculus VR, available at*: https://www.cbinsights.com/company/oculus-vr-funding.

psychological profile models, which relied on illegally obtained Facebook data.[246] According to Wylie, there was no "official" contract between Palantir and Cambridge Analytica. Rather, "Palantir staff [] would come into the office and work on the data . . . And we would go and meet with Palantir staff at Palantir.[247]

594. Documents reviewed by the *Observer* further confirmed that meetings took place in 2013 between Cambridge Analytica and Palantir where the possibility of a working relationship was discussed, and that "at least one senior Palantir employee consulted with Cambridge Analytica in relation to the Trinidad project and later political work in the US."[248] But Palantir ultimately "decided it was too much of a reputational risk for a more formal arrangement,"[249] hence the lack of any official contract and behind the scenes support.

595. Facebook executive Schroepfer later publicly confirmed that Facebook was investigating whether Palantir's had gained improper access to user data.[250]

---

[246] Wylie Tr., *supra* note 58, at Q1324.

[247] *Id*.

[248] Carole Cadwalladr, *The Great British Brexit Robbery: How Our Democracy was Hijacked*, THE GUARDIAN (May 7, 2017), *available at*: https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy; *see also* Confessore & Rosenberg, *supra* note 225.

[249] *Cadwalladr*, *supra* note 248.

[250] Schroepfer Tr., *supra* note 76, at Q2338.

Media reports followed up and discovered that the investigation of Palantir had been demanded by Defendants Zuckerberg and Sandberg, which was considering whether it could "potentially leverage relationship with Thiel to force Palantir to have conversation with FB regarding data abuse.'"[251]

596. There is also some evidence that Defendant Thiel may have been directly involved in Palantir's work to support Cambridge Analytica. Specifically, the Trump campaign has stated that Defendant Thiel "helped it with data" and that data campaign that "was led by Steve Bannon, who was then at Cambridge Analytica."[252] Indeed, Mr. Bannon was the Vice President, and a board member of Cambridge Analytica.[253] And Mr. Bannon has been quoted as being unable to "overstate [Defendant Thiel's] impact on the [presidential] transition."[254] Bannon

[251] E. Glazer, D. Seetharaman, & J. Horwitz, *Peter Thiel at Center of Facebook's Internal Divisions on Politics*, WALL ST. J. (Dec. 17, 2019), *available at*: https://www.wsj.com/articles/peter-thiel-at-center-of-facebooks-inter nal-divisions-on-politics-11576578601.

[252] *Cadwalladr*, *supra* note 248.

[253] *FTC v. Bannon*, 1:20-mc-00111-CRC, Petition Of The Federal Trade Commission For An Order Enforcing Civil Investigative Demand, at ¶3 (D.D.C. Nov. 9, 2020) (Dkt. #1).

[254] Adam Ciralsky, *Is Trump Mulling Peter Thiel for a Top Intelligence Advisory Post*, VANITY FAIR (Sept. 20, 2017), *available at*: https://www.vanityfair.com/news/2017/09/donald-trump-peter-thiel-top-intelligence-advisory-post.

further described Defendant Thiel as a hidden hand in shaping Team Trump because of, in part, the value he brought through the companies in his "portfolio,"[255] like Palantir.[256]

597. Defendant Thiel therefore faces substantial liability from this litigation, or otherwise received a material benefit from the alleged misconduct, because he knew (or should have known) about Facebook's illegal data sharing practices through his other business ventures.

598. Thiel also cannot independently and disinterestedly consider a litigation demand against Defendant Andreessen, because of their substantial business ties. In addition to their long-standing joint service on the Facebook Board, [redacted]

[255] *Id*.

[256] Defendant Thiel has further benefitted from Palantir and Cambridge Analytica's aid to the Trump campaign as Palantir has become one of the largest recipients of government defense contracts with the United States government after President Trump took office. *See* Dylan Byers & Ben Collin, *Trump Hosted Zuckerberg for Undisclosed Dinner at the White House in October*, NBC NEWS (Nov. 20, 2019), *available at*: https://www.nbcnews.com/tech/tech-news/trump-hosted-zuckerberg-undisclosed-dinner-white-house-october-n1087986.

599. As set forth *supra* §V.E. above, Defendant Thiel also engaged in substantial insider sales during the Relevant Period.

E. Reed Hastings

600. Defendant Hastings is the founder and CEO and President of Netflix, Inc. Like Defendant Zuckerberg, he serves in the dual role of Chairman and member of Netflix's Board. Defendant Hastings has served on Facebook's Board from June 2011 through May 30, 2019, and during that tenure served as the Chair of Facebook's Compensation, Nominating & Governance Committee.

601. Defendant Hastings has relied on and received a material benefit from the misconduct that is the subject of this litigation. Specifically, Defendant Hastings has benefited from Facebook's business relationship with Netflix,[257] including from Facebook's misappropriation of user data without user consent. For example, Netflix was a Whitelisted Developer following Facebook's platform changes in April 2014,[258] which allowed Netflix to maintain full access to Friends data

[257] For instance, Facebook and Netflix's joint "Friends and Community" initiative, launched in March 2013, which allowed Netflix obtained invaluable metrics and insights into how its customers used Netflix. The initiative was so powerful that Netflix's stock price increased 6 percent.

[258] 643 Docs, *supra* note 5, at FB-00045736.

indefinitely.[259] But Netflix's unique relationship with Facebook allowed it to get so much more than the typical user data given to the other Whitelisted Developers. Indeed, it was 1 of only 3 companies (out of the more than 150 Whitelist Partners) that Facebook allowed to read, write and delete Facebook users' messages and view all participants on a message thread—all of which was done without adequate disclosures and affirmative user consent.[260] Access to this type of highly specialized data allowed Netflix to introduce unique features, like letting customers recommend TV shows and movies to their Facebook friends via Facebook Messenger or Netflix.[261]

602. Defendant Hastings knowledge of and participation in Facebook's misappropriation of consumer data is perhaps unsurprising because Netflix, like Facebook, has adopted a business model that freely shares sensitive user information. Defendant Hastings has remarked that Netflix is like the "anti-Apple

---

[259] Colin Lecher, *Internal Facebook Documents Show How the Company Makes Deals for Data*, THE VERGE (Dec. 5, 2018), *available at*: https://www.theverge.com/2018/12/5/18127230/facebook-data-documents-parliament-deals-zuckerberg.

[260] *Id*.

[261] Todd Spangler, *Netflix Says It Never Accessed Facebook Users' Private Messages*, VARIETY (Dec. 19, 2018), *available at*: https://variety.com/2018/digital/news/facebook-netflix-user-messages-access-privacy-1203093053/.

you know how they compartmentalize; we did the opposite—which is everybody gets all the information."[262]

603. Indeed, Netflix's 2020 Form 10-K sets forth that a material risk to its business is "[p]rivacy concerns" which "could limit our ability to collect and leverage member personal information and other data and disclosure of member personal information and other data could adversely impact our business and reputation." Netflix admits that "in the ordinary course of business and in particular in connection with content acquisition and merchandising our service to our members, we collect and utilize information supplied by our members, which may include personal information and other data."

604. Limitations on Netflix's ongoing access, collection, and use of big data would put Hasting's fortune—like Andreessen and Thiel—at risk. Hastings could not be expected to consider demand in this action when a material portion of his financial and business interests favor, and indeed depend on the free flow of big data.

605. Defendant Hastings beneficially owns 134,000 share of Class A Common Stock in Facebook, currently worth over $20 million.

[262] Theodore Schleifer, *Facebook Board Member Reed Hastings Says Companies like Facebook are Trying to 'Grow Up Quickly'*, VOX (Apr. 14, 2018) *available at*: https://www.vox.com/2018/4/14/17238190/facebook-netflix-ceo-reed-hastings-board-member-cambridge-analytica-ted-conference.

F. Susan Desmond-Hellmann

606. Defendant Desmond-Hellmann served on Facebook's Board from March 2013 through April 2019 and was purportedly the "Lead Independent Director" and served on Facebook's Audit Committee.

607. Defendant Desmond-Hellmann faces a substantial risk of liability due to her role as a member of Facebook's Audit Committee and her participation in various meetings and presentations, which made her aware (or should have made her aware) of Facebook's improper third-party data sharing, failed data compliance practices and policies, and failure of the Board to fulfill its obligations under the 2012 FTC Consent Order.[263] Indeed, Defendant Desmond-Hellmann participated in an Audit Committee meeting held on December 6, 2017 that discussed [redacted] and then stood by while Facebook and its officers concealed [redacted] until Facebook was forced to acknowledge the data breach following news reports and whistleblowers accounts.

608. Defendant Desmond-Hellmann is also not independent of Defendant Zuckerberg and has repeatedly displayed her absolute allegiance to Defendant Zuckerberg. For example, in 2015, she sat on Facebook's special committee tasked with reviewing Defendant Zuckerberg's proposal to give him lifetime control of

[263] *See e.g.*, FB220-00001283.

Facebook without any corresponding benefits for shareholders. She later testified that the special committee approved of the transaction because it "believed that it had no real ability to say 'no' to Zuckerberg."[264]

609. Defendant Desmond-Hellmann again displayed her loyalty to Zuckerberg again when news of Cambridge Analytica broke in 2018 and she told reporters that she had 100 percent faith in Defendant Zuckerberg and supported him completely.[265] Then, in March 2019, Defendant Desmond-Hellmann belatedly

[redacted][266]

She then voted to adopt the Special Committee's recommendation to settle the Inquiry for $5 billion even though that amount was 50 times higher than the maximum penalty the Company believed the FTC could impose. The reason for this vote was because the hefty fine came without personal liability for Defendant Zuckerberg.[267] Later, after Defendant Zuckerberg decided not to re-nominate her to the Board, Defendant Desmond-Hellmann purportedly confided in friends that she

[264] *See supra* at ¶ 508 & n.188.

[265] The Board was in full support of Zuckerberg and Sandberg, *supra* note 211.

[266] FB220-00025602 at 25604.

[267] FB220-00027896-901.

did not think Facebook's Board was operating properly and that Facebook management refused to consider the Board's feedback.[268]

610. Yet another reason for Defendant Desmond-Hellmann's public loyalty to Defendant Zuckerberg stems from her role as the CEO of the Bill and Melinda Gates Foundation between 2014 and 2019.[269] In that capacity, Defendant Desmond-Hellmann relied heavily on building relationships and collaborating with Silicon Valley's elite, including: Defendant Zuckerberg and his spouse; Defendant Andreessen and his spouse; Defendant Thiel; Amazon founder Jeff Bezos; and Yahoo! co-founder Jerry Yang, among others.

611. The Gates Foundation, Facebook, and CZI also have a long history of working together on various philanthropic initiatives. For example, in 2014,

[268] Zuckerberg Asserts Control, *supra* note 242.

[269] Press Release, *Bill & Melinda Gates Foundation CEO Sue Desmond-Hellmann to Step Down, Longtime Foundation Executive Mark Suzman Appointed to Role*, GATES FOUNDATION (December 5, 2019), available at: https://www.gatesfoundation.org/Media-Center/Press-Releases/2019/12/CEO-Announcement-2019#:~:text=Bill%20%26%20Melinda%20Gates%20Foundation%20CEO%20Sue%20Desmond%2DHellmann%20to%20Step,Mark%20Suzman%20Appointed%20to%20Role&text=Bill%20and%20Melinda%20Gates%20have,officer%2C%20as%20the%20new%20CEO.

Defendant Zuckerberg donated $24 million towards one of the Gates Foundation's Ebola projects in strategic partnership with the CDC Foundation.[270]

612. Defendant Desmond-Hellmann had been handsomely compensated for her service to Facebook's Board, receiving about $428,000 annually.[271] Moreover, by the time she left Facebook, Defendant Desmond-Hellmann owned nearly 32,854 Class A Shares of Facebook, currently worth over $11.2 million,[272] which comprised a substantial portion of her overall wealth.

G. Erskine Bowles

613. Defendant Bowles is a career politician who, among other appointments, served as President Bill Clinton's Chief of Staff from 1996 to 1998. Defendant Bowles served as a member of Facebook's Board from September 2011 through May 2019 and during that tenure served as Chair of the Audit Committee (now known as the Audit & Risk Oversight Committee).

614. As Chair of the Audit & Risk Oversight Committee, Defendant Bowles faces a substantial risk of liability due principally to his participation in various

---

[270] Chris Isidore, *Zuckerberg Donates $25 Million to Fight Ebola*, CNN BUSINESS (October 14, 2014), *available at*: https://money.cnn.com/2014/10/14/technology/zuckerberg-ebola/.

[271] Facebook, Inc., Form DEF 14A, at 20 (Definitive Proxy Statement) (April 12, 2019).

[272] *Id*. at 41.

meetings and presentations, which made him aware (or should have made him aware) of Facebook's improper third-party data sharing, failed data compliance practices and policies, and failure of the Board to fulfill its obligations under the 2012 FTC Consent Order.[273] Indeed, Defendant Bowles participated in an Audit Committee meeting held on December 6, 2017 to discuss the [redacted] and then stood by while Facebook and its officers concealed [redacted] until Facebook was forced to acknowledge the data breach following news reports and whistleblowers accounts.

615. In early 2019, Defendant Zuckerberg decided that Defendant Bowles would not be re-nominated to the Board after disagreements on the Company's governance and political policies. After his departure, Defendant Bowles privately criticized Facebook leadership for failing to take his advice in response to the Cambridge Analytica scandal.[274]

616. Defendant Bowles lacks independence from Defendant Zuckerberg—even though he purportedly served as an "independent director"—as evidenced by his participation and conduct in the 2015 special committee that ultimately

[273] *See e.g.*, FB220-00001283.

[274] Zuckerberg Asserts Control, *supra* note 242.

recommended approval of granting Defendant Zuckerberg lifetime control over Facebook.[275]

617. Defendant Bowles lack of independence is further clarified from his record as a professional outside director who has served on the boards of many public companies where he has consistently bowed to the interests of CEOs. For example, Defendant Bowles has consistently voted to approve lavish payouts to CEOs while companies were underperforming. In 2012, Defendant Bowles voted to increase the Norfolk CEOs compensation by 16 percent while the stock fell below the S&P 500 average. Then, during Defendant Bowles' time on the Cousins board, with the company underperforming, he voted to increase the CEO's pay by 73 percent in 2011 and 276 percent in 2012. Similarly, during Defendant Bowles' tenure on Morgan Stanley's board, CEO pay went from less than $1.3 million annually in 2008 and 2009 to $38.8 million in 2010 through 2012. These pay increases were authorized even though Morgan Stanley's stock price declined.

618. In return for these favorable pay increases, Defendant Bowles has earned tens of millions of dollars in director compensation. For example, Defendant Bowles personally received over $3.8 million from Morgan Stanley for his services as a director from 2007 to 2017. Bowles was also a member of the General Motors

[275] *See supra* at §VI.B.

board from June 2005 until April 2009, when the auto giant filed for bankruptcy. At Facebook, Defendant Bowles received an annual fee and restricted stock worth $400,000 for his service. By early 2019, he owned over 29,898 shares of Facebook Class A stock, with a current market value of over $10.2 million, and which comprised a substantial portion of his overall wealth.[276]

H. Jan Koum

619. Defendant Koum was the co-founder and CEO of WhatsApp Inc. ("WhatsApp") a cross-platform mobile messaging application company that Facebook acquired in 2014 for billions of dollars. Defendant Koum was a member of the Board from October 2014 through April 2018.

620. Defendant Koum, like the other Board members, demonstrated his loyalty to Defendant Zuckerberg when he voted in favor of Defendant Zuckerberg's lifetime entrenchment.[277]

621. Defendant Koum also demonstrated his loyalty to Defendant Zuckerberg on numerous prior occasions. For example, despite Defendant Koum's belief that WhatsApp should focus on user experience and privacy, he watched as

[276] In 2018, Bowles receives $50,000 annually as a Facebook Board member, as well as $50,000 annually as chair of the audit committee, and an annual grant of RSUs equal to $321,194 (which vest in 2019). *See* 2018 Proxy Statement, *supra* note 271, at 20.

[277] *See supra* at §VI.B.

Defendant Zuckerberg changed WhatsApp's terms of service and privacy policies to combine user data across services. Defendants Zuckerberg and Sandberg took great pains to avoid negative press coverage of these changes. Defendant Koum was even instructed, in advance of a dinner event where he might have to address the changes to WhatsApp's data sharing policies, to "Try not to get too much into the weeds on the types of data we're sharing and for what use cases. It will get you trouble. Instead be prepared with a couple 'safe' examples, like spam/abuse."[278] Loyal to Defendant Zuckerberg and Sandberg, Defendant Koum followed his instructions.

622. Defendant Koum also profited off his confidential insider knowledge relating to Facebook's data sharing practices and violations of the 2012 Consent Order when he sold his Class A Facebook shares for almost $8 billion.

I. Peggy Alford

623. As a member of the Board since March 2019, Alford faces a substantial risk of liability for the wrongs set forth herein.

624. Alford cannot exercise independent business judgment when considering a demand to institute litigation against Zuckerberg and other Individual

[278] *State of New York et. al. v. Facebook, Inc.*, Case No. 1:20-cv-03589-JEB, Complaint, at ¶ 178 (D.D.C. Dec. 9, 2020).

Defendants named herein. Since March 2019, Alford has served as Senior Vice President, Core Markets of PayPal, which was co-founded by Thiel. From May 2011 through August 2017, she held several positions at PayPal, including Vice President, Chief Financial Officer of Americas, Global Customer and Global Credit, and Senior Vice President of Human Resources, People Operations and Global Head of Cross Border Trade.

625. From September 2017 to February 2019, Alford served as Chief Financial Officer and Head of Operations for CZI. Zuckerberg envisions CZI as the vehicle for his philanthropic legacy and has expressed his wish to donate most of his wealth through it during his lifetime. Before the Cambridge Analytica crisis forced him to devote all his time to Facebook, he spent at least one day per week managing CZI. His wife, Priscilla Chan, devotes all of her time to running CZI. At the same time, CZI is structured as a limited liability company rather than as a non-profit, because of Zuckerberg's stated desire to have maximal flexibility and control over how to spend his money. Thus, Alford had a critical role at CZI, because she managed the finances there, and it is reasonable to infer that Zuckerberg views her as one of his most trusted advisers.

626. Moreover, during Alford's time at CZI, she demonstrated her loyalty to Defendant Zuckerberg, her employer, by launching an important CZI's initiative, the Summit Learning Program, which involving personal online learning. To

support this initiative, Alford oversaw the creation and maintenance of an online learning platform that looked and operated exactly like Facebook, and was accomplished with the support of Facebook's engineers.[279]

627. To roll out the initiative, CZI and the Summit Learning Program partnered with the non-profit T.L.P. Education, which allowed the Summit Learning Program to vastly expand its footprint in schools across the United States. Alford is also on the board at T.L.P., Education where she serves alongside Defendant Zuckerberg's spouse, Priscilla Chan.[280]

628. In 2019, CZI donated $24 million to T.L.P. Education. T.LP. Education then spun off the lucrative platform (and all its data) to a new non-profit that is managed by a board comprised of Defendant Zuckerberg, Chan, and Alford.

---

[279] Katie McNeill, *From Paper to Platform: Summit's Education Technology Story* SUMMIT LEARNING BLOG (Oct. 10, 2017), *available at*: https://blog.summitlearning.org/2017/10/summit-technology-story/. Indeed, during a July 11, 2015 director-only meeting, the Demand Board discussed [redacted] FB220-00000712 at 760. Only that [redacted] was not *Facebook's* opportunity, but rather CZI's opportunity using Facebook's technology, engineers, legal team, and resources.

[280] Alford and Chan serve on the board of T.L.P. Education.

J. Kenneth Chenault

629. As a member of the Board since February 2018, Chenault faces a substantial risk of liability for the wrongs set forth herein.

630. In January 2018, while Chenault was CEO of American Express, it [redacted]

631. Chenault is also on the board of the Harvard Corporation (also known as the President and Fellows of Harvard College), one of the two governing boards of Harvard University. The Chan Zuckerberg Initiative has provided numerous grants, totaling over $13 million, to Harvard since 2018.

632. As described *supra* ¶¶462–64, Chenault was the only director who [redacted] and felt compelled to conduct his own meetings with Zients for some semblance of independent discussion. Yet, for the almost two-year period following [redacted], Chenault has shown no inclination to oversee or correct Facebook's privacy policies, procedures, or practices, and has, along with the other directors, condoned Facebook's illegal business model. Chenault's decision not to stand for reelection after the Company's next annual meeting does not absolve him of his fiduciary obligations.

K. Andrew Houston

633. Houston cannot exercise independent business judgment when considering a demand to institute litigation against Zuckerberg. Houston is described by *The Wall Street Journal* as "a friend of Mr. Zuckerberg's who has appeared with him at social events." A *Fast Company* article about Houston's mentors mentions "close friend and Facebook CEO Mark Zuckerberg, who is known to pop into Dropbox HQ from time to time." Indeed, Defendant Zuckerberg's whose personal involvement in Dropbox's improper integration to Facebook's API is indicative of the deep, personal friendship that exists between the two.

634. In 2012, Zuckerberg was photographed driving Houston around at the Allen & Co Sun Valley Conference. The Sun Valley Conference is a prestigious annual media finance hosted by Allen & Co and intended to facilitate discussion and coordination among executives of technology and media companies.

635. Then, in 2013, according to an April 4, 2013 article from *Business Insider*, Zuckerberg hosted Houston at Facebook's headquarters to discuss means to coordinate Dropbox with Facebook's then-newly launched Home app.

636. In a June 24, 2015 interview with *Bloomberg*, Houston gushed about the Zuckerberg's mentorship:

> [Zuckerberg's] given me a lot of advice just on company scaling, how do you organize people, how do you set up these systems. As scale, you have to be more thoughtful about, how do you compensate people, how do you think about mundane things like their titles, on how people advance, how do you decide where to place bets, because you have early stage things, you have more mature products, you have this whole portfolio, how do you keep that running, when the challenges are so different at either end of the spectrum. It's a lot of things like that.

637. Like Andreessen and Thiel, Houston and Zuckerberg are also close friends in addition to their long-standing business relationship. For example, in

2017, Zuckerberg attended Houston's 34th birthday party at SPiN, a San Francisco ping pong social club.

638. The two have even co-founded companies together. For example, in 2013, Houston and Defendant Zuckerberg also co-founded FWD.us, a group that mobilizes the tech industry for immigration reform.

639. In addition to Houston's deep personal and business ties to Zuckerberg, Houston received a material benefit from the misconduct that resulted in the FTC's fine. Specifically, Houston has known about Facebook's Whitelisting Agreements since at least 2015, when he directly negotiated Drobox's Whitelist Agreement with Facebook, thereby enabling Dropbox to have continued access to Friends' API.[281]

[281] 643 Summaries, *supra* note 5, at 39 (citing FB-00046063-66).

Defendant Zuckerberg then personally contacted Houston to discuss the integration of Drobox to Facebook's API.[282]

640. In fact, Houston used this specialized access to Facebook users' and Friend's data to grow his business. Over the years, Dropbox has also been given unique opportunities to integrate with Facebook. In 2012, Facebook announced that Dropbox and Facebook accounts would be linked to provide "the ability to share files with friends in Facebook groups," reflecting full reciprocity of data sharing. In 2016, Dropbox reportedly landed an additional file sharing deal with "Facebook Messenger." In 2020, Dropbox got special permission to access Facebook's photo and video transfer tool to obtain and provide the free flow of photos and videos to and from Facebook to Dropbox accounts.

L. Robert Kimmitt

641. Kimmitt cannot impartially consider a demand to bring litigation against Bowles. Both are members of the Council of Foreign Relations. Chenault was also a member of the Council of Foreign Relations until 2018.

M. Tracey Travis

642. Travis cannot impartially consider a demand to bring litigation against Zuckerberg. Travis graduated from Columbia University and sits on the board of

[282] *Id*. at 121 (citing FB-00492545).

Columbia's business school. CZI has donated $1.9 million to Columbia University. CZI has also donated over $1.5 million to the Pittsburg Collaborative Project, a collaboration between Carnegie Mellon University and the University of Pittsburg, where Travis received her undergraduate degree.

N. Jeffrey Zients

643. As a member of the Board since May 2018, Zients faces a substantial risk of liability for the wrongs set forth herein.

644. Zients' wife, Mary Menell Zients, is on the board for Women for Women International alongside Sandberg.

645. In 2019 Zients received $404,873 in cash and restricted stock for his Board service. Zients also engaged in substantial insider sales while in the possession of material undisclosed information concerning Facebook, as described herein.

O. Nancy Killefer

646. Killefer cannot exercise independent business judgment when considering a demand to institute litigation against Sandberg and Bowles.

647. Killefer began working McKinsey & Company in 1979 and, with the exception of 1997-2000, was there until her retirement in August 2013, becoming a Senior Partner. She was a Senior Partner at McKinsey when Sheryl Sandberg was hired there. From 1997 to 2000 Killefer was Assistant Secretary for Management,

CFO, and COO at the U.S. Department of Treasury, during the same time period (1996 through 2001) that Sandberg was Chief of Staff for Treasury Secretary Lawrence Summers.

648. Killefer's tenure at the U.S. Department of Treasury also overlaps with the time Bowles spent as President Clinton's chief of staff, December 1996 through October 1998. Killefer is a Member Emeritus of the board of the Partnership for Public Service (she was board member 2009-2014), where Bowles is on the advisory board of governors. Bowles and Killefer served together on the Forum Committee for Springboard: Mid-Atlantic 2000, a program showcasing women-run businesses to potential investors.

VIII. DAMAGES TO THE COMPANY

649. As a result of the foregoing breaches of fiduciary duty, Facebook has incurred significant expenses, and will continue to expend significant sums, including:

(a) the over $5 billion in damages already incurred by the Company as a result of fines from regulatory activity taken by the FTC, DOJ, SEC, and other regulatory agencies and authorities;

(b) the risk of having Facebook's users and advertisers abandon the Facebook platform as a result of a loss of confidence in Facebook's ability to handle, maintain and control sensitive information;

(c) the costs incurred to carry out internal investigations, including the costs of legal and other fees paid to outside counsel, auditors, and other experts,

(d) the costs incurred to rectify the Company's corporate governance failures, including any mandatory compliance measures instituted by the FTC;

(e) losses incurred as a result of the Insider Trading Defendants' misuse of Facebook's proprietary and material non-public information;

(f) compensation improperly paid to the Individual Defendants throughout the Relevant Period;

(g) loss in market value and shareholder equity;

(h) damage to Facebook's reputation and goodwill; and

(i) legal fees, costs, and amounts payable in settlement or satisfaction of lawsuits brought against the Company related to the foregoing wrongdoing.

650. Facebook has been directly and substantially injured by reason of the Individual Defendants' intentional breach and/or reckless disregard of their fiduciary duties of loyalty to the Company. Plaintiffs, as a stockholders and representatives of Facebook, seek damages and other relief for the Company.

IX. CLAIMS FOR RELIEF

COUNT I
Breach of Fiduciary Duty
(Against Zuckerberg, Sandberg and Papamiltiadis)

651. Plaintiffs incorporate by reference all prior paragraphs as if fully set forth herein.

652. As officers of Facebook, Zuckerberg Sandberg, and Papamiltiadis had a fiduciary duty to act with due care and loyally towards the Company and its stockholders.

653. Article III of Facebook's Certificate of Incorporation sets forth its purpose: "to engage in any lawful act or activity for which corporations may be organized under the General Corporation Law of the State of Delaware." Moreover, under Delaware law, a fiduciary cannot operate a corporation in an illegal manner, even if doing so is profitable for the corporation.

654. In violation of their fiduciary duties of care and loyalty, Zuckerberg, Sandberg and Papamiltiadis have knowingly and intentionally operated Facebook in contravention of law. Most glaringly, these defendants caused Facebook to violate the 2012 Consent Order, resulting in a $5 billion fine borne by Facebook and its stockholders while wrongfully shielding Zuckerberg from personal liability. Facebook's violation of the 2012 Consent Order and laws and regulations governing data privacy was not a result of tangential business operations, rouge employees or

good-faith misinterpretations of the law, but a top-down concerted effort to operate Facebook's core business in an illegal manner.

655. Plaintiffs bring this action to stop Zuckerberg, Sandberg and Papamiltiadis from operating Facebook in contravention of its Certificate of Incorporation, and to recover damages caused thereby. Plaintiffs have no adequate remedy at law.

COUNT II
Breach of Fiduciary Duty
(Against the Director Defendants—Zuckerberg, Sandberg, Alford, Andreessen, Chenault, Thiel, Zients, Bowles, Desmond-Hellmann, Hastings and Koum)

656. Plaintiffs incorporate by reference all prior paragraphs as if fully set forth herein.

657. By reason of their positions as officers and directors of the Company and because of their ability to control the business and corporate affairs of the Company, the Individual Defendants named in this Count owed the Company and its shareholders fiduciary obligations of good faith, loyalty, and candor, and were required to use their utmost ability to control and manage the Company in a fair, just, honest, and equitable manner. The Individual Defendants were required to act in furtherance of the best interests of the Company and its shareholders so as to benefit all shareholders equally, and not in furtherance of their personal interests or benefit. Each director and officer of the Company owed to the Company and its

shareholders a fiduciary duty to exercise good faith and diligence in the administration of the affairs of the Company, ensuring the Company's business was being conducted lawfully, and in the use and preservation of its property and assets, and the highest obligations of fair dealing.

658. The Individual Defendants, because of their positions of control and authority as directors and/or officers of the Company, were able to and did, directly and/or indirectly, exercise control over the wrongful acts complained of herein.

659. The Individual Defendants violated and breached their fiduciary duties of candor, good faith and loyalty. More specifically, the Individual Defendants violated their duty of good faith by creating a culture within Facebook formed on the basis of full reciprocity, that prioritized profits and disregarded the Company's legal obligation to obtain user consent before sharing personal user information with third-parties, and/or consciously failing to prevent the Company from engaging in the wrongful acts complained of herein. The Individual Defendants thus caused and/or allowed Facebook to surreptitiously collect massive amounts of personal user information through unfair, deceptive and illegal trade practices in violation of the 2012 Consent Order. This collection was done in furtherance of Facebook's business plan grounded in the full reciprocity of data sharing with third-party developers, which was developed by the Individual Defendants.

660. The Individual Defendants were each involved in the illegal activity, or aware of it and failed to act to stop it. To the extent any Individual Defendant was unaware of the illegal activity set forth therein, such Individual Defendant was reckless in disregarding their duties to monitor the Company's core operations.

661. As a direct and proximate result of the Individual Defendants' breaches of their fiduciary obligations, Facebook bas sustained damages, as alleged herein. As a result of the misconduct alleged herein, the Individual Defendants are liable to the Company.

662. Plaintiffs, on behalf of Facebook, have no adequate remedy at law.

COUNT III
***Brophy* Claim for Exploiting the Company's Material Non-Public Information**
(Against the Insider Trading Defendants)

663. Plaintiffs incorporate by reference all prior paragraphs as if fully set forth herein.

664. As directors and officers of the Company at the time they sold shares of Facebook stock, the Insider Trading Defendants owed Facebook and its stockholders a fiduciary duty of loyalty and good faith.

665. At the time of the Insider Trading Defendants' stock sales, the Insider Trading Defendants were in possession of material, adverse, non-public information as alleged herein, and sold Company stock on the basis of such information.

666. The information described above was proprietary, non-public information material to the Company's compliance with its affirmative legal obligations arising under the 2012 Consent Order, among other data privacy laws and regulations. It was a proprietary asset belong to the Company, which the Insider Trading Defendants exploited for their own benefit in connection with their stock sales.

667. At the time of the Insider Trading Defendants' stock sales, the Insider Trading Defendants possessed information concerning the Company's pervasive whitelisting practice and other means by which third-party platform developers were given access to users' personal information without the user's consent. The Insider Trading Defendants were also aware of the Company's affirmative obligations under the 2012 Consent Order and the attendant risk of future fines and violations on the Company's prospects. The Insider Trading Defendants' sale of Facebook stock while in possession of the materially adverse, non-public information described herein was a breach of the Insider Trading Defendants' fiduciary duties of loyalty and good faith.

668. As the use of Company's proprietary information for their own gain constitutes a breach of the Insider Trading Defendants' fiduciary duties, the Company is entitled to disgorge and impose a constructive trust on any illegal profits obtained thereby.

669. Plaintiffs, on behalf of Facebook, have no adequate remedy at law.

X. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs request the following relief:

A. An order declaring that Plaintiffs may maintain this action on behalf of Facebook, and that Plaintiffs are adequate representatives of the Company;

B. An order declaring that Defendants have breached their fiduciary duties to Facebook;

C. An order determining and awarding to Facebook the damages sustained by it as a result of the violations set forth above by Defendants, jointly and severally, together with pre-judgment and post-judgment interest thereon;

D. An order imposing a constructive trust upon and ordering disgorgement of all profits made, or all losses avoided, by the Insider Trading Defendants as a result of the fiduciary breaches alleged herein, together with pre-judgment and post-judgment interest thereon;

E. An order directing Facebook and Defendants to take all necessary actions to reform and improve its corporate governance and internal procedures to comply with applicable laws and to protect Facebook and its shareholders from a repeat of the wrongful conduct described herein;

F. Awarding Plaintiffs their costs and disbursements for this action, including reasonable attorneys' fees and expenses; and

G. Granting such other relief as this Court deems just and appropriate.

Dated: July 20, 2021

PRICKETT, JONES & ELLIOTT, P.A.

By: */s/ Samuel L. Closic*
Kevin H. Davenport (#5327)
Samuel L. Closic (#5468)
John G. Day (#6023)
Elizabeth Wang (#6620)
1310 King Street
Wilmington, DE 19801
Tel: 302-888-6500

Proposed Co-Lead Counsel and Counsel to Plaintiffs Construction and General Building Laborers' Local No. 79 General Fund, City of Birmingham Retirement and Relief System and Lidia Levy

OF COUNSEL:

SCOTT+SCOTT ATTORNEYS AT LAW LLP
Geoffrey M. Johnson
12434 Cedar Road
Suite 12
Cleveland Heights, OH 44106
Tel: 216-229-6088

Donald A. Broggi
William C. Fredericks
Scott R. Jacobsen
Jing-Li Yu (#6483)
The Helmsley Building
230 Park Avenue,
17th Floor
New York, NY 10169
Tel: 212-223-6444

Proposed Co-Lead Counsel and Counsel for Plaintiff City of Birmingham Retirement and Relief System

OF COUNSEL:

KAPLAN FOX & KILSHEIMER LLP
Frederic S. Fox
Laurence D. King
Hae Sung Nam
Donnie Hall
Aaron Schwartz
850 Third Avenue
New York, NY 10022
Tel: 212 687-1980

Proposed Co-Lead Counsel and Counsel for Plaintiffs California State Teachers' Retirement System and Firemen's Retirement System of St. Louis

HACH ROSE SCHIRRIPA & CHEVERIE LLP
Frank R. Schirripa
Daniel B. Rehns
Kurt M. Hunciker
112 Madison Avenue
10th Floor
New York, NY 10016
Tel: 212-213-8311

Counsel to Plaintiff Construction and General Building Laborers' Local No. 79 General Fund, and Additional Counsel to Plaintiffs

ROBBINS LLP
Brian J. Robbins
Stephen J. Oddo
Gregory E. Del Gaizo
Robbins LLP
5040 Shoreham Place
San Diego, CA 92122
Tel: 619-525-3990

Additional Counsel for Plaintiffs

DILWORTH PAXSON LLP
Catherine Pratsinakis (#4820)
1500 Market Street, Suite 3500E
Philadelphia, PA 19012
Tel: 215-575-7013

Counsel to Plaintiff Karen Sbriglio

GAINEY McKENNA & EGLESTON
Thomas J. McKenna
Gregory M. Egleston
501 Fifth Avenue
19th Floor
New York, NY 10017
Tel: 212 983-1300

Additional Counsel for Plaintiffs

BERMAN TABACCO
Joseph J. Tabacco, Jr.
Daniel E. Barenbaum
44 Montgomery Street
Suite 650
San Francisco, CA 94104
Tel: 415-433-3200

Additional Counsel for Plaintiffs

DILWORTH PAXSON LLP
Thaddeus J. Weaver (#2790)
704 King Street
Suite 500
P.O. Box 1031
Wilmington, DE 19899
Tel: 302-571-8867

Counsel to Plaintiff Karen Sbriglio and Additional Plaintiffs

ANDREWS & SPRINGER, LLC
Peter B. Andrews (#4623)
Craig J. Springer (#5529)
David M. Sborz (#6203)
4001 Kennett Pike, Ste 250
Wilmington, DE 19807
Tel: 302-504-4957

COTCHETT PITRE & McCARTHY LLP
Joseph W. Cotchett
Mark Molumphy
840 Malcolm Road
Suite 200
Burlingame, CA 90410
Tel: 650-697-6000

Additional Counsel for Plaintiffs

CERTIFICATE OF SERVICE

I, Samuel L. Closic, do hereby certify on this 6th day of August, 2021, I caused a copy of the foregoing to be served via File and Serve*Xpress* upon the following counsel:

David E. Ross, Esq.
R. Garrett Rice, Esq.
ROSS ARONSTAM & MORITZ LLP
100 S. West Street, Suite 400
Wilmington, Delaware 19801

Jon E. Abramczyk, Esq.
Alexandra Cumings, Esq.
MORRIS, NICHOLS, ARSHT & TUNNEL LLP
1201 North Market St.,16th Floor
Wilmington, Delaware 19801

Nathan A. Cook, Esq.
BLOCK & LEVITON LLP
3801 Kennett Pike, Suite C-305
Wilmington, Delaware 19807

Blake A. Bennett, Esq.
COOCH AND TAYLOR, P.A.
The Brandywine Building
1000 West Street, 10th Floor
Wilmington, Delaware 19899

Kurt M. Heyman, Esq.
Aaron M. Nelson, Esq.
HEYMAN ENERIO GATTUSO & HIRZEL LLP
300 Delaware Avenue, Suite 200
Wilmington, Delaware 19801

Daniel K. Astin, Esq.
CIARDI CIARDI & ASTIN
1204 N. King St.
Wilmington, Delaware 19801

/s/ *Samuel L. Closic*
Samuel L. Closic (Del. No. 5468)