

1 JOSEPH W. COTCHETT (SBN 36324)
jcotchett@cpmlegal.com
2 MARK C. MOLUMPHY (SBN 168009)
mmolumphy@cpmlegal.com
3 BRIAN DANITZ (SBN 247403)
bdanitz@cpmlegal.com
4 STEPHANIE D. BIEHL (SBN 306777)
sbiehl@cpmlegal.com
5 GINA STASSI (SBN 261263)
gstassi@cpmlegal.com

6 **COTCHETT, PITRE & MCCARTHY, LLP**
San Francisco Airport Office Center
7 840 Malcolm Road, Suite 200
Burlingame, CA 94010
8 Telephone: (650) 697-6000
Facsimile: (650) 697-0577

9 *Lead Counsel for Plaintiffs*

10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA**

**IN RE FACEBOOK, INC.
SHAREHOLDER DERIVATIVE
PRIVACY LITIGATION**

This Document Relates to:

ALL ACTIONS

Lead Case No. 4:18-cv-01792-HSG

**CONSOLIDATED SHAREHOLDER
DERIVATIVE COMPLAINT FOR:**

- (1) **VIOLATION OF SECTION 14(A)
OF THE EXCHANGE ACT;**
- (2) **VIOLATION OF SECTION 10(B)
OF THE EXCHANGE ACT;**
- (3) **MISAPPROPRIATION OF
INFORMATION AND BREACH OF
FIDUCIARY DUTY FOR INSIDER
SALES**
- (4) **VIOLATION OF CAL. CORPS.
CODE §§ 25402 AND 25403;**
- (5) **BREACH OF FIDUCIARY DUTY;**
- (6) **CONTRIBUTION AND
INDEMNIFICATION; AND**
- (7) **AIDING AND ABETTING BREACH
OF FIDUCIARY DUTY.**

**DEMAND FOR JURY TRIAL
ON ALL ISSUES SO TRIABLE**

TABLE OF CONTENTS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

| | Page |
|--|------|
| <u>NATURE OF THE ACTION</u> | 1 |
| <u>JURISDICTION AND VENUE</u> | 5 |
| <u>INTRADISTRICT ASSIGNMENT</u> | 6 |
| <u>PARTIES</u> | 6 |
| <u>BACKGROUND FACTS</u> | |
| I. DEFENDANTS WERE OBLIGATED TO SAFEGUARD THE COMPANY’S INTERESTS AND COMPLY WITH APPLICABLE LAWS | 8 |
| II. BACKGROUND OF THE COMPANY AND ITS BUSINESS | 11 |
| A. The Facebook Platform Allows Apps, Websites, and Devices to Access and Use the Personal Information of Billions of Users | 12 |
| B. Facebook’s Core Advertising Business Is the Primary Source of the Company’s Revenue | 13 |
| III. FACEBOOK’S TRANSFORMATION FROM “SOCIAL NETWORK” TO DATA GATHERING EMPIRE | 15 |
| A. Facebook Worked with Third Party Companies, Including Competitors, to Gain Access to Data Since 2007 | 15 |
| B. Defendants Expand Facebook’s Platform To App Developers | 17 |
| C. Defendants Transitioned Facebook’s Advertising Business to Mobile Devices Beginning in 2011 and the Company’s Revenues Skyrocketed | 18 |
| D. Facebook Purchased Data From Third Party Data Brokers Since at Least 2012 | 18 |
| E. The Board Increased Facebook’s Lobbying Expenditures and Efforts to Influence Legislators Rather Than Adopting Reasonable Privacy Practices to Protect Users and Comply with Existing Laws | 21 |
| IV. THE BOARD FAILED TO ENFORCE FACEBOOK’S POLICIES AND TURNED A BLIND EYE TO REPEATED VIOLATIONS OF DATA PRIVACY LAWS | 22 |
| A. Defendants Maintained Policies That Permitted Developers to Obtain Facebook Users’ Personal Information | 25 |

1 **B. Facebook Expanded Graph API in 2014 and Allowed Third Party**
2 **Developers to Access Users’ Inboxes on Facebook Messenger27**

3 **C. Defendants Falsely Assured Facebook’s Users That They Could Trust**
4 **Facebook to Protect Their Personal Information29**

5 **D. Defendants were Warned About Data Security Issues in 2012 By**
6 **Whistleblower Sandy Parakilas But Did Nothing30**

7 **E. Defendants Knew About The Cambridge Analytica “Breach” in 2015 But**
8 **Concealed The Fact And Failed To Act.....32**

9 **F. U.S. and Foreign Government Officials Commenced Investigations of**
10 **Facebook in Response to the Scandal.....41**

11 1. Facebook’s Terms of Use Are Designed to Entice Users to Grant the
12 Company Access to Their Data43

13 2. Facebook’s Users Did Not Consent to Provide Their Personal Information
14 to Third Parties or to Any Alteration or Aggregation of the Data for a
15 Commercial Use.....45

16 3. A German Court Found Facebook’s Privacy Settlements and Terms are
17 Invalid to Obtain Consent in 2018 50

18 **G. Early Litigation and Complaints About Facebook’s Privacy Violations**
19 **Should Have Prompted the Board to Implement Reasonable Controls51**

20 1. The FTC Complaint Alleged that Facebook’s Statements About its
21 Privacy Practices Were Unfair, Deceptive, and Violated Law 53

22 2. Defendants Ignored Concerns Raised By Facebook’s Chief Information
23 Security Officer About the Security of Facebook’s Platform.....59

24 3. Former Zuckerberg Mentor Warned of Data Security Issues in 2016.....60

25 **V. DEFENDANTS ALLOWED FACEBOOK TO ENGAGE IN ILLEGAL AND**
26 **DECEPTIVE BUSINESS PRACTICES FOR MORE THAN A DECADE.....62**

27 **A. Facebook’s Agreements with Third Party “Service Providers” Violated the**
28 **Consent Decree.....64**

B. PwC Improperly Certified That Facebook’s Privacy Program Satisfied the
 FTC Consent Decree in Audit Reports from 2013- 201766

C. Facebook’s Acquisition of WhatsApp Violated the European Union’s
 Merger Regulation 71

D. The FTC is Investigating Possible Consent Decree Violations 75

E. Zuckerberg’s Testimony at the U.S. Congressional Hearings in April 2018
 Was Evasive and Misleading..... 79

1 F. CTO Mike Schroepfer Testified Before the European Parliamentary
Committee in May 2018.....82

2

3 G. Defendant Zuckerberg Reluctantly Testified Before the EU Parliamentary
Committee in May 2018.....83

4

5 H. Facebook Has Been Repeatedly Fined for Violations of Foreign Privacy
Laws, and Recent Reports Suggest They Are Ongoing.....87

6 1. The European Commission Found the WhatsApp Acquisition Violated
the EU Merger Regulation and Fined Facebook €110 Million.....89

7 2. The German Supreme Court Declared Facebook’s “Friend Finder”
Feature Unlawful in 201690

8 3. The Spanish Agency for Data Protection Fined Facebook €1.2 Million
Euros in 201790

9 4. The French Data Protection Authority Fined Facebook its Maximum
Allowable Fine in 2017.....91

10 5. A German Court Found Facebook’s Default Settings are Illegal and
Facebook’s Terms of Service are Invalid to Obtain Consent in 201891

11 6. Facebook Was Ordered to Stop Tracking Internet Usage and Faces Up to
€100 Million in Fines.....92

12

13 VI. DEFENDANTS VIOLATED SECTION 14(A) OF THE EXCHANGE ACT AND
SEC RULE 14A-9 BY ISSUING MATERIALLY MISLEADING PROXY
14 STATEMENTS IN 2016, 2017 AND 201892

15

16 A. The Board Issued the Materially Misleading Proxy Statements in
17 Recommending a Vote AGAINST Shareholder Proposals on the Basis of the
Directors’ Misstatements About Facebook’s Privacy Practices and Board
Oversight.....93

18

19 B. The Board Issued the Materially Misleading Proxy Statement in Soliciting
20 the Directors’ Re-Election to Facebook’s Board and Compensation Packages
.....94

21 VII. DEFENDANTS VIOLATED SECTION 10(b) OF THE EXCHANGE ACT AND
SEC RULE 10b-5 BY KNOWINGLY OR RECKLESSLY ISSUING
22 MATERIALLY FALSE AND MISLEADING STATEMENTS.....95

23 VIII. CERTAIN DEFENDANTS SOLD THEIR FACEBOOK STOCK WHILE IN
24 POSSESSION OF MATERIAL, NONPUBLIC INFORMATION.....100

25 IX. DAMAGES TO FACEBOOK102

26 X. DEMAND ON FACEBOOK’S BOARD WAS FUTILE AND THUS, EXCUSED 103

27 A. Demand Is Excused Because the Board’s Conduct Did Not Constitute a
28 Valid Exercise of Business Judgment.....104

1 **B. Demand Is Excused Because Defendants Face a Substantial Likelihood of**
2 **Liability for Their Roles in Perpetuating Facebook’s Illegal Business**
3 **Practices104**
4 1. The Board Approved Executive Compensation Practices That Encouraged
5 the Unlawful Activity 105
6 2. The Board Failed to Comply with the 2011 FTC Consent Decree and Has
7 Exposed Facebook to Further Sanctions 107
8 **C. Facebook is “Controlled” By Zuckerberg and He Dominates the Board....109**
9 1. Demand was Futile as to Defendant Thiel 113
10 2. Demand was Futile as to Defendant Andreesen 115
11 3. Demand was Futile as to Defendant Hastings 118
12 4. Demand was Futile as to Defendant Sandberg 118
13 5. Demand was Futile as to Defendant Bowles 121
14 6. Demand was Futile as to Defendant Desmond-Hellmann 122
15 7. Demand was Futile as to Facebook Director Ken Chenault 123
16 **CAUSES OF ACTION124**
17 **FIRST CAUSE OF ACTION..... 124**
18 **Violation of Section 14(a) of the Exchange Act and SEC Rule 14a-9**
19 **SECOND CAUSE OF ACTION..... 124**
20 **Violation of Section 10(b) of the Exchange Act and SEC Rule 10b-5**
21 **THIRD CAUSE OF ACTION 129**
22 **Misappropriation of Information and Breach of Fiduciary Duty for Insider**
23 **Sales**
24 **FOURTH CAUSE OF ACTION 130**
25 **Violation of Section 25402 of the California Corporations Code**
26 **FIFTH CAUSE OF ACTION 130**
27 **Violation of Section 25403 of the California Corporations Code**
28 **SIXTH CAUSE OF ACTION 131**
29 **Breach of Fiduciary Duty**
30 **SEVENTH CAUSE OF ACTION 135**
31 **Contribution and Indemnification**
32 **EIGHTH CAUSE OF ACTION 136**
33 **Aiding and Abetting Breaches of Fiduciary Duty**
34 **PRAYER FOR RELIEF 139**
35 **JURY DEMAND 140**

1 Plaintiffs Jeremiah F. Hallisey, Ronald Martin, Natalie Ocegueda, James Karon, and
 2 The Gloria Stricklin Trust (collectively, “Plaintiffs”), shareholders of Facebook, Inc.
 3 (“Facebook” or the “Company”), bring this action on Facebook’s behalf seeking relief under
 4 federal and state laws for the misconduct perpetrated against the Company by its current and
 5 former officers and directors identified below (collectively, “Defendants”). Plaintiffs, through
 6 counsel, conducted an investigation of the facts supporting the allegations in this Complaint,
 7 and believe discovery will elicit further evidentiary support for the allegations herein.

8 NATURE OF THE ACTION

9 1. This case concerns pervasive breaches of fiduciary duty, misrepresentations and
 10 omissions by the named Defendants, Directors and Senior Officers of Facebook, relating to the
 11 Company’s handling of the confidential and private data of **tens of millions** users of
 12 Facebook’s social media platform. **It represents one of the worst examples of privacy abuse**
 13 **in the age of social media, and impacted Facebook as well as our nation’s democratic**
 14 **processes – all in the name of profit.**

15 2. Back in **2011**, Facebook was forced to adhere to strict user data protection
 16 measures as part of a **consent decree** with the Federal Trade Commission (“FTC Consent
 17 Decree”).¹ The Consent Decree required Facebook to, among other things, “establish and
 18 implement, and thereafter maintain, a comprehensive privacy program that is reasonably
 19 designed to address ... privacy risks related to the development and management of new and
 20 existing products and services for consumers” Defendants failed to comply with the
 21 decree.

22 3. On **December 11, 2015**, *The Guardian* published an article which showed the
 23 public that an English company, Cambridge Analytica, was paying researchers at Cambridge
 24 University to gather detailed personal data from a massive pool of unwitting Facebook users in
 25 order to create psychological profiles of U.S. voters to influence elections. Facebook

26 ¹ See Agreement Containing Consent Order, Fed. Trade Comm’n, *In the Matter of Facebook,*
 27 *Inc.*, File No. 092 3184 (Nov. 29, 2011) (“Consent Agreement”), available at
 28 <https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf>.
 The Decision and Order, Fed. Trade Comm’n, *In the Matter of Facebook, Inc.*, File No. 092
 3184 (July 27, 2012) is attached hereto as **Exhibit 1**.

1 immediately assured shareholders that misusing user data would be met with strict
2 consequences, and that it was in **full compliance** with the FTC Consent Decree.

3 4. On **June 29, 2018**, Facebook revealed in its report to Congress, that Facebook
4 and its Board of Directors not only failed to protect users' information, but intentionally shared
5 it with developers and hardware and software makers, including some of the largest companies
6 in the world, many of whom still have access to user information.

7 5. Despite being aware since 2015 that Cambridge Analytica and other third parties
8 had amassed data from millions of Facebook's users, management has done virtually nothing in
9 response. To the contrary, the Company's executive management and Board of Directors –
10 defendants herein – consistently misrepresented to users and shareholders that it had a
11 comprehensive privacy program in place, that it notified users if their information had been
12 compromised, and that it required third-party developers to adhere to strict confidentiality
13 provisions, much of which was misrepresented to shareholders.

14 6. On **March 17, 2018**, *The Guardian* published another dramatic report describing
15 how Facebook allowed Cambridge Analytica to misappropriate and retain the personal data of
16 **50 million** users in order to target them with **personalized political advertisements**. *The*
17 *Guardian's* investigation included documents provided by a whistleblower named Christopher
18 Wylie, a data analytics expert that formerly worked at Cambridge Analytica.

19 7. On **March 18, 2018**, *The New York Times* reported that members of Congress
20 called for an investigation of the Facebook data leak, and pressing Facebook's Chairman and
21 CEO, Mark Zuckerberg, to appear before the Senate Judiciary Committee to explain what the
22 social network knew about the misuse of its data **“to target political advertising and**
23 **manipulate voters.”** The article was a blow to the shareholders of Facebook.

24 8. On **March 20, 2018**, *The Guardian* followed up with a report from a Facebook
25 whistleblower, Sandy Parakilas, a former platform operations manager at Facebook, who
26 revealed that Facebook routinely shared user data without consent, had **“no idea what**
27 **developers were doing with the data,” “did not use its enforcement mechanisms” to**
28 **remedy known violations, and that the whistleblower had “warned senior executives at**

1 **the company,”** but that **“Facebook was in a stronger legal position if it didn’t know about**
2 **the abuse that was happening. . . . They felt that it was better not to know.”**²

3 9. On **March 26, 2018**, the FTC issued a press release confirming that it was
4 investigating Facebook’s privacy practices and compliance with the 2011 consent decree.

5 10. On **April 10 and 11, 2018**, Mark Zuckerberg appeared before Congress and
6 **apologized** for Facebook’s conduct, but tried to downplay the extent of the unauthorized use of
7 user data to the acts of a single, rogue company which intentionally skirted Facebook’s privacy
8 policies. According to Zuckerberg, Facebook had effectively restricted the disclosure of users’
9 personal information to outsiders in 2015, when it implemented new policies. This was a sham
10 and the Directors **knew it was false**.

11 11. On **April 13, 2018**, in the midst of the Cambridge Analytica scandal, Defendants
12 issued Facebook’s annual Proxy Statement (the “2018 Proxy Statement”), soliciting their re-
13 election to Facebook’s Board at the annual meeting scheduled for the following month.
14 Shockingly, Defendants did not disclose *anything* about the scandal. The 2018 Proxy
15 Statement did not contain a single statement regarding Cambridge Analytica, and it also failed
16 to disclose material facts concerning the FTC’s investigation into possible violations of the
17 Consent Decree. Defendants **recommended** that Facebook’s shareholders vote **AGAINST** the
18 proposals to create a new committee of the Board and to require reports that would enhance the
19 Board’s oversight of the very issues that gave rise to the scandal and to multiple government
20 investigations, and that have caused serious harm to Facebook. The Board’s recommendations,
21 like the rest of the 2018 Proxy Statement, were false and misleading because they fail to
22 disclose material facts concerning Facebook’s business practices and the Company’s policies
23 relating to gathering and sharing Facebook information and user data with third parties; instead,
24 Defendants assured Facebook’s stockholders that the Company’s “current corporate
25 governance structure is sound and effective.” Nothing could be further from the truth.
26

27 _____
28 ² See <https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas>.

1 12. On **June 29, 2018**, in response to Congressional questions to Zuckerberg,
 2 Facebook provided a 747 page document and **admitted** that it actually gave dozens of
 3 companies **special access** to user data, contrasting with the Company's prior public
 4 statements.³ Indeed, Facebook disclosed that it was still sharing information of users' friends,
 5 such as name, gender, birth date, current city or hometown, photos and page likes, with over 60
 6 app developers nearly six months after it said it stopped access to this data in 2015. Facebook
 7 also disclosed that it shared information about its users with 52 hardware and software makers,
 8 including such large United States corporations as Amazon.com, Apple Inc. and Microsoft
 9 Corp, as well as Chinese firms such as Huawei Technologies Co. and Alibaba Group. Fourteen
 10 companies continue to have access to information about Facebook's users.

11 13. As these recent reports make public, Defendants have repeatedly concealed
 12 critical facts that are necessary to inform users and comply with applicable law. This has
 13 severely damaged the Company's reputation and imposed significant costs, including due to
 14 the massive amounts of regulatory interest, inquiry, and investigations commenced in the wake
 15 of the Cambridge Analytica scandal. In addition, the Company has suffered a loss of user trust,
 16 harm to its core advertising business, and other damages associated with its exposure to
 17 litigation, regulation, fines, and other penalties. If Facebook is found to have violated the FTC
 18 Consent Decree, the Company could face billions more in fines and penalties.

19 14. Facebook lost **\$50 billion** in market value in the first two days following public
 20 revelation of the Cambridge Analytica scandal. The Board and senior executives have failed—
 21 repeatedly, and brazenly—to serve the best interests of Facebook, its shareholders, and the
 22 public at large. As a result of their misconduct, Defendants are liable to the Company for their
 23 **violations of federal law**, as well as for breach of their fiduciary duties and other violations of
 24 state laws, and all the costs and penalties now laid upon Facebook.

25
 26 _____
 27 ³ Plaintiffs incorporate by reference Facebook's June 29, 2018 responses to the House Energy
 28 and Commerce Questions for the Record, available at:
<https://docs.house.gov/meetings/IF/IF00/20180411/108090/HHRG-115-IF00-Wstate-ZuckerbergM-20180411-SD003.pdf>.

1 15. Plaintiff Shareholders seek to recover on behalf of Facebook, the damages
 2 caused by Defendants’ wrongdoing, and other equitable remedies for Facebook, including
 3 appropriate injunctive relief, if necessary on an expedited basis if necessary to prevent potential
 4 future or additional violations of the Consent Decree caused by Defendants’ ongoing
 5 compliance failures and structural deficiencies that are continuing to cause further harm and
 6 damage to Facebook. Shareholder plaintiffs, on behalf of Facebook, are entitled to such relief;
 7 in light of Defendants’ wrongdoing that is ongoing and is continuing to cause harm to
 8 Facebook, demand on Facebook’s Board was clearly futile, and is excused, because Defendants
 9 are liable for their wrongful conduct and will not pursue litigation or take any other action to
 10 recover for Facebook an appropriate remedy for the wrongdoing and claims alleged herein.

JURISDICTION AND VENUE

12 16. This Court has subject matter jurisdiction over this action under Article III of the
 13 United States Constitution and 28 U.S.C. § 1331 because of claims arising under Section 14(a)
 14 of the Exchange Act, 15 U.S.C. § 78n(a), and SEC regulation 14a-9 promulgated thereunder,
 15 over which the Court has exclusive jurisdiction under Section 27 of the Exchange Act, 15
 16 U.S.C. § 78aa. This Court has jurisdiction over the state-law claims in accordance with 28
 17 U.S.C. § 1367.

18 17. This Court has jurisdiction over each of the named Defendants because each
 19 defendant has sufficient contacts with California in order to render the exercise of jurisdiction
 20 by this Court over them permissible under California Code of Civil Procedure § 410.10 as well
 21 as the United States and California Constitutions and traditional notions of fair play and
 22 substantial justice. Facebook is headquartered in California, and Facebook’s Terms of Service
 23 provides that users of the Company’s website “**agree to submit to the personal jurisdiction**
 24 **of [this] court[]**” and that “**the laws of the State of California will govern these Terms and**
 25 **any claim, ...without regard to conflict of law provisions.**” Through their misconduct,
 26 Defendants caused substantial harm and injury in California to California citizens, and
 27 shareholders nationwide. According to the “State-by-State Breakdown of People Whose
 28 Facebook Information May Have Been Improperly Shared with Cambridge Analytica”

1 published by Facebook on its website, the Company estimates that there are 6,787,507 “Total
2 Impacted Users” from California, the most of any state.

3 18. This action is not a collusive one to confer jurisdiction that the court would
4 otherwise lack.

5 INTRADISTRICT ASSIGNMENT

6 19. Venue is proper in this District in accordance with Section 27 of the Exchange
7 Act. Venue is also proper under 28 U.S.C. § 1391(b) because: (i) Facebook maintains its
8 principal place of business in this District, and has its most significant contacts with the
9 Northern District of California; (ii) one or more of the Defendants resides in this District;
10 (iii) Defendants received substantial compensation in this District by doing business here and
11 engaging in numerous activities that had effects in this District; and (iv) a substantial portion of
12 the transactions and wrongs complained of in this Complaint occurred in San Mateo County,
13 California, and as such assignment to the San Francisco division is appropriate.

14 20. Venue is also proper in this District because Facebook’s Terms of Service
15 provides that “any claim, cause of action, or dispute ... that arises out of or relates to these
16 Terms or the Facebook Products” may be brought “exclusively in the U.S. District Court for
17 the Northern District of California or a state court located in San Mateo County.” *See*
18 <https://www.facebook.com/legal/terms> (last accessed June 13, 2018). Facebook’s website
19 states that the Terms of Service “include our commitments to people.”

20 PARTIES

21 Plaintiffs

22 21. Plaintiff **Jeremiah F. Hallisey** is a current shareholder of Facebook stock, and
23 has continuously held his Facebook stock since July 2013.

24 22. Plaintiff **Ronald Martin** is a current shareholder of Facebook stock and has
25 continuously held his Facebook stock since 2012.

26 23. Plaintiff **Natalie Ocegueda** is a current shareholder of Facebook stock and has
27 continuously held her Facebook stock since May 21, 2012. Plaintiff Ocegueda is also a current
28 user of Facebook’s social networking website user and was a user at the time of the events

1 alleged herein.

2 24. Plaintiff **James Karon**, a resident of Georgia, is a current shareholder of
3 Facebook stock and has continuously held his Facebook stock since March 22, 2017.

4 25. Plaintiff **The Gloria Stricklin Trust** is a current shareholder of Facebook stock
5 and has continuously held its Facebook stock since May 2012.

6 **Nominal Defendant**

7 26. Nominal defendant **Facebook** is a Delaware corporation headquartered at 1601
8 Willow Road, Menlo Park, CA 94025. Accordingly, Facebook is a citizen of Delaware and
9 California. Facebook's securities trade on the NASDAQ under the ticker symbol "FB."

10 **Individual Defendants**

11 27. Defendant **Mark Zuckerberg** ("Zuckerberg") is Facebook's Founder, Chairman
12 and Chief Executive Officer. Zuckerberg is responsible for Facebook's day-to-day operations,
13 as well as the overall direction and product strategy of the Company. Zuckerberg is the
14 Company's controlling stockholder with ownership of stock and proxies for stock representing
15 more than 53.3% of Facebook's voting power, though he owns 16% of Facebook's total equity
16 value.

17 28. Defendant **Sheryl Sandberg** ("Sandberg") is Facebook's Chief Operating Officer
18 ("COO") since 2008, overseeing the Company's business operations, and has been a Facebook
19 director since 2012.

20 29. Defendant **Marc Andreessen** ("Andreessen") is a Facebook director and has
21 been since June 2008. Andreessen is also a member of Facebook's Audit Committee and was a
22 member of Facebook's Compensation & Governance Committee until May 2018.

23 30. Defendant **Peter Thiel** ("Thiel") is a Facebook director and has been since April
24 2005. Thiel is also a member of Facebook's Compensation & Governance Committee.

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

27 32. Defendant **Erskine B. Bowles** ("Bowles") is a Facebook director and has been
28 since September 2011. Bowles is also the Chair of Facebook's Audit Committee.

1 33. Defendant **Dr. Susan D. Desmond-Hellmann** (“Desmond-Hellmann”) is a
2 Facebook director and has been since March 2013 and is the Lead Independent Director of
3 Facebook’s Board. Desmond-Hellmann is also a member of Facebook’s Compensation &
4 Governance Committee, and was a member of Facebook’s Audit Committee until May 2018.

5 34. Defendant **Jan Koum** (“Koum”) was a Facebook director from October 2014
6 until April 2018. Koum is a co-founder and was CEO of WhatsApp until April 2018, when he
7 resigned from Facebook’s Board and from his role at WhatsApp, a Facebook subsidiary since
8 its acquisition in 2014. According to Facebook’s website, defendant Koum was “responsible
9 for the design and interface of WhatsApp’s service and the development of its core technology
10 and infrastructure.”

11 35. The individuals identified above are referenced collectively in this Complaint as
12 the “Defendants.”

13 **BACKGROUND FACTS**

14 **I. DEFENDANTS WERE OBLIGATED TO SAFEGUARD THE COMPANY’S**
15 **INTERESTS AND COMPLY WITH APPLICABLE LAWS**

16 36. By reason of their positions as officers or directors of Facebook, and because of
17 their ability to control the business, corporate, and financial affairs of the Company,
18 Defendants owed Facebook and its shareholders the duty to exercise due care and diligence in
19 the management and administration of the affairs of the Company, including ensuring that
20 Facebook operated in compliance with all applicable federal and state laws, rules and
21 regulations. Defendants were and are required to act in furtherance of the best interests of
22 Facebook and its shareholders so as to benefit all shareholders equally and not in furtherance of
23 the Defendants’ personal interest or benefit. Each director and officer owes to Facebook and
24 its shareholders the fiduciary duty to exercise good faith and diligence in the administration of
25 the affairs of the Company and in the use and preservation of its property and assets, and the
26 highest obligations of fair dealing.

27 37. Because of their positions of control and authority as directors and officers of
28 Facebook, the Defendants were able to and did, directly or indirectly, exercise control over the

1 wrongful acts detailed in this Complaint. Due to their positions with Facebook, the Defendants
2 had knowledge of material non-public information regarding the Company.

3 38. To discharge their duties, the Defendants were required to exercise reasonable
4 and prudent supervision over the management, policies, practices, controls, and financial and
5 corporate affairs of the Company. By virtue of such duties, the officers and directors of
6 Facebook were required to, among other things:

- 7 a. Manage, conduct, supervise, and direct the employees, businesses, and
8 affairs of Facebook in accordance with laws, rules, and regulations, as well as the
9 charter and by-laws of Facebook;
- 10 b. Ensure that Facebook did not engage in imprudent or unlawful practices
11 and that the Company complied with all applicable laws and regulations;
- 12 c. Remain informed as to how Facebook was, in fact, operating, and, upon
13 receiving notice or information of imprudent or unsound practices, to take
14 reasonable corrective and preventative actions, including maintaining and
15 implementing adequate financial and operational controls;
- 16 d. Supervise the preparation, filing, or dissemination of any SEC filings,
17 press releases, audits, reports, or other information disseminated by Facebook,
18 and to examine and evaluate any reports of examinations or investigations
19 concerning the practices, products, or conduct of officers of the Company;
- 20 e. Preserve and enhance Facebook's reputation as befits a public
21 corporation;
- 22 f. Exercise good faith to ensure that the affairs of the Company were
23 conducted in an efficient, business-like manner so as to make it possible to
24 provide the highest quality performance of its business; and
- 25 g. Refrain from unduly benefiting themselves and other Facebook insiders at
26 the expense of the Company.

27 39. According to Facebook's preliminary proxy statement, filed with the SEC on or
28 about April 14, 2017 (the "2017 Proxy Statement"):

1 h. “The full board of directors has primary responsibility for evaluating
2 strategic and operational risk management, and for CEO succession planning.”

3 i. The audit committee “has the responsibility for overseeing our major
4 financial and accounting risk exposures as well as legal and regulatory risk
5 exposures[,]” “oversees the steps our management has taken to monitor and
6 control these exposures, including policies and procedures for assessing and
7 managing risk and related compliance efforts[,]” and “oversees our internal audit
8 function.”

9 j. The compensation & governance committee “evaluates risks arising from
10 our compensation policies and practices[.]”

11 k. The audit committee and the compensation & governance committee
12 “provide reports to the full board of directors regarding these and other matters.”

13 40. Defendants also have specific obligations under the FTC Consent Decree and are
14 duty-bound to oversee Facebook’s compliance with its terms. Specifically, under the Consent
15 Decree, Facebook is:

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

18 b. required to obtain consumers’ affirmative express consent before enacting
19 changes that override their privacy preferences;

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

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

26 e. required, every two years for the next 20 years after entry of the Consent
27 Decree, to obtain independent, third-party audits certifying that it has a privacy
28 program in place that meets or exceeds the requirements of the FTC order, and to

1 ensure that the privacy of consumers’ information is protected.

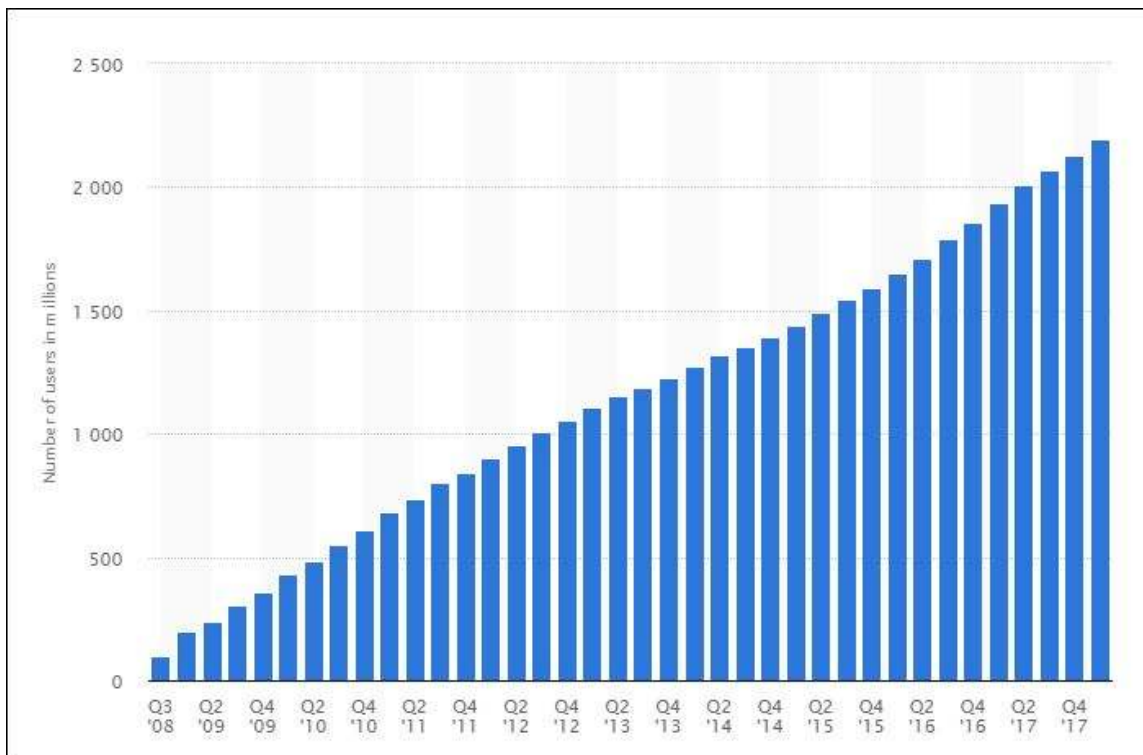
2 41. As FTC Chairman Jon Leibowitz stated in the FTC’s press release announcing
 3 the settlement and terms of the Consent Decree on November 29, 2011, “*Facebook is obligated*
 4 *to keep the promises about privacy that it makes to its hundreds of millions of users...*”
 5 Facebook’s innovation does not have to come at the expense of consumer privacy...”
 6 Defendants failed to do so, and permitted Facebook to violate federal law, the laws of various
 7 U.S. states, and the laws of other countries, as set forth below.

8 **II. BACKGROUND OF THE COMPANY AND ITS BUSINESS**

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

13 43. Monthly active users (“MAUs”) are those which have logged in to Facebook
 14 during the last 30 days. Facebook’s number of MAUs has increased in every quarter since
 15 2008, as shown in the following chart:

16 **Number of monthly active Facebook users worldwide as of 1st quarter 2018 (in millions)**



1
2 44. Facebook users must register before using the social network and are free to
3 create a personal profile in order to interact with other users which they can add as friends.
4 Furthermore, Facebook users may join user groups and can categorize their Facebook contacts
5 into lists. Users can post status updates or other content and message each other. Facebook
6 users can also interact with a wide selection of applications including social games or other
7 services like the photo-sharing app Instagram.

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

10 **A. THE FACEBOOK PLATFORM ALLOWS APPS, WEBSITES, AND DEVICES TO**
11 **ACCESS AND USE THE PERSONAL INFORMATION OF BILLIONS OF USERS**

12 46. The Facebook Platform has grown over time to allow ever greater access to the
13 personal information of Facebook users. The Facebook Platform was launched in 2007. The
14 platform originally supported only applications created by Facebook for use on Facebook, but
15 soon expanded to allow third party developers to develop their apps using the Facebook
16 Platform. Defendant Zuckerberg announced the expansion of the platform to third party
17 developers in 2008, stating: "With this evolution of Facebook Platform, we've made it so that
18 any developer can build the same applications that we can. And by that, we mean that they can
19 integrate their application into Facebook —into the social graph — the same way that our
20 applications like Photos and Notes are integrated."

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

25 48. Through Graph API and later iterations of the "social graph," Facebook obtains
26 and shares information about users through "features" that third parties can implement on their
27 own websites, such as the "Like" button, the "Share" button, and the "Log in with Facebook"
28 option, among other things. These "social plug-ins" enable Facebook and third-party websites

1 to exchange user information. Facebook obtains information about the websites' users and
2 activities, including purchases, and the third-party websites can also receive information from
3 Facebook.

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

9 50. As stated in a letter that Facebook sent to the Law Commission of New Zealand
10 in 2011, "At Facebook's core is the social graph: people and the connections they have to the
11 things they care about. In 2010, we began extending the social graph, via the Open Graph
12 protocol, to include websites and pages that people like throughout the web. This is referred to
13 as 'Facebook Platform.'" The letter further explained: "Facebook Platform enables developers
14 to build social apps, websites and devices that integrate with Facebook and reach millions of
15 people."

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

18 51. Facebook offers advertising services to its customers that include or have
19 included at various points in time, among other things, assisting customers in developing and
20 creating advertisements and advertising strategies, obtaining information about Facebook users
21 from the Company's website and third party sources, compiling user data and maintaining
22 databases of information about Facebook users, developing a marketing and advertising
23 strategy to target and exclude certain groups of Facebook users from receiving advertisements,
24 tracking and evaluating the effectiveness of advertisements and user targeting strategies,
25 implementing advertising campaigns, and delivering advertisements to Facebook users,
26 including via News Feed.

27 52. Facebook's customers (advertisers) can use Facebook's advertising services to
28 target users with specific attributes. Facebook applies its own algorithm to categorize
Facebook users and to determine which users and groups of users will be targeted to receive

1 advertisements via its advertising platform. As stated on Facebook’s website: “With our
2 powerful audience selection tools, you can target people who are right for your business.
3 Using what you know about your customers—like demographics, interests and behaviors—you
4 can connect with people similar to them.”

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

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

15 55. As demonstrated by the following chart, Facebook’s advertising business
16 accounts for substantially all of the Company’s revenues:



1 **III. FACEBOOK’S TRANSFORMATION FROM “SOCIAL NETWORK” TO DATA**
 2 **GATHERING EMPIRE**

3 **A. FACEBOOK WORKED WITH THIRD PARTY COMPANIES, INCLUDING**
 4 **COMPETITORS, TO GAIN ACCESS TO DATA SINCE 2007**

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

10 57. Facebook launched Beacon in 2007, by which information about a Facebook
 11 user’s purchases from third party websites would be provided to Facebook after the transaction
 12 occurred. Facebook then publicized this information to the user’s friends via News Feed,
 13 which would include the user’s name, what they did (bought something), what they bought,
 14 and where they bought it.

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

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

26 60. Defendants pursued their strategy of monetizing Facebook’s platform through
 27 partnerships with third party companies, utilizing third-party developers to obtain as much user
 28 data as possible, and by acquiring competitors.

61. **FriendFeed**: Facebook acquired FriendFeed in 2009 for \$47.5 million.

1 FriendFeed was a social media platform that created a number of features that Facebook
2 subsequently popularized, such as the “Like” button, and News Feed, which was the first time
3 that the website actively updated users with news (about their friends’ activities) in real-time.

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

10 63. **Face.com:** In 2012, Facebook purchased Face.com, which pioneered facial
11 recognition technology on mobile devices, for a reported \$100 million. Facebook uses
12 Face.com’s technology to power its photo-tagging feature, which allows users to receive quick
13 and accurate suggestions on who to tag in their photos.

14 64. **Onavo:** Facebook acquired Onavo in October 2013. Onavo has two parts: a
15 consumer-facing app that helps improve app and data performance on Android and iOS
16 devices, and an analytics business, which giving mobile publishers tools to track how well their
17 apps are performing, compared to the competition.

18 65. **Atlas:** Facebook purchased Atlas from Microsoft in 2013 and relaunched it the
19 following year with a focus on what it calls “people-based marketing” – namely, the ability for
20 advertisers to track users across devices. In short, Atlas tracks the relationship between
21 Facebook’s online advertising and actual offline sales.

22 66. **Oculus:** Facebook acquired Oculus, a virtual reality (“VR”) device maker, in
23 2014 for \$2 billion. According to defendant Zuckerberg, the goal is to first develop immersive
24 VR gaming and then expand to include all sorts of virtual experiences, including social
25 networking. Facebook operates Oculus through Oculus Ireland Limited.

26 67. **WhatsApp:** Facebook brought WhatsApp in 2014 for \$19 billion. Notably,
27 former Facebook director defendant Koum is the co-founder and was CEO of WhatsApp until
28 April 2018. WhatsApp is the preferred instant messaging platform in the developing world.

1 **B. DEFENDANTS EXPAND FACEBOOK’S PLATFORM TO APP DEVELOPERS**

2 68. Defendant Zuckerberg announced the expansion of the platform to third party
3 developers in 2008, stating: “With-this evolution of Facebook Platform, we’ve made it so that
4 any developer can build the same applications that we can. And by that, we mean that they can
5 integrate their application into Facebook —into the social graph — the same way that our
6 applications like Photos and Notes are integrated.”

7 69. In a further expansion of the platform, in 2010, defendant Zuckerberg announced
8 the launch of Graph Application 19 Programming Interface (“Graph API”) at Facebook’s
9 annual developer conference. Graph API allows developers to read and write data from and to
10 Facebook and to obtain, track, and share information.

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

18 71. Facebook has similarly expanded its access to and use of personal information
19 through partnership agreements and referral services with third party companies. For example,
20 Facebook’s agreements with mobile device manufacturers allow Facebook to implement its
21 features directly on mobile devices. This has enabled Facebook to obtain information about
22 mobile device users, including non-Facebook users, and to track users across devices.

23 72. As stated in a letter that Facebook sent to the Law Commission of New Zealand
24 in 2011, “At Facebook’s core is the social graph: people and the connections they have to the
25 things they care about. In 2010, we began extending the social graph, via the Open Graph
26 protocol, to include websites and pages that people like throughout the web. This is referred to
27 as ‘Facebook Platform.’” The letter further explained: “Facebook Platform enables developers
28 to build social apps, websites and devices that integrate with Facebook and reach millions of

1 people.”

2 **C. DEFENDANTS TRANSITIONED FACEBOOK’S ADVERTISING BUSINESS TO**
 3 **MOBILE DEVICES BEGINNING IN 2011 AND THE COMPANY’S REVENUES**
 4 **SKYROCKETED**

5 73. In **2011 and 2012**, to transition Facebook from its collapsing desktop advertising
 6 business to mobile advertising, Zuckerberg and the other Defendants implemented a strategy to
 7 leverage user data through what they called “reciprocity.” It has since been revealed
 8 that “reciprocity” meant that Facebook shared user data with over 50 companies, pursuant to
 9 agreements that for the most part, are still in effect. The plan involved obtaining additional data
 10 about Facebook users and non-users from third parties, including data brokers; and leveraging
 11 data that Facebook obtained through relationships and agreements with other third party
 12 companies.

13 74. In **2012**, most of Facebook’s revenue came from generic banner ads delivered to
 14 users visiting the Company’s website on a desktop computer. By the fourth quarter of 2013,
 15 fifty-three percent of the Company’s advertising revenue came from targeted advertisements
 16 that Facebook delivered to smartphones, tablets, and other mobile devices, with many of those
 17 ads highly targeted by gender, age and other user demographics. “I think it’s inarguable that
 18 Facebook is a mobile-first company,” Facebook’s chief financial officer said in an interview at
 19 the time.

20 75. Facebook had total revenue of \$2.59 billion in the quarter that ended December
 21 31, 2013, up from \$1.59 billion in the same quarter the previous year. Revenue from
 22 advertising was \$2.34 billion, up 76 percent from the previous year. Excluding compensation
 23 costs related to Facebook’s initial public offering (“IPO”) in 2012, the Company’s profits were
 24 up 83 percent. “It’s hard to see any flaws in this quarter,” commented one analyst, Ron Josey
 25 of JMP Securities. “They’re seeing demand for their ad product go through the roof.”

26 **D. FACEBOOK PURCHASED DATA FROM THIRD PARTY DATA BROKERS SINCE AT**
 27 **LEAST 2012**

28 76. Beginning in or around **2012**, Facebook obtained information from data
 collection companies like Datalogix, Acxiom, Epsilon, and BlueKai, which collect information

1 about consumers through store loyalty cards, mailing lists, public records information
2 (including home or car ownership), browser cookies, and other devices. Facebook combined
3 its user information with the information obtained from these companies to generate more
4 information about Facebook users and to enhance its targeted advertising services.

5 77. A ProPublica blog post dated December 27, 2017, titled “Facebook Doesn’t Tell
6 Users Everything It Really Knows about Them” reported that “Facebook has been working
7 with data brokers since 2012 when it signed a deal with Datalogix.” This prompted Jeffrey
8 Chester, executive director of the privacy advocate Center for Digital Democracy, to file a
9 complaint with the FTC alleging that Facebook had violated the Consent Decree with the
10 agency on privacy issues. Facebook was “not being honest,” said Chester. “Facebook is
11 bundling a dozen different data companies to target an individual customer, and an individual
12 should have access to that bundle as well.” The FTC did not publicly responded to that
13 complaint, and Facebook subsequently signed deals with five other data brokers.

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

26 79. However, as ProPublica noted, “[l]imiting commercial data brokers’ distribution
27 of your personal information is no simple matter.” Basically, a Facebook user would need to
28 opt out in at least three different places: with Acxiom, Datalogix, and Epsilon. BlueKai did not

1 offer a direct way to opt out, however, and Acxiom required people to send the last four digits
2 of their social security number to obtain their data. Further, because Facebook changes its
3 providers from time to time, users would have to regularly visit the help center page to protect
4 their privacy. Most shocking, however, is ProPublica’s report that, “[f]or non-Facebook users
5 whose data had been involuntarily collected, individuals are directed to creating a Facebook
6 account, and accessing the account settings in order to view the data collected by the social
7 media platform.”

8 80. ProPublica’s investigation confirmed that limiting commercial data brokers’
9 distribution of your personal information is no simple matter. For instance, opting out of
10 Oracle’s Datalogix, which provides about 350 types of data to Facebook according to our
11 analysis, requires “sending a written request, along with a copy of government-issued
12 identification” in postal mail to Oracle’s chief privacy officer.

13 81. ProPublica’s report also indicated that one reporter (Julia Angwin) had actually
14 tried to do what Facebook suggested, and tried to opt out from as many data brokers as she
15 could, in 2013. Of the 92 brokers she identified that accepted opt-outs, 65 of them required her
16 to submit a form of identification such as a driver’s license. In the end, *she could not remove*
17 *her data from the majority of providers.*

18 82. Facebook entered into a data-matching deal with Datalogix, a U.S.-based data-
19 mining company that collects information about consumer behavior from more than 1,000
20 offline retailers, as part of a larger expansion of advertising based on the personal information
21 of Facebook users. Under the deal terms, Facebook allowed Datalogix to match the personal
22 information of Facebook users with personal information held by Datalogix in order to track
23 Facebook users’ offline commercial activity.

24 83. According to the Electronic Privacy Information Center (“EPIC”), Facebook did
25 not attempt to notify users of its decision to disclose user information to Datalogix, and that
26 neither Facebook’s data use policy nor its statement of rights and responsibilities adequately
27 explains the specific types of information Facebook discloses, the manner in which the
28 disclosure occurs or the identities of the third parties receiving the information.

1 **E. THE BOARD INCREASED FACEBOOK’S LOBBYING EXPENDITURES AND**
2 **EFFORTS TO INFLUENCE LEGISLATORS RATHER THAN ADOPTING**
3 **REASONABLE PRIVACY PRACTICES TO PROTECT USERS AND COMPLY WITH**
4 **EXISTING LAWS**

5 84. Beginning in 2011, Defendants sharply increased Facebook’s lobbying
6 expenditures in an effort to influence key bills and regulations that threatened to prohibit the
7 type of data gathering and information sharing that Defendants’ strategy of targeted advertising
8 services – and its revenues – depended upon. In 2011, Facebook’s efforts centered largely on
9 federal policy involving Internet privacy. Defendants targeted several existing privacy laws
10 slated for updates in 2011, including the Children’s Online Privacy Protection Act, the
11 Electronic Communications Privacy Act, and the Communications Assistance for Law
12 Enforcement Act, lobbied against policies relating to location-based services, including the
13 proposed Location Privacy Protection Act, and lobbied against two other bills, the Do-Not-
14 Track Online Act and the Personal Data Privacy and Security Act, which proposed creating a
15 mechanism for allowing people to easily opt out of behavioral tracking online, and increased
16 penalties for unauthorized access to data containing personal information

17 85. Defendants characterized Facebook’s lobbying efforts and expenditures as a
18 general push to raise awareness about its functions and overall goals, but were purposefully
19 vague about what those goals were, and deliberately failed to disclose that the “service”
20 Defendants sought to protect was Facebook’s advertising service that generated nearly all of its
21 revenue; protecting Facebook’s users was not a priority: “This increase represents a
22 continuation of our efforts to explain how our service works as well as the important actions we
23 take to protect people who use our service and promote the value of innovation to our
24 economy,” said Facebook spokesman Andrew Noyes.

25 86. At the time, John Simpson, director of the nonprofit Consumer Watchdog’s
26 privacy project, called Facebook’s increased spending on lobbying and hiring of Washington
27 heavy-hitters a worrying development. Facebook, he said, was moving farther away from
28 protecting consumers. “When large corporations spend big dollars to get their agenda through,
 it is not at all a positive sign for their customers or consumers,” Simpson said. “The troubling
 thing is that these guys have a record of overstepping and overreaching on privacy issues, and

1 they haven't been at all responsible about protecting users.”

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

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

14 89. Facebook set a new company record for lobbying expenditures again in the first
15 quarter of 2014, as Defendants continued their attempts to influence federal lawmakers on
16 similar cybersecurity issues and issues relating to “government surveillance,” according to
17 Facebook's disclosures.

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

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

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

1 92. Notwithstanding the Board’s heightened duties under the Consent Decree to
2 oversee Facebook’s compliance with pertinent data privacy laws and regulations, however,
3 Defendants failed to ensure that Facebook implemented adequate internal controls and
4 reporting systems that would detect and prevent similar violations of law as gave rise to the
5 FTC Consent Decree.

6 93. Since the Cambridge Analytica scandal, and after this action was filed, it has
7 been reported that Defendants continue to ignore reports of data sharing and exfiltration of
8 Facebook information and user data occurring on a similar scale.

9 94. On **June 29, 2018**, MobileMarketing Magazine reported that a security
10 researcher had discovered a third party app called NameTest had accessed the data of up to
11 **120 million** Facebook users that was left exposed as recently as the previous month.

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

20 96. De Ceukelaire said he installed the NameTest app which, like Kogan’s
21 “thisisyourdigitallife” app, is a personality test. After he tried it, he tracked how his data was
22 being processed and said he discovered that his personal information, along with that of every
23 other person who had taken the quiz, was being held in a JavaScript file that could easily be
24 requested by any website that knew to ask. In addition to enabling any site to request data
25 points, NameTest provided those who requested information with an access token that would
26 allow continued access to a user's posts, photos and friends data for up to two months.

27 97. “Depending on what quizzes you took, the javascript could leak your Facebook
28 ID, first name, last name, language, gender, date of birth, profile picture, cover photo, currency,

1 devices you use, when your information was last updated, your posts and statuses, your photos
2 and your friends," said De Ceukelaire. "If you ever took a quiz and removed the app
3 afterwards, external websites would still be able to read your Facebook ID, first name, last
4 name, language, gender, date of birth. You would have only prevented this from happening if
5 you manually deleted your cookies, as the website does not offer a logout functionality."

6 98. On **June 27, 2018**, De Ceukelaire posted the following "Timeline of Events,"
7 along with Facebook's response, on his blog:

- 8 • **On April, 22nd**, I reported this to Facebook's Data Abuse program.
- 9 • **On April 30th**, I received an initial response from Facebook, stating that they're looking
10 still looking into it.
- 11 • **On May 14th**, I sent a follow-up mail, asking whether they already reached out to the app
12 developers.
- 13 • **On May 22th**, Facebook said that it could take three to six months to investigate the issue
14 (as mentioned in their initial automated reply) and that they would keep me in the loop.
At this time, the NameTests quizzes were still up and running.
- 15 • **On June, 25th** I noticed NameTests had changed the way they process data. Third-parties
16 could no longer access its users personal information. I contacted them about the fix, told
17 them about this blogpost and asked them to donate the bounty to Freedom of the Press
Foundation.
- 18 • **On June, 26th**, I reached out to NameTest's Digital Protection Officer to answer some
19 questions regarding the vulnerability and the disclosure process by Facebook.
- 20 • **On June, 27th**, Facebook informed me they donated \$8,000 (\$4,000 bounty, doubled
21 because I chose to donate it to charity) to the Freedom of the Press foundation as part of
22 their data abuse bounty program:

23 ///

24 ///

26 ///

28

**Our reply**

Yesterday

Hi Inti,

Thank you for confirming the fix.

After reviewing this issue, we have decided to award you a bounty of \$4,000. Below is an explanation of the bounty amount.

The app had an endpoint (https://en.nametests.com/appconfig_user/) that can be included by referencing it as an external JS file. This could have allowed an attacker to determine the details of a logged-in user to Facebook's platform (while requiring the logged-in user to actively reference that endpoint - for example by surfing to a malicious website) . Following your submission, we've approached nametests, and as a result the issue is now fixed (as confirmed by nametests, Facebook, and you).

As you mentioned you would like us to donate the bounty to a recognized charitable organization, we've matched the bounty amount, and have donated \$8,000 to the Freedom of the Press Foundation (transaction ID - ch_D7npKyaW5HvLZf).

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

A. DEFENDANTS MAINTAINED POLICIES THAT PERMITTED DEVELOPERS TO OBTAIN FACEBOOK USERS' PERSONAL INFORMATION

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

Granting us permission to use your information not only allows us to provide Facebook as it exists today, but it also allows us to provide you with innovative features and services we develop in the future that use the information we receive about you in new ways. While you are allowing us to use the information we receive about you, you always own all of your information. Your trust is important to us, which is why we don't share information we receive about you with others unless we have:

- received your permission
- given you notice, such as by telling you about it in this policy; or
- removed your name and any other personally identifying information from it.

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

1 101. Despite this policy, until **2014**, developers could generally launch apps on the
 2 Facebook Platform without affirmative approval or review by Facebook. Facebook allowed
 3 third-party app developers to use the Facebook API to download a user’s friends and
 4 friendships.

5 102. A Facebook developer page from 2013 shows that Facebook’s API allowed
 6 developers to access user and a user’s friends account information.

| User permission | Friends permission | Description |
|------------------------|---------------------------|--|
| user_age | friends_age | Provides access to the "About Me" section of the profile in the <code>about</code> property. |
| user_activities | friends_activities | Provides access to the user's list of activities as the <code>activities</code> connection. |
| user_birthday | friends_birthday | Provides access to the birthday with year as the <code>birthday</code> property. Note that your app may determine if a user is "old enough" to use an app by obtaining the <code>age_range</code> public profile property. |
| user_checkins | friends_checkins | Provides read access to the authored user's check-ins or a friend's check-ins that the user can see. This permission is superseded by <code>user_status</code> for new applications as of March, 2013. |
| user_education_history | friends_education_history | Provides access to education history as the <code>education</code> property. |
| user_events | friends_events | Provides access to the list of events the user is attending as the <code>events</code> connection. |
| user_groups | friends_groups | Provides access to the list of groups the user is a member of as the <code>groups</code> connection. |
| user_hometown | friends_hometown | Provides access to the user's hometown in the <code>hometown</code> property. |
| user_interests | friends_interests | Provides access to the user's list of interests as the <code>interests</code> connection. |
| user_likes | friends_likes | Provides access to the list of all of the pages the user has liked as the <code>likes</code> connection. |

| | | |
|---------------------------|------------------------------|---|
| user_location | friends_location | Provides access to the user's current city as the location property. |
| user_notes | friends_notes | Provides access to the user's notes on the user's timeline. |
| user_photos | friends_photos | Provides access to the photos the user has uploaded, and photos the user has been tagged in. |
| user_questions | friends_questions | Provides access to the questions the user or friend has asked. |
| user_relationships | friends_relationships | Provides access to the user's family and personal relationships and relationship status. |
| user_relationship_details | friends_relationship_details | Provides access to the user's relationship preferences. |
| user_religion_politics | friends_religion_politics | Provides access to the user's religious and political affiliations. |
| user_status | friends_status | Provides access to the user's status messages and checks. These are the documentation for the location_post table for information on how the permission may affect content of information about the location associated with posts. |
| user_subscriptions | friends_subscriptions | Provides access to the user's subscribers and subscribers. |
| user_videos | friends_videos | Provides access to the videos the user has uploaded, and videos the user has been tagged in. |
| user_website | friends_website | Provides access to the user's web-site URL. |
| user_work_history | friends_work_history | Provides access to work history on the user's profile. |

Updated: Nov 28, 2014 (UTC)

Facebook © 2014 - English (US) [Help](#) [Advertising](#) [Careers](#) [Privacy Policy](#) [Terms of Service](#)

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

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

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

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

1 when Facebook messages were more of an inbox and less of a real-time messaging service –
2 this enabled things like desktop apps that combined Facebook messages with messages from
3 other services like SMS so that a person could access their messages all in one place,” the
4 spokesperson said.

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

13 107. A Law360 article noted that Facebook’s changes to the privacy practices were
14 prompted by the approval of a contested \$20 million privacy settlement that required the
15 Company to make changes to its policies in order to give minor and adult users more
16 information about how their names and likenesses are employed in connection with ads
17 displayed through the site’s Sponsored Stories program and that, contrary to Facebook’s
18 statement on its website, they were not changes Facebook had “elected” to make on its own.

19 108. On **November 13, 2014**, Facebook announced it would give users more
20 information about how their data is being collected and used, rolling out privacy policy
21 changes that allow the site to do more with location and transactional data and implementing
22 new controls that enable users to limit the ads they see.

23 109. The updates included explaining that Facebook will soon begin showing users
24 that share location information menus from restaurants nearby or friends in the area, and
25 clarifying that it will ask for permission to use a phone’s location to offer optional features like
26 check-ins or adding locations to posts. The policy changes also revealed that Facebook was
27 testing a “buy” button to help people discover and purchase products without leaving the site,
28 as part of its foray into mobile payments, and provide more information about how the

1 company's growing family of companies and apps — which now included services such as
2 Instagram and WhatsApp — work together.

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

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

13 **C. DEFENDANTS FALSELY ASSURED FACEBOOK'S USERS THAT THEY COULD**
14 **TRUST FACEBOOK TO PROTECT THEIR PERSONAL INFORMATION**

15 112. Defendants recognized the importance of maintaining user trust and repeatedly
16 emphasized in public statements that privacy and data security are critically important to
17 Facebook's brand.

18 113. Throughout the relevant period, Defendants emphasized the importance of user
19 privacy to Facebook's revenues and business, while concealing the fact that the Company's
20 policies allowed third party developers to obtain massive amounts of Facebook users' personal
21 information without verification as to the nature of its use. Defendants claimed to protect this
22 information by reasonable efforts to maintain its secret nature.

23 114. Facebook's Data Policy states, “We will never sell your information to anyone.
24 We have a responsibility to keep people's information safe and secure, and we impose strict
25 restrictions on how our partners can use and disclose data. We explain all of the circumstances
26 where we share information and make our commitments to people more clear.”

27 115. Maintaining user privacy and data security has long been considered central to
28 Facebook's business and growth prospects. Defendants have assured users and investors for

1 years that the Company monitors user accounts for precisely the type of leaks that allowed
 2 Cambridge Analytica to obtain millions of users' personal information without their
 3 knowledge, and to retain such information for years after Facebook claimed to have confirmed
 4 that neither Cambridge Analytica nor any unauthorized person or entity associated with it was
 5 in the possession of any misappropriated user data.

6 116. For instance, a **June 21, 2013** blog post entitled "Important Message from
 7 Facebook's White Hat Program" states: "At Facebook, we take people's privacy seriously, and
 8 we strive to protect people's information to the very best of our ability. We implement many
 9 safeguards, hire the brightest engineers and train them to ensure we have only high-quality
 10 code behind the scenes of your Facebook experiences. We even have teams that focus
 11 exclusively on preventing and fixing privacy related technical issues before they affect you....
 12 *Your trust is the most important asset we have, and we are committed to improving our safety*
 13 *procedures and keeping your information safe and secure.*"

14 117. Defendants repeatedly emphasized the importance of data security and privacy to
 15 the Company in Facebook's public statements, and acknowledged their specific responsibility
 16 for overseeing the substantial risks that a breach, like the Cambridge Analytica incident, posed
 17 to the Company. According to Facebook's preliminary proxy statement, filed with the SEC on
 18 or about **April 14, 2017** (the "2017 Proxy Statement"):

19 Our board of directors as a whole has responsibility for overseeing our risk
 20 management. The board of directors exercises this oversight responsibility
 21 directly and through its committees. *The oversight responsibility of the board*
 22 *of directors and its committees is informed by reports from our management*
 23 *team and from our internal audit department that are designed to provide*
 24 *visibility to the board of directors about the identification and assessment of*
 25 *key risks and our risk mitigation strategies.*

26 **D. DEFENDANTS WERE WARNED ABOUT DATA SECURITY ISSUES IN 2012 BY**
 27 **WHISTLEBLOWER SANDY PARAKILAS BUT DID NOTHING**

28 118. In testimony to the British Parliament's Digital, Culture, Media and Sport
 committee, Sandy Parakilas, a former Facebook platforms operations manager for policing data
 breaches by third-party software developers between **2011 and 2012**, stated that hundreds of
 millions of Facebook users are likely to have had their private information harvested by

1 companies that exploited the same terms as the firm that collected data and passed it on to
 2 Cambridge Analytica. Parakilas stated that in **2012** he warned senior executives at the
 3 company that its lax approach to data protection risked a major breach: “My concerns were that
 4 all of the data that left Facebook servers to developers could not be monitored by Facebook, so
 5 [Facebook] had no idea what developers were doing with the data,” Parakilas said. When
 6 asked what kind of control Facebook had over the data accessed by outside developers,
 7 Parakilas replied: “**Zero. Absolutely none. Once the data left Facebook servers there was**
 8 **not any control, and there was no insight into what was going on.**” According to Parakalis,
 9 the Company did not use enforcement mechanisms, including audits of external developers, to
 10 ensure data was not being misused. Parakilas confirmed that Facebook’s “trust model” was
 11 rife with security vulnerabilities and a near total abnegation of its responsibility to audit its own
 12 rules limiting use of Facebook data by third parties. Or, in Parakilas’ own words, “[Facebook]
 13 felt that it was better not to know.”

14 119. Parakilas testified that he had created a PowerPoint presentation warning about
 15 the areas where the Company was exposed and user data was at risk, and that he had shared the
 16 presentation with Facebook’s senior executives, but they ignored his concerns. According to
 17 Parakilas, “it was known and understood ... that there was risk with respect to the way that
 18 Facebook Platform was handling data” but “*it was a risk that they were willing to take.*”

19 120. Parakilas also related how he discovered a social games developer using
 20 Facebook data to automatically generate profiles of children without their consent, and another
 21 developer asking permission to gain access to a user’s Facebook messages and posted photos.
 22 In an Op-Ed in the *New York Times*, Parakilas stated that when he reported these incidents to
 23 his superiors, they didn’t care at all:

24 At a company that was deeply concerned about protecting its users, this
 25 situation would have been met with a robust effort to cut off developers who
 26 were making questionable use of data. But when I was at Facebook, the
 27 typical reaction I recall looked like this: *try to put any negative press*
 28 *coverage to bed as quickly as possible, with no sincere efforts to put*
safeguards in place or to identify and stop abusive developers. When I
 proposed a deeper audit of developers’ use of Facebook’s data, one
 executive asked me, “Do you really want to see what you’ll find?”

1 The message was clear: The company just wanted negative stories to stop.
2 It didn't really care how the data was used.

3 **E. DEFENDANTS KNEW ABOUT THE CAMBRIDGE ANALYTICA "BREACH" IN 2015**
4 **BUT CONCEALED THE FACT AND FAILED TO ACT**

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

7 Ms. Eshoo: ...When did Facebook learn that? And when you learned it, did you
8 contact their CEO immediately, and if not, why not?

9 Mr. Zuckerberg. Congresswoman, yes. When we learned in 2015
10 that a Cambridge University researcher associated with the academic
11 institution that built an app that people chose to share their data
12 with –

13 Ms. Eshoo. We know what happened with them, but I am asking you.

14 Mr. Zuckerberg. Yes, I am answering your question.

15 Ms. Eshoo. Right.

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

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

18 Mr. Zuckerberg. ***Yes.***

19 122. But Zuckerberg took no action at the time, nor did anyone else at Facebook, until
20 more than two years *after* he learned of the incident.

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

1 124. Defendants also publicly affirmed the Company’s commitment to continually
2 monitor and improve its data security systems. “[M]isleading people or misusing their
3 information is a direct violation of our policies and we will take swift action against companies
4 that do, including banning those companies from Facebook and requiring them to destroy all
5 improperly collected data,” a Facebook spokesman said in a statement to the *Guardian* in 2015.

6 125. When the truth came out in 2018, Facebook representatives insisted that Kogan
7 had violated Facebook policies. In a statement posted to Facebook’s Newsroom on March 16,
8 2018, a Facebook attorney said that Kogan had “gained access to this information in a
9 legitimate way and through the proper channels,” but “violated Facebook’s platform policy” by
10 “passing information on” to third parties, including Cambridge Analytica. As a result, Kogan’s
11 app was removed from Facebook and “all parties” who received the data from Kogan were
12 required to certify that it had been destroyed in 2016.

13 126. According to Facebook, “Facebook obtained written certifications from Dr.
14 Kogan, GSR, and other third parties declaring that all such data they had obtained was
15 accounted for and destroyed. In March 2018, after Mr. Milner’s testimony, Facebook received
16 information from the media suggesting that the certifications we [Facebook] received may not
17 have been accurate... As part of our investigation, we have hired a forensic auditor to
18 understand what information Cambridge Analytica had and whether it has been destroyed.”
19 Although three years was more than enough time for Facebook to confirm the authenticity and
20 accuracy of the certifications, it did not. Further, the letter agreement that Facebook sent to
21 Kogan and GSR regarding the destruction of the data and their “certifications” does not appear
22 to have been signed by anyone at Facebook, suggesting that no one followed up until the truth
23 came out in 2018, and that the agreement to destroy the data could potentially be invalid.

24 127. It was not until the *Observer* asked Facebook to comment just a few days prior to
25 breaking the news of the Cambridge Analytica leak, that Facebook announced that it was
26 (finally) suspending Cambridge Analytica and Kogan from the platform pending further
27 information over misuse of data. Facebook also said it was suspending Wylie from accessing
28 the platform while it carried out its internal investigation, despite his role as a whistleblower.

1 128. Just one month earlier, in February 2018, both Facebook and the CEO of
2 Cambridge Analytica, Alexander Nix (“Nix”), had told a U.K. parliamentary inquiry on fake
3 news that the company did not have or use private Facebook data. Nix told officials: “We do
4 not work with Facebook data and we do not have Facebook data.” Simon Milner, Facebook’s
5 U.K. policy director, when asked if Cambridge Analytica had Facebook user data, told U.K.
6 officials: “They may have lots of data but it will not be Facebook user data. It may be data
7 about people who are on Facebook that they have gathered themselves, but it is not data that we
8 have provided.”

9 129. Notwithstanding their significant obligations as members of the Board or
10 corporate officers, and (for some of the Defendants) as members of committees charged with
11 overseeing Facebook’s risk exposure, corporate governance, and other critical aspects of the
12 Company’s business and operations, the Defendants maintained policies that allowed Kogan
13 and other third party app developers to obtain mass amounts of Facebook user information
14 without verification as to the nature of its use, and upon learning that 50 million users’ personal
15 information had been misappropriated and used by Cambridge Analytica, failed to notify users
16 or disclose anything about the incident, or its significant impact on the Company, publicly and
17 to investors. Worse, Defendants affirmatively misrepresented and concealed these facts from
18 the Company’s regulators and in public statements and filings with the SEC.

19 130. Defendants’ failure to detect and prevent the Cambridge Analytica leak, or to
20 adequately respond with proper notification and disclosures in accordance with best practices
21 and applicable laws, belies any claim that Facebook’s actual “monitoring” practices and
22 internal controls were sufficient. In fact, Facebook’s statements throughout the relevant period
23 indicate that Defendants sought to conceal the deficiencies in Facebook’s user privacy data
24 security practices through materially false and misleading statements denying that any such
25 leak had ever occurred and falsely assured that the Company maintained effective internal
26 controls.

1 131. For example, an October 16, 2015 post by Stamos, Facebook’s Chief Information
2 Security Officer, stated:

3 ***The security of people’s accounts is paramount at Facebook, which is why we***
4 ***constantly monitor*** for potentially malicious activity and offer many options to
5 proactively secure your account. Starting today, we will notify you if we believe
6 your account has been targeted or compromised by an attacker suspected of
7 working on behalf of a nation-state.

8 * * *

9 While we have always taken steps to secure accounts that we believe to have been
10 compromised, we decided to show this additional warning if we have a strong
11 suspicion that an attack could be government-sponsored. We do this because these
12 types of attacks tend to be more advanced and dangerous than others, and we
13 strongly encourage affected people to take the actions necessary to secure all of
14 their online accounts.

15 It’s important to understand that ***this warning is not related to any compromise of***
16 ***Facebook’s platform or systems***, and that having an account compromised in this
17 manner may indicate that your computer or mobile device has been infected with
18 malware. Ideally, people who see this message should take care to rebuild or replace
19 these systems if possible.

20 To protect the integrity of our methods and processes, we often won’t be able to
21 explain how we attribute certain attacks to suspected attackers. That said, we plan
22 to use this warning only in situations where the evidence strongly supports our
23 conclusion. We hope that these warnings will assist those people in need of
24 protection, and we will continue to improve our ability to prevent and detect attacks
25 of all kinds against people on Facebook.

26 132. In a post to the Company’s website on March 18, 2018, Facebook VP Adam
27 Bosworth also noted that maintaining user privacy is in the Company’s best interests, and noted
28 the purportedly indirect effects on Facebook’s revenues. “Yes developers can receive data that
helps them provide better experiences to people, but we don’t make money from that directly
and have set this up in a way so that no one’s personal information is sold to businesses,”
Bosworth wrote. “If people aren’t having a positive experience connecting with businesses and
apps then it all breaks down. This is specifically what I mean when we say our interests are
aligned with users when it comes to protecting data.”

133. On March 22, 2018, *The Guardian* reported, “Facebook provided the dataset of
‘every friendship formed in 2011 in every country in the world at the national aggregate level’

1 to Kogan” for a study on international friendships that was co-authored by two Facebook
2 employees in 2015. Further, a University of Cambridge press release concerning the study’s
3 publication noted that the paper was “the first output of *ongoing research collaborations*
4 *between [Kogan’s] lab in Cambridge and Facebook.*”

5 134. Wylie, a Canadian data analytics expert who worked with Cambridge Analytica
6 and Kogan to create the app, also provided evidence about the data misuse to *The Observer*, the
7 U.K.’s National Crime Agency’s cybercrime unit, and the Information Commissioner’s Office,
8 including emails, invoices, contracts and bank transfers that reveal more than 50 million
9 profiles – mostly belonging to registered U.S. voters – were obtained from Facebook, and
10 Wylie said the Company was aware of the volume of data being pulled by Kogan’s app. “Their
11 security protocols were triggered because Kogan’s apps were pulling this enormous amount of
12 data, but apparently Kogan told them it was for academic uses,” Wylie said. “So they were
13 like: ‘Fine.’”

14 135. The evidence Wylie supplied to U.K. and U.S. authorities includes a letter from
15 Facebook lawyers sent to him in August 2016, asking him to destroy any data he held that had
16 been collected by GSR, the company set up by Kogan to “harvest” the profiles. “Because this
17 data was obtained and used without permission, and because GSR was not authorized to share
18 or sell it to you, it cannot be used legitimately in the future and must be deleted immediately,”
19 the letter said. According to Wylie, Facebook did not pursue a response when the letter
20 initially went unanswered for weeks because Wylie was travelling, nor did it follow up with
21 forensic checks on his computers or storage. “That to me was the most astonishing thing. They
22 waited two years and did absolutely nothing to check that the data was deleted. All they asked
23 me to do was tick a box on a form and post it back.”

24 136. On March 27, 2018, Wylie testified before a U.K. Parliamentary Committee that
25 is investigating “Fake News.” According to Wylie, the personal information that Kogan’s app
26 was able to obtain via Facebook formed the “foundational dataset” underpinning Cambridge
27 Analytica and its targeting models. “This is what built the company,” he claimed. “This was the
28 foundational dataset that then was modeled to create the algorithms.”

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

5 For example, if you are able to create profiling algorithms that can predict
6 certain traits — so let’s say a high degree of openness and a high degree of
7 neuroticism — and when you look at that profiles that’s the profile of a
8 person who’s more prone towards conspiratorial thinking, for example,
9 they’re open enough to kind of connect to things that may not really seem
10 reasonable to your average person. And they’re anxious enough and
11 impulse enough to start clicking and reading and looking at things — and
12 so if you can create a psychological profile of a type of person who is
13 more prone to adopting certain forms of ideas, conspiracies for example,
14 you can identify what that person looks like in data terms.

15 You can then go out and predict how likely somebody is going to be to
16 adopt more conspiratorial messaging. And then advertise or target them
17 with blogs or websites or various — what everyone now calls fake news
18 — so that they start seeing all of these ideas, or all of these stories around
19 them in their digital environment. They don’t see it when they watch
20 CNN or NBC or BBC. And they start to go well why is that everyone’s
21 talking about this online? Why is it that I’m seeing everything here but
22 the mainstream media isn’t talking about [it]...

23 Not everyone’s going to adopt that — so that advantage of using profiling
24 is you can find the specific group of people who are more prone to
25 adopting that idea as your early adopters... So if you can find those people
26 in your datasets because you know what they look like in terms of data
27 you can catalyze a trend over time. But you first need to find what those
28 people look like.

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

1 139. Wylie also suggested Facebook found out about the GSL data harvesting project
2 as early as July 2014 —around the time Kogan had told him that he had spoken to Facebook
3 engineers after his app’s data collection rate had been throttled by the platform. “He told me
4 that he had a conversation with some engineers at Facebook,” said Wylie. “So Facebook would
5 have known from that moment about the project because he had a conversation with
6 Facebook’s engineers — or at least that’s what he told me... Facebook’s account of it is that
7 they had no idea until the *Guardian* first reported it at the end of 2015 — and then they decided
8 to send out letters. They sent letters to me in August 2016 asking do you know where this data
9 might be, or was it deleted?” Wylie noted, “[i]t’s interesting that... the date of the letter is the
10 same month that Cambridge Analytica officially joined the Trump campaign. So I’m not sure
11 if Facebook was genuinely concerned about the data or just the optics of y’know now this firm
12 is not just some random firm in Britain, it’s now working for a presidential campaign.”

13 140. When asked whether Facebook made any efforts to retrieve or delete data, Wylie
14 responded, “No they didn’t.” It was not until Facebook’s image was threatened in 2018, “after
15 I went public and then they made me suspect number one” that Wylie said he had heard
16 anything from the Company. Wylie said that he suspected that when Facebook looked at what
17 happened in 2016, “they went if we make a big deal of this this might be optically not the best
18 thing to make a big fuss about.... So I don’t think they pushed it in part because if you want to
19 really investigate a large data breach that’s going to get out and that might cause problems. So
20 my impression was they wanted to push it under the rug.” He added, “[a]ll kinds of people
21 [had] access to the data. *It was everywhere.*”

22 141. In his testimony to the committee, Wylie discussed a connection between
23 Cambridge Analytica and Palantir, a company that was co-founded in 2003 by defendant Thiel.
24 Palantir is known for providing government agencies and organizations with analytics, security
25 and other data management solutions. According to Wylie, Palantir staff helped Cambridge
26 Analytica build models based on the Facebook data. “That was not an official contract
27 between Palantir and Cambridge Analytica but there were Palantir staff who would come into
28 the office and work on the data,” Wylie stated. “And we would go and meet with Palantir staff

1 at Palantir. So, just to clarify, Palantir didn't officially contract with Cambridge Analytica. But
2 there were Palantir staff who helped build the models that we were working on."

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

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

13 144. Silvester is a co-founder of AIQ, which was founded to "to provide IT and web
14 services to help [political] campaigns use technology to better organize operations." Until
15 2015, SCL was AIQ's largest client.

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

20 Facebook provides a platform that allows an advertiser to show ads to its users
21 based on criteria such as demographic information And interests that people
22 may have identified on Facebook. All of this allows a campaign to run a very
23 complex and comprehensive advertising campaign without the need for any
24 external information."

25 With that info "We would place this information ont tej Facebook platform along
26 with the ads that we create at the direction of the client. Each ad consists of a
27 picture, often with a few words on it, along with some descriptive text and a link to
28 the webpage should someone click on the ad. We also sometimes assist in creating
that web or "landing" page. We then work with the client to decide how many
times people should see these ads and over what time period.

The Facebook platform takes care of the rest, showing these ads to its users and
providing reports on how any times the ads have been shown and how many times
the ads have been clicked...

1 Facebook also gives advertisers the ability to count the number of people who might land on a
2 certain webpage on the client site using a piece of code called a pixel. We often help our
3 clients place this pixel code on their site so that the client can measure if a particular ad is
4 reaching its goal to show people a video, versus signing up to be on a mailing list for example.

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

16 147. Facebook still has not because it cannot confirm that its users’ data is secure.

17 148. Mike Schroepfer, Facebook’s Chief Technology Officer admitted recently that he
18 cannot determine what data has been transferred and shared across Facebook’s platform. In an
19 interview on **May 30, 2018**, Schroepfer stated, “The problem is we can’t observe the actual
20 data transfer that happens there. I don’t actually even know physically how the data went from
21 one to the other. There isn’t a channel that we have some sort of control over.”

22 149. Worse, notwithstanding Defendants’ repeated promises about the importance of
23 privacy and maintaining trust, Schroepfer made clear that Facebook executives continue to
24 blame *users* for trusting the Company. Schroepfer stated, “Well, as a consumer you’re
25 ultimately trusting a third party with your data. Whatever data you brought from Facebook,
26 whatever data, you’re taking these personality quizzes and you’re inputting new data in there.
27 That’s a relationship with that developer that you have to trust that they’ll be responsible with
28 the data they’re using. Whether it’s on Facebook or some map you downloaded from an app

1 store, so we didn't observe that until we heard about it through third-party reports."

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

6 151. On April 11, 2018, defendant Zuckerberg testified before Congress that "[t]he
7 consent decree is extremely important to how we operate the company. . ." However, he and
8 the rest of Facebook's Board of Directors failed to ensure that Facebook complied with the
9 terms of the FTC Consent Decree.

10 152. In an interview with the *Washington Post*, David Vladeck, former director of the
11 FTC's Bureau of Consumer Protection, said the Cambridge Analytica incident may have
12 violated Facebook's 2011 consent decree. "I will not be surprised if at some point the FTC
13 looks at this. I would expect them to," he said. Jessica Rich, who also served as director of the
14 Bureau, said, "Depending on how all the facts shake out, Facebook's actions could violate any
15 or all of these provision, to the tune of many millions of dollars in penalties. They could also
16 constitute violations of both U.S. and EU laws," adding, "*Facebook can look forward to*
17 *multiple investigations and potentially a whole lot of liability here.*"

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

21
22 **F. U.S. AND FOREIGN GOVERNMENT OFFICIALS COMMENCED INVESTIGATIONS**
23 **OF FACEBOOK IN RESPONSE TO THE SCANDAL**

24 154. In the days after the scandal was publicly revealed, the Attorney General of
25 Massachusetts announced an investigation into Facebook and Cambridge Analytica. Senator
26 Ron Wyden followed up with a detailed series of questions for Facebook to answer, and
27 Senators Amy Klobuchar and John Kennedy asked the chairman of the Judiciary Committee,
28 Charles E. Grassley, Republican of Iowa, to hold a hearing. Republican leaders of the Senate

1 Commerce Committee, organized by Senator John Thune (“Thune”), also wrote a letter to
2 defendant Zuckerberg demanding answers to questions about how the data had been collected
3 and if users were able to control the misuse of data by third parties. “It’s time for Mr.
4 Zuckerberg and the other CEOs to testify before Congress,” Senator Mark Warner said. “The
5 American people deserve answers about social media manipulation in the 2016 election.”
6 Zuckerberg eventually testified before Congress on April 10 and 11, 2018.

7 155. On March 20, 2018, a committee in the British Parliament sent a letter to
8 defendant Zuckerberg and asked him to appear before the panel to answer questions on the
9 Company’s connection to Cambridge Analytica. The president of the European Parliament also
10 requested an appearance by defendant Zuckerberg. “The committee has repeatedly asked
11 Facebook about how companies acquire and hold on to user data from their site, and in
12 particular about whether data had been taken without their consent,” wrote Damian Collins,
13 chairman of the British committee. “*Your officials’ answers have consistently understated this*
14 *risk, and have been misleading to the committee.*”

15 156. On **March 21, 2018**, former Facebook employee Sandy Parakilas, who was a
16 platform operations manager from 2011 to 2012, appeared before the Digital, Culture, Media
17 and Sport Committee of the House of Commons, which is investigating the impact of social
18 media on recent elections, and testified about a PowerPoint presentation he had created and
19 shared “with a number of people in the company” outlining his concerns about Facebook’s
20 platform. “I made a map of the various data vulnerabilities of the Facebook platform,”
21 Parakilas told the committee. “I included lists of bad actors and potential bad actors,” he said,
22 “and said here’s some of the things these people could be doing and here’s what’s at risk.”
23 Parakilas said that he “shared that around with a number of people in the company at the
24 time[,]” including “senior executives in charge of Facebook Platform and people in charge of
25 privacy.” When asked by the Chair of the Digital, Culture, Media and Sport Committee if any
26 of those executives were still at the Company, and Parakilas said they were, but declined to
27 name them in public.

28 157. Parakilas also told the *Guardian*, on **March 20, 2018**, that he had warned senior

1 executives at Facebook of the risk that its data protection policies could be breached given the
 2 Company’s minimal or nonexistent procedures for auditing and enforcing those policies.
 3 Parakilas explained, “My concerns were that all of the data that left Facebook servers to
 4 developers could not be monitored by Facebook.” According to Parakilas, Facebook did not
 5 conduct regular audits, and although his primary responsibilities “were over policy and
 6 compliance for Facebook apps and data protection, Parakilas said that “during my 16 months in
 7 that role at Facebook, I do not remember a single physical audit of a developer’s storage.”
 8 Parakilas “asked for more audits of developers and a more aggressive enforcement regime”
 9 Parakilas said he did not get a specific response, but “[e]ssentially, they did not want to do
 10 that.” According to Parakilas, “the company felt that it would be in a worse legal position if it
 11 investigated and understood the extent of abuse, and it did not.” The Committee Chair
 12 commented, “*it sounds like they turned a blind eye because they did not want to find out that*
 13 *truth.*” Parakilas agreed, stating, “That was my impression, yes.”

14 158. In response to a question from the U.K. Parliament’s Digital, Culture, Media and
 15 Sport Committee (the “DCMSC”), regarding how many developers Facebook had taken action
 16 against between **2011-2014**, Rebecca Stimson, Facebook U.K.’s Head of Public Policy,
 17 initially replied, “Due to system changes, we do not have records for the time-period before
 18 2014 that establish we terminated for developer violations...” The DCMSC wrote back, “Do
 19 you really have no records of developer violations for the time-period before 2014? If you
 20 don’t have records, would you agree that is a serious omission?”⁴

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

25 **1. Facebook’s Terms of Use Are Designed to Entice Users to Grant the**
 26 **Company Access to Their Data**

27 160. Facebook’s user agreement and associated privacy policies are set forth in the

28 ⁴ The DCSMC correspondence is attached hereto as **Exhibit 2**.

1 “Terms of Service” available on the Company’s website. This document explains the
2 Company’s business model and represents the user’s relationship with Facebook. The current
3 version of the agreement is meant to inform users about Facebook’s intentions with their data
4 and act as the mechanism that gives the company permission to proceed with its data gathering
5 and data sharing practices.

6 161. Facebook’s Terms of Service available on its website and in effect on December
7 1, 2008, prohibited “harvest[ing] or collect[ing] email addresses or other contact information of
8 other users from the Service or Site by electronic or other means for the purposes of sending
9 unsolicited emails or other unsolicited communications.

10 162. In his testimony before Congress, defendant Zuckerberg highlighted that “the
11 first line of our Terms of Service says that you control and own the information and content
12 that you put on Facebook...you own [your data] in the sense that you chose to put it there, you
13 could take it down anytime, and you completely control the terms under which it’s used.”

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

18 164. Facebook highlights that users always have the option to “allow” it to collect and
19 process your information. But because Facebook’s business depends upon users selecting the
20 “permission” option, their incentive is to use every possible strategy to engineer your consent.
21 The notion of privacy as control benefits Facebook, at the expense of its users, by allowing the
22 Company to leverage an illusion of agency via terms and settings to keep the data engine
23 humming.

24 165. Congress seemed to acknowledge these issues during the two-day hearing when
25 defendant Zuckerberg testified in **April 2018**. Senator Brian Schatz told Zuckerberg that with
26 terms of service at 3,200 words and a privacy policy at 2,700 words, “people really have no
27 earthly idea of what they’re signing up for.” Facebook’s full-length privacy policy would take
28 most people more than 10 minutes to read, though comprehension is another matter altogether.

1 Indeed, some academics have hypothesized that it would take users 25 days to read every
2 agreement on every site they've visited.

3 166. Facebook's policies are so broad as to be meaningless. Facebook's Terms of Use
4 say that Facebook collects almost everything users expose to it, from "things you do and
5 information you provide" and "your networks and connections" to "information from third-
6 party companies." But the availability of knowledge doesn't necessarily translate into
7 meaningfully informed decisions. In this context, users are being asked to consider the privacy
8 implications of each post they create—an impossibly complex calculation to make about future
9 risks and consequences, particularly given the highly technical issues involved. When
10 combined with Facebook's purposefully ambiguous and unclear representations about its
11 technology and the nature of its business, Facebook's Terms of Use and overall approach to
12 user privacy seriously oversimplifies risk. The modern data ecosystem is mind-bogglingly
13 complex, with many different kinds of information collected in many different ways, stored in
14 many different places, processed for many different functions, and shared with many other
15 parties.

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

24 **2. Facebook's Users Did Not Consent to Provide Their Personal**
25 **Information to Third Parties or to Any Alteration or Aggregation of**
26 **the Data for a Commercial Use**

27 168. According to PwC's Initial Assessment Report, Facebook's Privacy Program
28 encompasses the Facebook Platform, and "[t]he platform terms and policies outline a variety of

1 privacy obligations and restrictions, such as limits on an application’s use of data received
2 through Facebook, requirements that an application obtain consent for certain data uses, and
3 restriction on sharing user data.”

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

14 170. Former Facebook employee Parakilas explained, “Facebook had very few ways
15 of either discovering abuse once data had been passed or enforcing on abuse once it was
16 discovered.” Parakilas stated in his testimony before the British Parliament’s House of
17 Commons on March 21, 2018:

18 ... I can start by giving a brief description of how Facebook Platform, which is
19 what apps use, works, because it would be helpful in understanding this. When
20 you connect to an app, you being a user of Facebook, and that app is connected
21 to Facebook there are a number of categories of these apps, including games,
22 surveys and various other types. Facebook asks you, the user, for permission to
23 give the developer, the person who made the app, certain kinds of information
24 from your Facebook account, and once you agree Facebook passes that data
25 from Facebook servers to the developer. You then give the developer access to
26 your name, a list of the pages that you have liked and access to your photos, for
27 example.

28 The important thing to note here is that *once the data passed from Facebook servers to the developer, Facebook* lost insight into what was being done with the data and *lost control over the data*. To prevent abuse of the data once developers had it, Facebook created a set of platform policies—rules, essentially—that forbade certain kinds of activity, for example selling data or passing data to an ad network or a data broker.

1 However, *Facebook had very few ways of either discovering abuse once data*
2 *had been passed or enforcing on abuse once it was discovered.* In the event
3 that Facebook received a report of a data violation, it could do one of four
4 things: it could call up the developer and demand to know what they were doing
5 with the data; it could demand an audit of the developer’s application, their data
6 storage, and that was a right that was granted to Facebook in these policies, the
7 platform policies; it could delete the app and potentially ban the developer from
8 using Facebook Platform or even using other Facebook products such as
9 advertising; or it could sue the developer and pursue that app. Those are the
10 only four things that Facebook could do once it had determined that the
11 developer had been in breach of those policies....

12 I think one of the key things to understand is that if you do not have access to
13 the developer’s data storage, which you would not have unless you sued them
14 or they granted it to you willingly, then you cannot really see what data they
15 have, because what is exposed to the public view is not indicative.

16 171. Defendants claimed that Facebook had implemented a new app review process in
17 **2014**, where the Company would purportedly ensure that any new third party apps were only
18 using a limited amount of Facebook’s data for legitimate purposes that were permitted under
19 the Company’s updated policy, which Facebook’s users were informed of and had consented to
20 by virtue of their acceptance of Facebook’s terms of use. “People want more control,”
21 Facebook said at that time. “It’s going to make a huge difference with *building trust* with your
22 app’s audience.”

23 172. Facebook’s response to an inquiry from WIRED regarding the Cambridge
24 Analytica incident confirms that Facebook personnel were aware of similar user privacy issues
25 by at least **2014**, and knew that updates to Facebook’s policies and data security practices were
26 necessary to alleviate concerns that had already expressed by Facebook users. “In 2014, after
27 hearing feedback from the Facebook community, we made an update to ensure that each person
28 decides what information they want to share about themselves, including their friend list,”
29 Facebook stated. “Before you decide to use an app, you can review the permissions the
30 developer is requesting and choose which information to share. You can manage or revoke
31 those permissions at any time.”

32 173. In **April 2014**, Facebook announced it was changing what data were accessed on
33 the site. In a buried footnote suggesting that Facebook were eliminating several “rarely used

1 endpoints,” developers were able to discover that Facebook was in fact removing their access
 2 to a user’s newsfeed, their friendships, and data about friends (e.g., education, photos, and
 3 location). These end points were not rarely used, and given the millions of users of apps that
 4 leveraged Facebook’s photo-sharing APIs, it is clear that something else was afoot. This data
 5 was being used at that time in many highly popular applications, to the extent that technology
 6 journalism site Mashable Infographic suggested that Facebook platform data were used in
 7 seven of the top 10 apps on the Apple iOS app store as of 2012.

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

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

20
 21 An email receipt of a Facebook message from 2010 reviewed by TechCrunch
 22 proves Zuckerberg sent people messages that no longer appear in their
 23 Facebook chat logs or in the files available from Facebook’s Download Your
 24 Information tool.

25 When asked by TechCrunch about the situation, Facebook claimed in this
 26 statement it was done for corporate security: “After Sony Pictures’ emails were
 27 hacked in 2014 we made a number of changes to protect our executives’
 28 communications. These included limiting the retention period for Mark’s
 messages in Messenger. We did so in full compliance with our legal obligations
 to preserve messages.” However, Facebook never publicly disclosed the
 removal of messages from users’ inboxes, nor privately informed the recipients.

* * *

1
2
3
4
5
6
Facebook’s power to tamper with users’ private message threads could alarm some. The issue is amplified by the fact that Facebook Messenger now has 1.3 billion users, making it one of the most popular communication utilities in the world. Zuckerberg is known to have a team that helps him run his Facebook profile, with some special abilities for managing his 105 million followers and constant requests for his attention. *For example, Zuckerberg’s profile doesn’t show a button to add him as a friend on desktop, and the button is grayed out and disabled on mobile.*

7
8
9
10
11
12
176. TechCrunch commented that while it could be true that “Facebook may have sought to prevent leaks of sensitive corporate communications[,]” Facebook also “may have looked to thwart the publication of potentially embarrassing personal messages sent by Zuckerberg or other executives.” TechCrunch pointed to the “now-infamous instant messages from a 19-year-old Zuckerberg to a friend shortly after starting The Facebook” in 2004:

13
14
15
“yea so if you ever need info about anyone at harvard . . . just ask . . . i have over 4000 emails, pictures, addresses, sns” Zuckerberg wrote to a friend. “what!? how’d you manage that one?” they asked. *“people just submitted it . . . i don’t know why . . . they ‘trust me’ . . . dumb fucks”* Zuckerberg explained.

16
17
18
19
20
21
22
23
24
25
26
177. Although Facebook’s practice of tracking users through their use of mobile devices was not well-known at the time, defendant Zuckerberg likely did not want to be personally subjected to the same tracking methods and sharing of his personal information obtained by third parties as easily as Facebook allowed them to access information about all of its other users.

27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000

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

179. The unredacted portion of the Initial Assessment Report states with regard to Facebook’s “Ongoing Monitoring of the Privacy Program”: “The XFN process ensures that new products and changes to existing products that result in material and/or retroactive changes

1 to the use of information are evaluated to determine whether additional notice or consent from
2 Facebook users is required. Where required, key decisions around the need for additional
3 consent from users are discussed and recommendations are made and implemented by the XFN
4 team.

5 180. The fact that Facebook refers to the possibility of learning about “retroactive
6 changes to the use of information” that may require consent is further confirmation that the
7 Company’s policies and views on consent are completely unreasonable given that they depend
8 on a presumption that it is possible to obtain “retroactive” consent. It is not.

9 **3. A German Court Found Facebook’s Privacy Settings and Terms are**
10 **Invalid to Obtain Consent in 2018**

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

18 182. The Federation also argued that various clauses in the terms and conditions of
19 Facebook were invalid, including clauses that provide consent of the user (i) to transferring
20 personal data to and processing personal data in the U.S. and (ii) using the name and profile
21 picture of the user for commercial, sponsored or related content.

22 183. The court held that Facebook’s default privacy settings and parts of their terms
23 and conditions were invalid. The court found, among other things, that the default privacy
24 settings include a location service in the app that reveals the location of the person that the user
25 is chatting to. In addition, boxes were pre-ticked allowing search engines to link the user’s
26 timeline. The court noted that there was no valid consent as there was no guarantee that users
27 knew that these boxes were ticked by default.
28

1 **G. EARLY LITIGATION AND COMPLAINTS ABOUT FACEBOOK’S PRIVACY**
2 **VIOLATIONS SHOULD HAVE PROMPTED THE BOARD TO IMPLEMENT**
3 **REASONABLE CONTROLS**

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

10 185. In **2009**, Facebook began making users’ posts, which had previously been
11 private, public by default. That incident triggered anger, confusion, an investigation by the
12 FTC, and, ultimately, a consent decree.

13 186. Defendants responded by proposing a “site governance” system under which its
14 users would supposedly be given some collective control over their data through “referendums”
15 that Facebook planned to hold. At the time, defendant Zuckerberg explained, “Rather than
16 simply reissue a new Terms of Use, the changes we’re announcing today are designed to open
17 up Facebook so that users can participate meaningfully in our policies and our future.”
18 Just three years later, in 2012, the final referendum was held, which involved setting the terms
19 under which Facebook could share user data with other organizations. Because a relatively
20 small percentage of users had voted in the prior referendums, Defendants decided that the
21 referendum would only be considered binding in the (extremely unlikely) case that 30 percent
22 of its global users voted. Ultimately, only 668,000 users voted, and Defendants ignored the
23 result, and never held another user referendum again.

24 187. In **March 2010**, Facebook settled a class action for \$9.5 million to resolve claims
25 regarding its Beacon feature, which tracked what users buy online and shared the information
26 with their friends. Users were unaware that such features were being tracked, and the privacy
27 settings originally did not allow users to opt out. As a result of widespread criticism, Beacon
28 was eventually shut down. Reflecting on Beacon, defendant Zuckerberg attributed part of
 Facebook’s success to giving “people control over what and how they share information.” He

1 said that he regretted making Beacon an “optout system instead of opt-in ... if someone forgot
2 to decline to share something, Beacon went ahead and still shared it with their friends.”

3 188. In September 2011, the Office of the Data Protection Commissioner of Ireland
4 initiated an audit of Facebook’s activities outside the U.S. and Canada, after receiving
5 complaints about how the social networking giant handled users’ information. In its December
6 2011 audit report, the regulator suggested that the company implement several changes to
7 improve compliance with EU data protection laws, including better educating users about its
8 tag suggest tool. On September 21, 2012, a follow-up audit revealed that Facebook has failed
9 to minimize the potential for ad targeting based on words and terms that could be considered
10 “sensitive personal data,” and that Facebook improve its new user education, deletion of social
11 plug-in impression data for EU users and account deletion practices within the next month in
12 order to bring it into compliance with Irish and EU data protection requirements.

13 189. On December 9, 2011, a bipartisan group sought answers from defendant
14 Zuckerberg regarding the Company’s privacy practices, questioning why the site’s privacy
15 policy was longer than the U.S. Constitution. In a letter to Facebook, the group pointed out
16 that Facebook’s current privacy policy was almost six times as long as it was in 2005, longer
17 than other social networks’ policies and the Constitution, not including the amendments. The
18 representatives asked Zuckerberg to give them data regarding the percentage of Facebook users
19 who read the full policy. “We are concerned ... that long, complex privacy policy statements
20 make it difficult for consumers to understand how their information is being used,” the letter
21 said.

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

26 Facebook, like every significant internet service, is frequently targeted by those
27 who want to disrupt or access our data and infrastructure. As such, *we invest*
28 *heavily in preventing, detecting, and responding to threats that target our*
infrastructure, and we never stop working to protect the people who use our
service. The vast majority of the time, we are successful in preventing harm

1 before it happens, and our security team works to quickly and effectively
2 investigate and stop abuse.

3 Last month, Facebook Security discovered that our systems had been targeted
4 in a sophisticated attack. As soon as we discovered the presence of the
5 malware, we remediated all infected machines, informed law enforcement, and
6 began a significant investigation that continues to this day. We have found no
7 evidence that Facebook user data was compromised.

8 As part of our ongoing investigation, we are working continuously and closely
9 with our own internal engineering teams, with security teams at other
10 companies, and with law enforcement authorities to learn everything we can
11 about the attack, and how to prevent similar incidents in the future.

12 * * *

13 We will continue to work with law enforcement and the other organizations and
14 entities affected by this attack. It is in everyone's interests for our industry to
15 work together to prevent attacks such as these in the future.

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

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

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

23 a. In December 2009, Facebook changed its website so certain information that
24 users may have designated as private – such as their Friends List – was made public.
25 They didn't warn users that this change was coming, or get their approval in advance.

26 b. Facebook represented that third-party apps that users' installed would have
27 access only to user information that they needed to operate. In fact, the apps could access
28 nearly all of users' personal data – data the apps didn't need.

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

d. Facebook had a "Verified Apps" program & claimed it certified the security of

1 participating apps. It didn't.

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

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

7 g. Facebook claimed that it complied with the U.S.- EU Safe Harbor Framework
8 that governs data transfer between the U.S. and the European Union. It didn't.

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

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

24 195. In the Consent Agreement, Defendants agreed that Facebook will not
25 "misrepresent in any manner, expressly or by implication, the extent to which it maintains the
26 privacy or security of covered information," including "the extent to which [Facebook] makes
27 or has made covered information accessible to third parties;" that prior to sharing of a user's
28 nonpublic information, the company will "obtain the user's affirmative express consent;" and

1 the company would “establish and implement, and thereafter maintain, a comprehensive
2 privacy program that is reasonably designed to (1) address privacy risks related to the
3 development and management of new and existing products and services for consumers, and
4 (2) protect the privacy and confidentiality of covered information,” among other stipulations.

5 196. The Consent Decree barred Facebook from making any further deceptive privacy
6 claims, required Facebook to obtain consumers’ approval before it changed the way it shared
7 their data, and required Facebook to obtain periodic assessments of its privacy practices by
8 independent, third-party auditors for 20 years following its entry.

9 197. The Board was well aware of the FTC Consent Decree and the obligations placed
10 on Facebook, as each director personally received a copy of the Consent Decree on September
11 12, 2012, according to the Facebook Compliance Report that was submitted to the FTC by
12 Facebook’s in-house attorneys on November 13, 2012, and those who joined the Board after
13 that date also received a copy within thirty (30) days after their appointment as directors.⁵
14 Moreover, each of the directors is specifically obligated to oversee the Company’s compliance
15 with its terms.

16 198. Defendants’ failure to comply with the Consent Decree has exposed Facebook to
17 liability for violating the Consent Decree. The FTC confirmed on March 23, 2018, that it is
18 investigating Facebook for potential violations of the Consent Decree.

19 199. Rather than complying with the Consent Decree and adopting a reasonable
20 Privacy Program and internal controls and procedures designed to detect and prevent violations
21 of law, Defendants deliberately concealed from Facebook’s users, shareholders, regulators, and
22 government officials the true nature of Facebook’s business.

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

26 201. Defendants’ actions (and inactions) have exposed Facebook to liability for
27 violating the FTC Consent Decree. Defendants failed to comply with the Consent Decree in at

28 ⁵ The Facebook Compliance Report dated November 13, 2012 is attached hereto as **Exhibit 3**.

1 least the following ways.

2 202. ***First***, the public statements of Defendants and others do not comply with Section
3 I of the Order, which prohibits Facebook from misrepresenting any of its privacy settings. The
4 FTC evaluates misrepresentations based on what consumers reasonably understand. In its
5 Complaint, the FTC found that Facebook had misrepresented the extent of access that third-
6 party apps had to user data. After the Order went into effect, Facebook continued to grant
7 third-party apps the same level of access to user data as it had before, without ever correcting
8 its misrepresentation. GSR, the company that transferred data to Cambridge Analytica,
9 acquired its data from Facebook in June 2014, two years after the Order went into effect.

10 203. ***Second***, the Board failed to implement and revise Facebook’s policies and terms
11 of use to ensure they complied with Section II of the Order, which required Facebook to obtain
12 affirmative express consent and give its users clear and prominent notice before disclosing their
13 previously collected information with third parties in a way that exceeds the restrictions
14 imposed by their privacy settings. As the FTC found, Facebook granted third-party apps access
15 to user data by overriding users’ privacy settings. After the Order went into effect, Facebook
16 never clearly and prominently disclosed this practice to users and did not retroactively seek
17 users’ express affirmative consent to continue disclosing their previously-collected data to
18 third-party apps.

19 204. On April 19, 2018, Senator Blumenthal sent a letter to the FTC, noting that
20 Facebook by default continued to provide access to personal and non-public data to third-party
21 apps even after the consent decree. As he did at the April 10 Senate hearing, Senator
22 Blumenthal specifically called out Facebook for failing to notice that Kogan submitted terms of
23 service for his app that explicitly stated that he reserved the right to sell user data and would
24 collect profile information from the friends of those who downloaded the app. “***Even the most***
25 ***rudimentary oversight would have uncovered these problematic terms of service,***”
26 Blumenthal wrote. “This ***willful blindness*** left users vulnerable to the actions of Cambridge
27 Analytica.”

28 205. According to PwC’s Initial Assessment Report, which is based on Management

1 Assertions, Facebook’s Privacy Program is routinely monitored, reviewed, and improved. The
2 report states, in relevant part:

3
4 **Monitoring Activities:** Members of Facebook’s Legal team periodically review
5 the Privacy Program to ensure it, including the controls and procedures contained
6 therein, remains effective. These legal team members also will serve as point of
7 contacts for control owners and will update the Privacy Program to reflect any
8 changes or updates surfaced.

9
10 **Monitoring:** Facebook’s Privacy Program is designed with procedures for
11 evaluating and adjusting the Privacy Program in light of the results of testing and
12 monitoring of the program as well as other relevant circumstances. The Privacy
13 XFN Team assesses risks and controls on an on-going basis through weekly
14 meetings and review processes. Members of Facebook’s legal team support the
15 Privacy Program and serve as points of contact for all relevant control owners to
16 communicate recommended adjustments to the Privacy Program based on regular
17 monitoring of the controls for which they are responsible, as well as any internal or
18 external changes that affect those controls.

19 206. The “Management Assertions” and other statements in PwC’s reports about
20 Facebook’s Privacy Program are misleading and contradict Defendants’ own representations.
21 For example, defendant Sandberg admitted in an interview with Recode Media on May 30,
22 2018 that Facebook had not audited Cambridge Analytica to ensure they had actually deleted
23 the data. “*Looking back, we definitely wish we had put more controls in place.* We got legal
24 certification that Cambridge Analytica didn’t have the data, *we didn’t audit them,*” she said.

25 207. **Third,** Facebook was required under Section IV of the Order to establish a
26 “comprehensive privacy program” that would: “(1) address privacy risks related to the
27 development and management of new and existing products and services, and (2) protect the
28 privacy and confidentiality of covered information.” The privacy program must be designed to
prevent “unauthorized collection, use, or disclosure of covered information.” PwC’s Initial
Assessment Report, which is based on Management Assertions, states that “Facebook has
implemented technical, physical, and administrative security controls designed to protect user
data from unauthorized access, as well as to prevent, detect, and respond to security threats and
vulnerabilities.” But defendant Zuckerberg admitted in testimony before Congress and the
British Parliament that Facebook failed to read the terms and conditions of the GSR app which

1 sold the data to Cambridge Analytica.

2 208. Senator Blumenthal, in his letter to the FTC sent on April 19, 2018, noted that
3 although the FTC explicitly put Facebook on notice about the privacy risks of third-party apps
4 with the 2011 consent decree, the Company has “*continued to turn a blind eye*” to other
5 outside parties that collect data from its users, and its procedures for verifying that new apps
6 comply with its remain “murky,” Senator Blumenthal said in his letter. Indeed, as the *New*
7 *York Times* reported on June 3, 2018, Facebook still allows others besides “third party apps” to
8 access the same user data that the Company purportedly banned when it revised its policy in
9 2015, including Chinese mobile device manufacturers, such as Huawei, which poses a national
10 security risk. *See* Section IX, *infra*.

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

19 210. Defendants not only had the ability (and responsibility) to change Facebook’s
20 policies and practices with respect to third party developer access to user information, they
21 were also well aware of, and facilitated, this activity through Facebook’s unlawful business
22 practices and inadequate privacy policies which they knew could cause substantial damage to
23 Facebook and potential violations of the FTC Consent Decree.

24 211. FTC Commissioner Chopra noted in a recent memorandum to FTC staff that
25 going forward, “[w]hen orders are violated, a key question [the FTC] will evaluate is
26 whether the proposed remedies address the underlying causes of the noncompliance.” Chopra
27 said the FTC will “hold individual executives accountable for order violations in which they
28 participated, even if these individuals were not named in the original orders[.]” noting that

1 “[t]his relief is expressly contemplated by Fed. R. Civ. P. 65(d), which provides that an
2 injunction against a corporation binds its officers.” Moreover, Chopra explained, “this relief is
3 important, because it ensures that individual executives who control the operation of the firm –
4 and not just shareholders – bear the costs of noncompliance.”⁶

5 2. **Defendants Ignored Concerns Raised By Facebook’s Chief
6 Information Security Officer About the Security of Facebook’s
7 Platform**

8 212. Facebook’s Chief Information Security Officer Stamos wrote a memo in 2016 that
9 was subsequently turned into a “White Paper” entitled “Information Operations and Facebook,”
10 which unquestionably alerted Defendants that those activities were pervasive and supported by
11 management. The “White Paper” also confirmed that Defendants’ public statements were false
12 and misleading. Among other things, the White Paper affirmatively misrepresented that
13 Facebook had “no evidence of any Facebook accounts being compromised” in connection with
14 the 2016 election as of the date it was published on April 27, 2017.

15 213. Stamos later said that he had initially provided a written report to Facebook
16 executives concerning the circumstances which led to the Cambridge Analytica leak, but instead
17 of taking appropriate action and disclosing the leak, the report was rewritten and presented as a
18 hypothetical scenario, which appeared in the whitewashed “White Paper” that Facebook
19 published which further suppressed and concealed the wrongdoing at the Company.

20 214. On September 6, 2017, Stamos published “An Update on Information Operations
21 On Facebook” in the Facebook newsroom, and addressed some of the concerns that had been
22 raised in the media about possible Russian interference with the U.S. presidential election.

23 215. Despite warnings from Stamos and others of similar concerns that Russian
24 interference could have occurred via Facebook’s platform, Defendants brushed them aside as
25 frivolous and initially acted as though it was impossible.

26 216. But on October 22, 2017, the *Guardian* reported that Facebook had handed to the
27 special counsel and congressional investigators looking into the Kremlin’s interference the

28 _____
⁶ The Memorandum is attached hereto as **Exhibit 4**.

1 content of 3,000 political ads paid for by a shadowy Russian entity called the Internet Research
2 Agency (IRA).

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

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

18 3. Former Zuckerberg Mentor Warned of Data Security Issues in 2016

19 219. Roger McNamee (“McNamee”), a longtime Silicon Valley investor and reported
20 Facebook insider also warned Facebook executives about data security issues by at least 2016,
21 which also went unheeded. McNamee was Zuckerberg’s mentor before Facebook went public,
22 and an early investor in the Company. McNamee and Zuckerberg first met in 2006 when
23 Facebook’s then Chief Privacy Officer, Chris Kelly, called McNamee to give some advice to
24 Zuckerberg on whether or not to sell the company to Yahoo!. As McNamee describes his first
25 encounter with Zuckerberg: “I began by letting Mark know the perspective I was coming from.
26 Soon I predicted, he would get a billion-dollar offer to buy Facebook from either Microsoft or
27 Yahoo, and everyone, from the company’s board to the executive staff to Mark’s parents,
28 would advise him to take it. I told Mark that he should turn down any acquisition offer. He

1 had an opportunity to create a uniquely great company if he remained true to his vision... I told
2 Mark the market was much bigger than just young people; the real value would come when
3 busy adults, parents and grandparents, joined the network and used it to keep in touch with
4 people they didn't get to see often." McNamee advised against selling the company. After this
5 meeting, McNamee and Zuckerberg developed a close mentoring relationship, and McNamee
6 reportedly acted as a father figure to Zuckerberg. McNamee suggested to Zuckerberg that he
7 hire Sandberg as Facebook's COO. By the time Facebook went public, McNamee was no
8 longer a mentor to Zuckerberg. That role was taken over by Facebook directors defendants
9 Andreessen and Thiel.

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

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

21 222. On October 30, 2016, McNamee sent a draft of the op-ed piece to Zuckerberg
22 and Sandberg. According to McNamee, "They each responded the next day. The gist of their
23 messages was the same: We appreciate you reaching out; we think you're misinterpreting the
24 news; we're doing great things that you can't see. Then they connected me to Dan Rose, a
25 longtime Facebook executive with whom I had an excellent relationship. Dan is a great listener
26 and a patient man, but *he was unwilling to accept that there might be a systemic issue*.
27 Instead, he asserted that Facebook was not a media company, and therefore was not responsible
28 for the actions of third parties." McNamee ultimately decided to not publish the op-ed piece,

1 explaining, “Mark and Sheryl were my friends, and my goal was to make them aware of the
2 problems so they could fix them. I certainly wasn’t trying to take down a company in which I
3 still hold equity.”

4 223. Defendants ignored the warnings from McNamee. McNamee told *Quartz* that he
5 didn’t expect Zuckerberg to “just accept” the warning message that he sent him, “We hadn’t
6 spoken in a number of years at that point, but we had traded emails and it was always positive.
7 But when I saw what was going on in 2016, I was genuinely concerned. I just assumed that he
8 would have trouble accepting it, because they hadn’t had anything negative in three or four
9 years. It must have been really hard for him to appreciate that everything wasn’t perfect. But I
10 kind of hoped that if I talked to Dan Rose over a period of weeks or months, they would have
11 eventually follow through. The shock would pass and they would think ‘Roger is actually
12 really serious about this, maybe we should just check it out.’ But after three months, I realized
13 they were never going to check it out.”

14 224. Defendants also ignored numerous other “red flag” warnings regarding the
15 Company’s inadequate internal controls.

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

19 226. On November 29, 2011, Facebook settled the FTC’s claims that it deceived its
20 users, which numbered 750 million worldwide at the time, about the privacy of their personal
21 data, including names, birthdays, location, friends and sexual orientation. The FTC took
22 particular issue with privacy changes Facebook made in December 2009 that overrode users’
23 privacy settings with no notice or consent.

24 **V. DEFENDANTS ALLOWED FACEBOOK TO ENGAGE IN ILLEGAL AND**
25 **DECEPTIVE BUSINESS PRACTICES FOR MORE THAN A DECADE**

26 227. Since at least 2008, Facebook’s Board has pursued profits at the expense of
27 compliance with the law.

28 228. Facebook’s source code and associated documentation was used to (a) access

1 other third party websites to which Facebook's users did not consent and which was in
2 violation of Facebook's Terms of Service; (b) other third party websites to and acquire
3 Facebook user information and related data for commercial purposes; (c) download acquired
4 user data to Facebook's own website, (d) use downloaded user data to display Facebook
5 information on other third party websites and on Facebook's website without the users'
6 permission; and (e) to employ automated scripts to initiate unauthorized communications with
7 non-Facebook users soliciting them to join Facebook. All of this source code was used by
8 Facebook to improperly connect to other websites without users' permission to further
9 Defendants' own commercial purposes and gain.

10 229. The source code includes at least facebook.com website (i.e., html) source code,
11 website sitemap, scripts, build files, readme files, tutorial examples, functional specifications
12 and diagrams, architecture specifications and diagrams, system specifications and diagrams,
13 website specifications and diagrams, server file system and database security documentation.
14 The source code data is the best evidence of how Facebook initiated unauthorized access to
15 other websites, acquired, downloaded and displayed user information on Facebook's own
16 website, and then "spammed" non-Facebook users with invitations to join Facebook, and
17 includes any scripts, both server-side (runs on facebook.com servers) and client side (runs on
18 the user's computer), all application source code written or used for gathering Facebook users'
19 content or executing functions using Facebook's "Like" button, the database or databases used
20 by the website and/or by Facebook, documentation on the email service or services used by
21 Facebook, files written or read by the programs, the source code used to compile, interpret, and
22 execute scripts, and the source code for any spider(s) and any crawler(s) used by Facebook.

23 230. Facebook used various attributes and variables to associate downloaded
24 information that Facebook obtained from third parties with the information Facebook stored
25 about its own users, interacted with other websites' software, and was used and could be used
26 to initiate events (such as Group Events) to solicit Facebook users to join Power, what
27 commands were used by Power to obtain information from and/or to send communications to
28 Facebook users, what database files were used in Power's own database reflecting who were

1 Facebook users, how Facebook user profile information was parsed and reformatted on the
2 website www.power.com, or similar important critical technical details.

3 231. On April 18, 2018, researchers at Princeton University reported that third-party
4 tracking code, used across the internet to track user behaviors on websites, optimize ads and
5 other purposes, obtains Facebook user information on websites that support logging in through
6 the social media platform. When users log in to websites using Facebook’s Login feature,
7 trackers can grab Facebook user IDs and in some cases other information such as email address
8 or gender, potentially without the knowledge of the operators of the websites where the
9 trackers are installed, according to the researchers. “[W]hen a user grants a website access to
10 their social media profile, they are not only trusting that website, but also third parties
11 embedded on that site,” write Gunes Acar, Arvind Narayanan, and Steven Englehardt, a
12 Mozilla privacy engineer who also researches privacy at Princeton. The researchers posted
13 their findings on Freedom to Tinker, a website that is hosted by Princeton’s Center for
14 Information Technology Policy, a research center that studies digital technologies in public
15 life.⁷

16 232. The researchers said that they had found “another type of surreptitious data
17 collection by third-party scripts” – “the exfiltration of personal identifiers from websites
18 through “login with Facebook” and other such social login APIs.” Specifically, they found that
19 “*seven third parties abuse websites’ access to Facebook user data*” and “one third party uses
20 its own Facebook ‘application’ to track users around the web.” With regard to the seven third
21 parties, researchers said that while “these scripts query the Facebook API and save the user’s
22 Facebook ID, we could not verify that it is sent to their server due to obfuscation of their
23 code[.]” The researchers concluded, “*This unintended exposure of Facebook data to third*
24 *parties is not due to a bug in Facebook’s Login feature. Rather, it is due to the lack of*
25 *security boundaries* between the first-party and third-party scripts in today’s web.”

26 **A. FACEBOOK’S AGREEMENTS WITH THIRD PARTY “SERVICE PROVIDERS”**
VIOLATED THE CONSENT DECREE

27 ⁷ See “No boundaries for Facebook data: third party trackers abuse Facebook Login” *available*
28 *at* <https://freedom-to-tinker.com/2018/04/18/no-boundaries-for-facebook-data-third-party-trackers-abuse-facebook-login/>

1 233. On June 3, 2018, an article published by *The New York Times* reported that
2 Facebook had entered into agreements over the past decade with at least 60 device makers,
3 including Apple, Amazon, BlackBerry, Microsoft and Samsung, that allowed them to access
4 vast amounts of Facebook information, including data about users’ friends who had blocked
5 such third-party access. These data-sharing partnerships, which Facebook entered into as early
6 as 2007, gave these companies the ability to offer “features” of the social network, such as
7 messaging, “like” buttons and friends (contacts) lists, on their own websites and mobile
8 devices. *The Times* reported that Facebook provided mechanisms for certain phone and device
9 manufacturers to build software accessing user data, supposedly to integrate Facebook features
10 before app markets came into widespread use.

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

16 235. According to a 2012 report by the CIA and the FBI, an agreement like this with
17 Huawei could present a substantial threat of “economic espionage.” Although Huawei has
18 been flagged by American intelligence officials as a national security threat, Facebook’s
19 agreement with Huawei was still in effect as of June 5, 2018, when Facebook representatives
20 acknowledged these arrangements publicly for the first time.

21 236. Francisco Varela, Facebook’s vice president of mobile partnerships, said in a
22 statement that “many other U.S. tech companies have worked with [Huawei] and other Chinese
23 manufacturers” and that “Facebook’s integrations were controlled from the get go – and
24 [Facebook] approved” everything they built using Facebook information. Varela said that
25 these agreements with manufacturers were common at the time they were developed, and the
26 deals were supposedly struck to help users access Facebook features such as the “like” button
27 on their devices. Varela told the *Times* that Huawei used its Facebook access to feed a social
28 phone app that lets users see messages and social media accounts in one place, and emphasized

1 that the data Huawei had access to stayed on phones and was not transferred to or stored on its
 2 servers. “Given the interest from Congress, we wanted to make clear that all the information
 3 from these integrations with Huawei was stored on the device, not on Huawei’s servers,”
 4 Varela said.

5 237. Facebook’s Vice President of Product Partnerships, Ime Archibong
 6 (“Archibong”), also addressed the agreements in a Facebook Newsroom post titled “Why We
 7 Disagree With The New York Times.” According to Archibong, “in the early days of mobile,”
 8 Facebook had built a set of private APIs that allowed companies like Apple, Amazon and HTC
 9 to “recreate Facebook-like experiences for their individual devices or operating systems” for
 10 users who weren’t able to put a Facebook app on their device.

11 238. The Company’s representatives claimed that Facebook had already decided to
 12 start winding down these arrangements in April 2018, but did not explain why they had never
 13 previously been disclosed, particularly during defendant Zuckerberg’s testimony before
 14 Congress. He also disputed the assertion that this access went beyond what users had agreed to
 15 or were expecting.

16 239. Indeed, defendant Zuckerberg did not even mention the contracts with other third
 17 party companies in his testimony. There are two kinds of arrangements that Facebook has that
 18 are supposedly “winding down” because both appear, unsurprisingly, to violate Defendants’
 19 promises to protect user privacy (and perhaps, the Consent Decree).

20 **B. PWC IMPROPERLY CERTIFIED THAT FACEBOOK’S PRIVACY PROGRAM**
 21 **SATISFIED THE FTC CONSENT DECREE IN AUDIT REPORTS FROM 2013- 2017**

22 240. PwC is the supposedly “independent” auditor that Facebook retained to conduct
 23 the audits that are required under Section VI of the Consent Decree. Thus far, PwC has
 24 prepared three assessments that Facebook has submitted to the FTC certifying that Facebook’s
 25 privacy program meets or exceeds the requirements of the 2011 Consent Decree.⁸

26 ⁸ The Independent Assessor’s Report on Facebook’s Privacy Program, Initial Assessment Report
 27 for the period August 15, 2012 to February 11, 2013 is attached hereto as **Exhibit 5**. A redacted
 28 version of the report was initially submitted by Facebook to the FTC on April 22, 2013 in a letter
 to James A. Kohn, the FTC’s Associate Director for the Division of Enforcement, which is
 attached hereto as **Exhibit 6**.

1 241. In all three audit reports that Facebook has submitted to the FTC, PwC certified
2 that Facebook’s privacy controls were operating with sufficient effectiveness to provide
3 reasonable assurance to protect the privacy of covered information and that the controls have so
4 operated throughout the reporting periods.⁹

5 242. PwC’s certifications are based on purported facts, called “assertions” in the audit
6 reports, which are actually management’s own assertions that were admittedly provided to
7 PwC by Facebook for the purpose of the supposedly “independent” audits. These “assertions”
8 were assumed true for purposes of the audit and were not determined in the course of an
9 independent audit conducted by PwC or confirmed by PwC based upon reasonable auditing
10 procedures developed independently of Facebook’s management. PwC acted unreasonably in
11 relying on management’s assertions, and taking them as “fact,” without conducting an
12 appropriate investigation and review of the information that was provided to determine whether
13 it was sufficiently reliable and supported by Facebook’s records, documentation, or other
14 evidence.

15 243. According to the audit report for the period February 12, 2015 to February 11,
16 2017, Facebook constantly enhances or updates its program to protect individual/users
17 information, and Facebook’s Privacy XFN Team assists the chief officers and his team to
18 review and feedback on new product proposals and any material changes to existing products
19 from a privacy perspective.

20 244. The audit report for the period August 15, 2012 to February 11, 2013 indicates
21 that Facebook’s Privacy Program was defined by the following assertions: responsibility for the
22 Facebook Privacy Program, privacy Risk Assessment, Privacy and Security awareness, notice,
23 choice, consent, collection and assess, security for privacy, third-party developers, service
24 provider, and on-going monitoring of the privacy program. These assertions are based on the
25 following “facts” that were not independently verified by PwC:

26 a. Facebook provides notices to users regarding its privacy policies and procedures,

27 ⁹ Plaintiffs expressly incorporate by reference as though fully set forth herein the Independent
28 Assessor’s Report on Facebook’s Privacy Program, Biennial Report, for the periods February
12, 2013 to February 11, 2015, and February 12, 2015 to February 11, 2017.

1 identifies the purposes for which personal information is collected, used, retained
2 and disclosed.

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

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

8 245. Although defendant Zuckerberg admitted that he learned of the data exfiltration
9 to Cambridge Analytica in 2015, he claimed Facebook had no knowledge or reason to believe
10 that it was not deleted until more than two years later — the same period that PwC assessed
11 Facebook's privacy program and found the Company's internal controls were effective to
12 detect and prevent similar wrongdoing.

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

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

26 248. Defendants knew (or should have known) that once the data was exfiltrated by a
27 third party, there was no way for Facebook to recover the data or to ensure it would not be
28 further exposed or compromised in the future. Even if there was, Defendants did not even

1 attempt to secure Facebook’s user data and failed to implement any auditing or enforcement
2 procedures. Instead, Defendants turned a blind eye to obvious violations of Facebook’s
3 policies, failed to ensure that the Company’s privacy program was effective and that their
4 statements about Facebook’s data security and user privacy practices were not misleading.

5 249. The FTC announced on March 17, 2016, that it had issued warning letters to 12
6 app developers who installed SilverPush software in their apps, which allowed them to monitor
7 the television viewing habits of consumers who used the apps across various devices. The FTC
8 warned that embedding this software in their apps without notifying users could violate Section
9 5 of the Federal Trade Commission Act.

10 250. The FTC had shown an interest in cross-device tracking because consumers were
11 beginning to connect to the internet in a variety of ways, including smartphones, tablets and
12 wearable devices, which raised (and continues to raise) privacy and security concerns as
13 businesses develop new methods to track their behavior across devices. The FTC warning
14 letters sought to address the privacy implications of the SilverPush software even *before* the
15 technology had been directed at the U.S., and they demonstrate the need for Facebook to make
16 disclosures about cross-device tracking, among other things.

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

21 252. Facebook’s statements on its website confirm the Company’s cross-device
22 tracking capabilities, and its partnerships with third party device manufacturers indicate a much
23 larger – and more dangerous – scale than the FTC warned about.

24 253. Defendants knew, and PwC should have uncovered in its audit, that Facebook
25 embedded software and certain Facebook “features” in mobile devices manufactured by Apple
26 and even allowed Chinese companies to embed Facebook “features” in their mobile devices
27 despite the serious threat it poses to national security.

28 254. In PwC’s Initial Assessment Report, Facebook’s Control Activity with regard to

1 Service Providers states, “The privacy policies of Facebook and Instagram contain a section
2 that ‘informs users that the information Facebook and Instagram receive may be shared with
3 service organizations when a user signs up for Facebook and Instagram accounts.’” The
4 unredacted portions of the report do not disclose that Facebook apparently referred to but did
5 not disclose that these multinational corporations are the “service providers” with which
6 Facebook maintained data sharing agreements.

7 255. Although other companies are also referred to in the report, they are “Facebook
8 Experience application developers” that “must read and sign-off on the Extended API
9 Addendum (the ‘Addendum’), or ... the terms and conditions for a developer’s adherence to
10 Facebook’s Platform Policies, Statement of Rights and Responsibilities and data policies and
11 procedures” that apply to third party app developers like Kogan, who were supposedly required
12 to follow the same policies that Defendants did not enforce.

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

17 257. PwC’s report makes clear that Defendants may not actually enforce the terms of
18 those agreements, just as they failed to enforce Facebook’s platform policies, which would
19 similarly provide users with essentially no protection from the exfiltration of their data. PwC,
20 had it conducted a reasonable review or audit beyond Management’s Assertions, would have
21 learned these facts. Facebook’s agreements with mobile device manufacturers have been in
22 effect since 2012, throughout the entire audit period thus far, and the FTC stated in 2013 that it
23 was focusing increasingly on privacy disclosures in apps because “mobile technology raises
24 unique privacy concerns” given that mobile devices are “almost always on[] and with the user”
25 and “can facilitate unprecedented amounts of data collection.”¹⁰

26 258. The FTC warning letters also demonstrate the need for disclosures concerning

27 ¹⁰ See Fed. Trade Comm’n Press Release, FTC Staff Report Recommends Ways to Improve
28 Mobile Privacy Disclosures, Feb. 1, 2013, *available at* <https://www.ftc.gov/news-events/press-releases/2013/02/ftc-staff-report-recommends-ways-improve-mobile-privacy>.

1 cross-device tracking, because consumers are now connecting to the internet in a variety of
 2 ways, including through smartphones, tablets and wearable devices, and the FTC noted
 3 concerns about privacy violations arising as businesses develop new methods to track
 4 consumer behavior across devices as early as 2015, and again in 2016.¹¹

5 259. The FTC further made clear as early as 2013 that these activities implicate
 6 privacy issues and must be disclosed, and PwC's failure to detect or determine that Facebook's
 7 privacy program may be insufficient to prevent these type of disclosure violations is
 8 particularly egregious given the circumstances. Facebook acquired the Atlas technology from
 9 Microsoft in 2012 and also partnered with Apple; thus, it essentially pioneered this very
 10 activity.¹²

11 260. The fact that PwC found no deficiencies in Facebook's internal controls
 12 following the WhatsApp acquisition in 2014 is similarly egregious, given that the FTC
 13 specifically warned Defendants in 2014 about their obligations to protect the privacy of their
 14 users in light of the proposed acquisition.¹³

15 **C. FACEBOOK'S ACQUISITION OF WHATSAPP VIOLATED THE EUROPEAN**
 16 **UNION'S MERGER REGULATION**

17 261. In a letter to Facebook and WhatsApp general counsel sent on April 10, 2014,
 18 Jessica Rich, Director of the FTC's Bureau of Consumer Protection, noted that WhatsApp has
 19 made clear privacy promises to consumers, and that both companies have told consumers that
 20 after any acquisition, WhatsApp will continue its current privacy practices. "We want to make

21 ¹¹ See, e.g., Fed. Trade Comm'n Press Release, FTC To Host Workshop on Cross-Device
 22 Tracking Nov. 16, Mar. 17, 2015, *available at* [https://www.ftc.gov/news-events/press-](https://www.ftc.gov/news-events/press-releases/2015/03/ftc-host-workshop-cross-device-tracking-nov-16)
 23 [releases/2015/03/ftc-host-workshop-cross-device-tracking-nov-16](https://www.ftc.gov/news-events/press-releases/2015/03/ftc-host-workshop-cross-device-tracking-nov-16). Center for Democracy &
 Technology, Comments for November 2015 Workshop on Cross-Device Tracking. *available at*
https://www.ftc.gov/system/files/documents/public_comments/2015/10/00056-99849.pdf.

24 ¹² See Fed. Trade Comm'n Staff Report, Mobile Privacy Disclosures: Building Trust Through
 25 Transparency, Feb. 2013, *available at*
 26 [https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-](https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf)
[trust-through-transparency-federal-trade-commission-staff-](https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf)
[report/130201mobileprivacyreport.pdf](https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf).

27 ¹³ See Fed. Trade Comm'n Press Release, FTC Notifies Facebook, WhatsApp of Privacy
 28 Obligations in Light of Proposed Acquisition, Apr. 10, 2014, *available at*
[https://www.ftc.gov/news-events/press-releases/2014/04/ftc-notifies-facebook-whatsapp-](https://www.ftc.gov/news-events/press-releases/2014/04/ftc-notifies-facebook-whatsapp-privacy-obligations-light-proposed)
[privacy-obligations-light-proposed](https://www.ftc.gov/news-events/press-releases/2014/04/ftc-notifies-facebook-whatsapp-privacy-obligations-light-proposed).

1 clear that, regardless of the acquisition, WhatsApp must continue to honor these promises to
2 consumers. Further, if the acquisition is completed and WhatsApp fails to honor these
3 promises, both companies could be in violation of Section 5 of the Federal Trade Commission
4 (FTC) Act and, potentially, the FTC’s order against Facebook,” the letter states.¹⁴

5 262. The FTC specifically noted that the Consent Decree applies equally to “Facebook
6 and its subsidiaries” and instructed that “[b]efore changing WhatsApp’s privacy practices in
7 connection with, or following, any acquisition, you must take steps to ensure that you are not in
8 violation of the law or the FTC’s order. First, if you choose to use data collected by WhatsApp
9 in a manner that is materially inconsistent with the promises WhatsApp made at the time of
10 collection, you must obtain consumers’ affirmative consent before doing so. Second, you must
11 not misrepresent in any manner the extent to which you maintain, or plan to maintain, the
12 privacy or security of WhatsApp user data.... Finally, if you choose to change how you collect,
13 use, and share newly collected WhatsApp data, we recommend that you offer consumers an
14 opportunity to opt out of such changes[.]”

15 263. On April 10, 2014, the FTC noted in a letter to Facebook and WhatsApp’s
16 general counsel, “Following the announcement of the proposed acquisition of WhatsApp,
17 Facebook chief executive Mark Zuckerberg was quoted as saying ‘We are absolutely not going
18 to change plans around WhatsApp and the way it uses user data.’ Similarly, a Facebook
19 spokesperson stated that ‘As we have said repeatedly, WhatsApp will operate as a separate
20 company and will honor its commitments to privacy and security.’” The FTC concluded that
21 Facebook had “promised consumers that it would not change the way WhatsApp uses customer
22 information” and specifically advised that “any use of WhatsApp’s subscriber information that
23 violates these privacy promises, by either WhatsApp or Facebook, could constitute a deceptive
24 or unfair practice under the FTC Act” and “could violate the FTC’s order against Facebook.”

25
26
27 ¹⁴ See Fed. Trade Comm’n Press Release, FTC Notifies Facebook, WhatsApp of Privacy
28 Obligations in Light of Proposed Acquisition, Apr. 10, 2014, *available at*
<https://www.ftc.gov/news-events/press-releases/2014/04/ftc-notifies-facebook-whatsapp-privacy-obligations-light-proposed>.

1 264. On March 12, 2018, WhatsApp attorneys signed an “undertaking” with the
2 Information Commissioner responsible for enforcement of the Irish Data Protection Act
3 (“DPA”), acknowledging that WhatsApp’s “shar[ing] any personal data with the Facebook
4 family of companies” would be a violation of the DPA because WhatsApp had: (i) “not
5 identif[ied] a lawful basis of processing for any such sharing of personal data”; (ii) “fail[e]d to
6 provide adequate fair processing information to users in relation to any such sharing of
7 personal data”; and (iii) [i]n relation to existing users, such sharing ... involved the processing
8 of personal data for a purpose that is incompatible with the purpose for which such data were
9 obtained.” WhatsApp “commit[ed]” not to engage in these practices only with respect to users
10 in the European Union, and WhatsApp and Facebook continue to share the personal data of
11 U.S. users with each other and with other third party companies.

12 265. The acquisition of WhatsApp was made on the foundation of “no ads, no games,
13 and no gimmicks.” However, defendant Zuckerberg broke his promise and reportedly
14 pressured WhatsApp’s founders to change its business model in order to generate more
15 advertising revenue. When defendant Koum complained that he “didn’t have enough people”
16 to implement the project, Zuckerberg dismissed him with, “I have all the people you need,”
17 according to one person familiar with the conversation.

18 266. WhatsApp co-founder Brian Acton (“Acton”) left Facebook in November of
19 2017 according to *The New York Times*. Acton later became the executive chairman of the
20 Signal Foundation, the nonprofit that has run the encrypted communication app Signal, and he
21 personally invested \$50 million into the project that focus on the development of privacy-
22 focused apps.

23 267. On April 30, 2018, defendant Koum publicly announced his departure from
24 WhatsApp and resignation from Facebook’s board of directors. “Koum’s exit is highly unusual
25 at Facebook,” *The Washington Post* reported. “The inner circle of management, as well as the
26 board of directors, has be fiercely loyal during the scandals that have rocked media giant. In
27 addition, Koum is the sole founder of a company acquitted by Facebook to serve on its board.
28 Only two other Facebook executives, Zuckerberg and Chief Operating Officer Sheryl

1 Sandberg, are members of the board.”

2 268. Defendant Koum did not give any reasons for his exit. Nevertheless, he
3 explained that he deeply cared about the privacy of communication in 2014 when he sold
4 WhatsApp to Facebook, stating in a blog post, “respect for your privacy is coded into our
5 DNA, and we built WhatsApp around the goal of knowing as little about you as possible... If
6 partnering with Facebook meant that we had to change our values, we wouldn’t have done it.”

7 269. The split between Facebook and WhatsApp is considered as messy and
8 expensive, according to *The Wall Street Journal*. “Behind the dishiness, however, is a very
9 important story that pretty much clears up any doubt as to whether Mark Zuckerberg is a
10 trustworthy man who keeps his promises – ***or a profit-obsessed machine who’s much stronger***
11 ***on greed than he is on morals.***” While Zuckerberg told stock analysts that he and Koum
12 agreed that advertising wasn’t the right way to make money from messaging apps,” it was
13 Zuckerberg’s decision alone, but he broke his promise.

14 270. According to *The Washington Post*, which spoke to “people familiar with internal
15 discussions” over Koum’s departure, there were tensions with Facebook over WhatsApp’s end-
16 to-end encryption, which ensures that messages can’t be intercepted and read by anyone
17 outside of the conversation, including by WhatsApp or Facebook. Koum and other WhatsApp
18 executives believed that Facebook’s desire to make it easier for businesses to use its tools
19 would require weakening some of the encryption.

20 271. Brian Acton (“Acton”), who co-founded WhatsApp with Koum in 2009, left
21 Facebook last November, according to the *New York Times*. Acton later became the executive
22 chairman of the Signal Foundation, the nonprofit that has run the encrypted communication app
23 Signal, and he personally invested \$50 million into the project that focus on the development of
24 privacy-focused apps. On March 20, 2018, Acton wrote on twitter five days after the
25 Cambridge Analytica scandal, “It is time. #deletefacebook” to support the chorus of the
26 #deletefacebook movement, *Techcrunch* reported.

27 Both Acton and defendant Koum are purportedly big believers in
28 privacy, and that’s the reason why WhatsApp insisted no ads and
operated independently even though Facebook scrapped the 99-cent

1 annual charge to prevent WhatsApp from generating revenue,
2 according to the *Washington Post*.

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

6 272. On May 18, 2017, the European Commission announced in a press release that it
7 had fined Facebook €110 million “for providing incorrect or misleading information during the
8 Commission’s 2014 investigation under the EU Merger Regulation of Facebook’s acquisition
9 of WhatsApp.” The press release explained:

10
11 When Facebook notified the acquisition of WhatsApp in 2014, it
12 informed the Commission that it would be unable to establish
13 reliable automated matching between Facebook users’ accounts and
14 WhatsApp users’ accounts. It stated this both in the notification
15 form and in a reply to a request of information from the
16 Commission. However, in August 2016, WhatsApp announced
17 updates to its terms of service and privacy policy, *including the*
18 *possibility of linking WhatsApp users’ phone numbers with*
19 *Facebook users’ identities*.

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

28 274. In its reply to the Commission’s Statement of Objections, Facebook
acknowledged its infringement of the rules.

D. THE FTC IS INVESTIGATING POSSIBLE CONSENT DECREE VIOLATIONS

275. Facebook is also facing an investigation by the FTC relating to the Company’s
compliance with the 2011 Consent Decree, after the FTC found that the company had told

1 users that third-party apps on the social media site, like games, would not be allowed to access
2 their data. The FTC found that the apps, by contrast, were able to obtain almost all personal
3 information about a user.

4 276. On March 20, 2018, former FTC Commissioner Terrell McSweeney issued the
5 following statement regarding recent news reports of allegedly unauthorized use of Facebook
6 user information by a data analytics firm: “*The FTC takes the allegations that the data of*
7 *millions of people were used without proper authorization very seriously*. The allegations also
8 highlight the limited rights Americans have to their data. Consumers need stronger protections
9 for the digital age such as comprehensive data security and privacy laws, transparency and
10 accountability for data brokers, and rights to and control over their data.”

11 277. A Facebook representative also said at that time that the Company expected to
12 receive questions from the FTC related to potential violations of the 2011 Consent Decree.
13 “We remain strongly committed to protecting people’s information,” Facebook’s deputy chief
14 privacy officer, Rob Sherman, said in a statement. “We appreciate the opportunity to answer
15 questions the FTC may have.”

16 278. Just a few days later, the FTC announced it was investigating Facebook for
17 violations of the 2011 Consent Decree. On March 26, 2018, Tom Pahl, Acting Director of the
18 Federal Trade Commission’s Bureau of Consumer Protection, issued the following statement
19 regarding reported concerns about Facebook’s privacy practices:

20
21 The FTC is firmly and fully committed to using all of its tools to protect the privacy
22 of consumers. Foremost among these tools is enforcement action against companies
23 that fail to honor their privacy promises, including to comply with Privacy Shield,
24 or that engage in unfair acts that cause substantial injury to consumers in violation
25 of the FTC Act. Companies who have settled previous FTC actions must also
26 comply with FTC order provisions imposing privacy and data security
27 requirements. Accordingly, the FTC takes very seriously recent press reports
28 raising substantial concerns about the privacy practices of Facebook. Today, the
FTC is confirming that it has an open non-public investigation into these practices.

29 279. In an April 4, 2018 *Washington Post* article, David Vladeck, who was the
30 Director of the FTC’s Bureau of Consumer Protection when the Consent Decree issued, stated
31 that Facebook is “likely grossly out of compliance with the FTC consent decree,” adding, “I

1 don't think that after these revelations they have any defense at all." In an April 8, 2018
2 article, Vladeck, was reported as saying that Facebook may face fines of \$1 billion or more for
3 failing to comply with the Consent Decree, and that "[t]he agency will want to send a signal ...
4 that the agency takes its consent decrees seriously."

5 280. On April 19, 2018, Senator Blumenthal sent a letter to Acting Chairman of the
6 FTC Maureen Ohlhausen, stating that he was "pleased" the FTC had opened an investigation of
7 Facebook and identifying "evidence that Facebook may have violated its consent decree." He
8 also "encourage[d] the FTC to pursue strong legal remedies ... and [to] set enforceable rules on
9 [Facebook's] future conduct." Blumenthal's letter attaches evidence of the certifications
10 Facebook obtained from Cambridge Analytica and GSR, which confirm that the Company did
11 not even sign the "settlement agreement" concerning the data sharing, suggesting that it is
12 possibly not even enforceable.¹⁵

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

23 282. The Commissioner noted in his memorandum that "[w]hile these aggressive
24 remedies are typically applied [only] in fraud cases, [the FTC] should not hesitate to apply
25 them against repeat offender corporations and their executives[,] [r]egardless of their size and
26 clout[.]"

27
28 ¹⁵ Senator Blumenthal's letter dated April 19, 2018 is attached hereto as **Exhibit 7**.

1 283. On June 4, 2018, Senators Markey and Blumenthal sent a letter to the FTC and
 2 noted that Facebook may have violated the FTC Consent Decree. “*The American people*
 3 *deserve to fully understand* with whom and under what conditions Facebook provides access
 4 to user data[.]” they stated. Also on June 4, 2018, Cicilline and New York Attorney General
 5 Barbara Underwood sent a letter to defendant Zuckerberg that raises the issue of whether
 6 Facebook’s data-sharing practices violate the Consent Decree.

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

13 285. PwC’s reports to the FTC indicate that the Company’s Privacy Program
 14 encompasses these “service providers.” The Initial Assessment Report states, in relevant part:

15
 16 **Service Providers:** Facebook has implemented controls with respect to third-party
 17 service providers, including implementing policies to select and retain service
 18 providers capable of appropriately protecting the privacy of covered information
 19 received from Facebook. Facebook’s Security team has a process for conducting
 20 due diligence on service providers who may receive covered information in order
 21 to evaluate whether their data security standards are aligned with Facebook’s
 22 commitments to protect covered information.

23
 24 As part of the due diligence process, Facebook asks prospective service providers
 25 to complete a security architecture questionnaire or vendor security questionnaire
 26 to assess whether the provider meets Facebook’s functional security requirements
 27 to protect the privacy of user data. Based upon the service provider’s response to
 28 the vendor security questionnaire and other data points, Facebook’s Security team
 determines whether further security auditing is required.

Facebook partners with an outside security consulting firm to conduct security
 audits, which may include testing of the service provider’s controls, a vulnerability
 scanning program, a web application penetration test, and/or a code review for
 security defects. Facebook also has a contract policy which governs the review,
 approval, and execution of contracts for Facebook.

286. Accordingly, after it was revealed that Facebook has data sharing agreements

1 with companies like Apple and Huawei, Facebook representatives attempted to distinguish
 2 those agreements from the developer policies that allowed third party apps to obtain Facebook
 3 information and user data. According to *The New York Times*, Facebook officials called the
 4 Company’s partnerships with device manufacturers “private data channels” and said they did
 5 not violate the Consent Decree because “the company viewed its hardware partners as ‘service
 6 providers,’ akin to a cloud computing service paid to store Facebook data or a company
 7 contracted to process credit card transactions.”

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

10 **E. ZUCKERBERG’S TESTIMONY AT THE U.S. CONGRESSIONAL HEARINGS IN**
 11 **APRIL 2018 WAS EVASIVE AND MISLEADING**

12 288. On April 10 and 11, 2018, defendant Zuckerberg testified before Congress.

13 289. In his testimony before both the Senate and House committees, Zuckerberg
 14 claimed ignorance about the Company he created and has controlled for 14 years. Zuckerberg
 15 wasn’t dodging questions about obscure corners of the Company or corporate minutiae, but the
 16 most plainly fundamental aspects of Facebook’s business and privacy policies.

17 290. For example, when asked about the role of Palantir, a data-mining defense
 18 contractor co-founded by Facebook Board member and early Zuckerberg ally defendant Thiel,
 19 defendant Zuckerberg responded, “I’m not really that familiar with what Palantir does.”

20 291. Defendant Zuckerberg acted similarly confused when asked whether Facebook
 21 does things it openly says it does on its own website. When Senator Roger Wicker asked
 22 Zuckerberg if he could confirm whether “Facebook can track a user’s internet browsing
 23 activity, even after that user has logged off of the Facebook platform,” he replied, “Senator — I
 24 — I want to make sure I get this accurate, so it would probably be better to have my team
 25 follow up afterwards.” The answer is unequivocally yes, according to Facebook.com, which
 26 stated: “*If you’re logged out* or don’t have a Facebook account and visit a website with the
 27 Like button or another social plug-in, *your browser sends us a more limited set of info.*”

28 292. When Senator Roy Blunt asked whether Facebook tracks users across devices

1 (e.g., from their iPhone to their iPad), Zuckerberg replied that he was “not sure of the answer to
2 that question.” Meanwhile, Facebook.com prominently displays a diagram and instructions
3 about how to “Advertise to real people *cross-device*.” In his follow up responses in June,
4 Zuckerberg admitted that “we associate information across different devices” and that
5 “Facebook’s services *inherently operate* on a cross-device basis.”

6 293. On the second day of testimony, Representative Ben Lujan of New Mexico noted
7 that “Facebook recently announced that — a search feature allowing malicious actors to scrape
8 data on virtually all of Facebook’s 2 billion users” had previously been raised to Facebook in
9 2013, and again in 2015, and asked Zuckerberg, “Yes or no: This issue of scraping data was
10 again raised in 2015 by a cyber security researcher, correct?” Zuckerberg responded,
11 “Congressman, I’m not specifically familiar with that. The feature that we identified — I think
12 it was a few weeks ago, or a couple weeks ago, at this point — was a search feature that
13 allowed people to look up some information that people had publicly shared on their profiles....
14 So names, profile pictures, public information.”

15 294. Representative Lujan pressed Zuckerberg for an answer, stating: “I will recognize
16 that Facebook did turn this feature off. My question, and the reason I’m asking about 2013 and
17 2015, is Facebook knew about this in 2013 and 2015, but you didn’t turn the feature off until
18 Wednesday of last week — the same feature that Mr. Kinzinger just talked about, where this is
19 essentially a tool for these malicious actors to go and steal someone’s identity and put the
20 finishing touches on it. So, again, you know, one of your mentors, Roger McNamee, recently
21 said *your business is based on trust, and you are losing trust*. This is a trust question. Why
22 did it take so long, especially when we’re talking about some of the other pieces that we need
23 to get to the bottom of? Your failure to act on this issue has made billions of people potentially
24 vulnerable to identity theft and other types of harmful, malicious actors.”

25 295. Defendant Zuckerberg said he believed it was due to the fact that there are more
26 than 100 million Facebook “like” buttons around the internet, but did not provide any
27 explanation as to why Facebook did not turn the feature off until after a catastrophic breach two
28 years after the data scraping issue had been reported for a second time.

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

8 297. While defendant Zuckerberg eventually admitted to the data collection of non-
9 Facebook users, he stated it was “to prevent the kind of scraping” described by Representative
10 Lujan, and claimed that he was not familiar with the “shadow profiles” that organize the data of
11 non-Facebook users. Yet, Facebook’s developer website specifically mentions “shadow
12 profiles” that were permitted by the Company’s policies.

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

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

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

24 ***You didn’t know about major court cases regarding your privacy policies***
25 ***against your company. You didn’t know that the FTC doesn’t have fining***
26 ***authority and that Facebook could not have received fines for the 2011***
27 ***consent order.*** You didn’t know what a shadow profile was. You didn’t
28 know how many apps you need to audit. You did not know how many other
 firms have been sold data by Dr. Kogan other than Cambridge Analytica
 and Eunoia Technologies, even though you were asked that question
 yesterday. And yes, we were all paying attention yesterday. ***You don’t even***

1 *know all the kinds of information Facebook is collecting from its own*
 2 *users.*

3 Here's what I do know. You have trackers all over the Web. On practically
 4 every website you go to, we all see the Facebook Like or Facebook Share
 5 buttons. And with the Facebook pixel, people browsing the Internet may not
 6 even see that Facebook logo. It doesn't matter whether you have a Facebook
 7 account. Through those tools, Facebook is able to collect information from
 8 all of us. So I want to ask you, how many Facebook like buttons are there
 9 on non-Facebook Web pages?

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

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

19 303. During the House committee hearing on April 11, 2018, Representative David
 20 McKinley ("McKinley") noted that online pharmacies are using Facebook's website to sell
 21 drugs illegally, telling defendant Zuckerberg, "Your [Facebook's] platform *is still being used*
 22 *to circumvent the law*, and allow people to buy highly addictive drugs without a
 23 prescription[.]" Representative McKinley noted that it happens all the time, and pointed out
 24 that Zuckerberg isn't fulfilling the promise he made to remove ads for illegal online pharmacies
 25 from Facebook's website, telling Zuckerberg, "you didn't do it." "Opioids are still available on
 26 your site ... without a prescription on your site." McKinley added, "*Facebook is actually*
 27 *enabling an illegal activity, and in so doing, you are hurting people.*"¹⁶

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

¹⁶ Plaintiffs expressly incorporate by reference as though fully set forth herein the transcripts of the Congressional hearings held on April 10, 2018 and April 11, 2018, including Zuckerberg's testimony to both the House and Senate committees concerning Facebook's user privacy.

1 304. On April 26, 2018, Facebook’s Chief Technology Officer Mike Schroepfer
 2 (“Schroepfer”) appeared before the European Parliamentary Committee to explain Facebook’s
 3 response to a sequence of data, privacy, and fake news scandals, according to *Business Insider*.
 4 During the meeting, Schroepfer admitted that it was a mistake to not alert users when
 5 Defendants initially learned that Facebook’s data had been sold to Cambridge Analytica in
 6 2015, and Schroepfer apologized for the breach of users’ trust. Schroepfer also stated that
 7 Facebook “not never, but rarely” read the terms and conditions of the app that improperly
 8 shared user data with Cambridge Analytica, *BBC News* reported.

9 305. The Parliamentary committee criticized Facebook practices regarding political
 10 advertising. Damian Collins (“Collins”), the chair of the Department of Culture, Media, and
 11 Sport Committee accused Facebook of having tools on its platform that work for the advertiser
 12 more than they work for the consumer. Schroepfer responded, “we were slow to understand
 13 the impact of this at the time,” and promised to make political advertising far more transparent
 14 in the future yet admitted that there was currently no way for people to opt out of it entirely,
 15 reported *BBC News*.

16 306. The Conservative MP Julian Knight described Facebook as a “*morality free*
 17 *zone*.”; while Paul Farrelly, the MP from the Labour Party quoted journalist Matt Taibbi in
 18 describing Facebook as “*a great vampire squid wrapped around the face of humanity,*
 19 *relentlessly jamming its blood funnel into anything that smells like money*,” reported the
 20 *Register*.

21 307. Schroepfer’s appearance before the parliamentary committee left dozens of
 22 questions unanswered, and “the evidence presented by Schroepfer lacked many of the
 23 important details that we need,” committee chair Damian Collins said. The MP committee
 24 once again urged defendant Zuckerberg to appear and testify before the committee, but he
 25 refused a second time.

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

28 308. When he finally appeared before the committee on May 22, 2018, European
 Parliament officials laid into Zuckerberg for Facebook’s data privacy failings and raised the

1 prospect of breaking up the social network, which some suggested had amassed an unfair share
2 of power online.

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

7 310. The questions included what steps Facebook is taking to avoid future data "leaks"
8 and to combat so-called fake news, whether the company will allow users to truly opt-out of
9 targeted advertising, and whether the Company has an anticompetitive stranglehold on the
10 social media market. Other questions included what data Facebook collects on non-Facebook
11 users; whether the company can promise that personal data collected for "security purposes"
12 won't be used for targeted advertising; and whether the company would consider showing the
13 public how its algorithms work.

14 311. Many of the EU officials, including Parliament member Guy Verhofstadt,
15 appeared skeptical of the Zuckerberg's promises to do better. "You have to ask yourself how
16 you will be remembered, as one of the three internet giants, along with Steve Jobs and Bill
17 Gates, who have enriched our world and our society, or on the other hand, *as the genius who*
18 *created a digital monster that is destroying our democracy and our society?"* said
19 Verhofstadt, a former prime minister of Belgium.

20 312. Under new EU General Data Protection Regulation ("GDPR"), which went into
21 effect in May of 2018, Facebook and other technology companies could be fined up to 4% of
22 their global revenue for privacy breaches. For Facebook, this could mean a fine of more than
23 \$1.5 billion.

24 313. On June 30, 2018, Facebook provided the House Energy and Commerce
25 Committee with 747 pages of written responses to the questions that defendant Zuckerberg had
26 been asked by the committee during the hearing on April 11, 2018, but claimed he did not
27 know the answers. Notably, of just six questions that the committee members had asked
28 defendant Zuckerberg to answer concerning Facebook's Board, not one was directly answered

1 in the Facebook responses:

2 314. The Honorable Anna G. Eshoo:

3 **Isn't Facebook's Board complicit after years of transgressions and apologies by**
4 **management?**

5
6 Facebook: We recognize that we have made mistakes, and we are committed to
7 learning from this experience to secure our platform further and make our
community safer for everyone going forward.

8 As our CEO Mark Zuckerberg has said, when you are building something
9 unprecedented like Facebook, there are going to be mistakes. What people
10 should hold us accountable for is learning from the mistakes and continually
doing better—and, at the end of the day, making sure that we're building things
that people like and that make their lives better.

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

13
14 We've heard loud and clear that privacy settings and other important tools are
15 too hard to find and that we must do more to keep people informed. So, we're
taking additional steps to put people more in control of their privacy. For
16 instance, we redesigned our entire settings menu on mobile devices from top to
bottom to make things easier to find.

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

20
21 We explain the services we offer in language that's easier to read. We've also
updated our Data Policy to better spell out what data we collect and how we use
22 it in Facebook, Instagram, Messenger, and other products.”

23 315. The Honorable Anna G. Eshoo:

24 **Does your board want you to resign?** Not addressing security is amateur behavior?

25
26 Facebook: We recognize that we have made mistakes, and we are committed to
learning from this experience to secure our platform further and make our
27 community safer for everyone going forward.

28 As our CEO Mark Zuckerberg has said, when you are building something
unprecedented like Facebook, there are going to be mistakes. What people should

1 hold us accountable for is learning from the mistakes and continually doing better—
2 and, at the end of the day, making sure that we’re building things that people like
and that make their lives better.

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

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

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

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

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

20
21 We use a variety of tools to enforce Facebook policies against violating parties,
22 including developers. We review tens of thousands of apps per year and regularly
disapprove noncompliant apps as part of our proactive review process.

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

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

28 We have invested significant resources in these efforts. Facebook is presently
investigating apps that had access to large amounts of information before we

1 changed our platform policies in 2014 to significantly reduce the data apps could
2 access.

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

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

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

14 317. On March 31, 2015, a team of researchers tapped by Belgium’s data protection
15 regulator to probe Facebook’s privacy policy changes released an updated report accusing the
16 company of violating European Union privacy law by tracking the activities of nonusers.
17 According to version 1.2 of the report prepared by the Interdisciplinary Center for Law and
18 ICT at the University of Leuven in Belgium, which was first released in February 2015,
19 Facebook violated the EU’s 2002 e-privacy directive by carrying out tracking practices that are
20 even more expansive than the researchers had initially discovered.

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

28 319. The updated report added the discovery that Facebook also tracks nonusers in a
way that the researchers allege violates the laws’ notice and consent requirements. “Facebook
places cookies whenever someone visits a webpage belonging to the facebook.com domain,

1 even if the visitor is not a Facebook user,” the report said. “This means that Facebook tracks its
2 users across websites even if they do not make use of social plug-ins, and even if they are not
3 logged in, and Facebook tracking is not limited to Facebook users.”

4 320. Facebook’s Chief Technology Officer, Mike Schroepfer, admitted in a May 30,
5 2018 interview with Recode that the Company obtains information about non-users via cookies
6 and that this data cannot be recaptured or deleted, stating, “in many cases you have cookie data
7 from a device or from a browser, but I don’t know which person this is associated with, and so
8 *it’s pretty hard to get that data back for an individual.*”

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

17 322. The report concludes that Facebook’s practice violates the EU’s e-privacy
18 directive by taking users’ silence to mean that they want to be tracked across third-party
19 websites for ad targeting purposes, and by failing to inform nonusers that their information may
20 be gathered when they interact with a Facebook plug-in on a third-party site. While Facebook
21 has claimed that the cookies it sets on nonusers’ browsers are for security purposes, which are
22 generally allowed under an exemption to the e-privacy directive, the report noted that the
23 exemption does not cover the use of cookies for the security of websites or services that have
24 not been explicitly requested by the user. “As a result, Facebook’s tracking of nonusers, even
25 if the data is not used for ad targeting or other purposes, violates ... the e-privacy directive,”
26 the report concluded.

27
28

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

3 323. On March 12, 2018, WhatsApp attorneys signed an “undertaking” with the
 4 Information Commissioner responsible for enforcement of the Irish Data Protection Act
 5 (“DPA”), acknowledging that WhatsApp’s “shar[ing] any personal data with the Facebook
 6 family of companies” would be a violation of the DPA because WhatsApp had: (i) “not
 7 identif[ied] a lawful basis of processing for any such sharing of personal data”; (ii) “fail[e]d to
 8 provide adequate fair processing information to users in relation to any such sharing of
 9 personal data”; and (iii) [i]n relation to existing users, such sharing ... involved the processing
 10 of personal data for a purpose that is incompatible with the purpose for which such data were
 11 obtained.” WhatsApp “commit[ed]” not to engage in these practices only with respect to users
 12 in the European Union, and WhatsApp and Facebook continue to share the personal data of
 13 U.S. users with each other and with other third party companies.

14 324. On May 18, 2017, the European Commission announced in a press release that it
 15 had fined Facebook €110 million “for providing incorrect or misleading information during the
 16 Commission’s 2014 investigation under the EU Merger Regulation of Facebook’s acquisition
 17 of WhatsApp.” The press release explained:

18
 19 When Facebook notified the acquisition of WhatsApp in 2014, it
 20 informed the Commission that it would be unable to establish
 21 reliable automated matching between Facebook users’ accounts and
 22 WhatsApp users’ accounts. It stated this both in the notification
 23 form and in a reply to a request of information from the
 24 Commission. However, in August 2016, WhatsApp announced
 25 updates to its terms of service and privacy policy, *including the*
 26 *possibility of linking WhatsApp users’ phone numbers with*
 27 *Facebook users’ identities.*

28 325. The Commission found that, “*contrary to Facebook’s statements in the 2014*
 29 *merger review process*, the technical possibility of automatically matching Facebook and
 30 WhatsApp users’ identities already existed in 2014, *and that Facebook staff were aware of*
 31 *such a possibility.*” The Commission said the decision was “based on a number of elements
 32 going beyond automated user matching” and was “unrelated to either ongoing national antitrust

1 procedures or privacy, data protection or consumer protection issues,” but noted that those
2 issues “may arise following the August 2016 update of WhatsApp terms of service and privacy
3 policy.”

4 326. In its reply to the Commission’s Statement of Objections, Facebook
5 acknowledged its infringement of the rules.

6 **2. The German Supreme Court Declared Facebook’s “Friend Finder” 7 Feature Unlawful in 2016**

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

12 328. Facebook’s users did not provide the same information to Facebook that was
13 ultimately used for targeting advertisements – while it was developed with user data, this data
14 was aggregated and ultimately new information was generated through Facebook’s algorithm
15 that was used for targeting purposes. Because this was not the same information that Facebook
16 users had provided, they did not (and could not) know the information existed, let alone was
17 being shared or used for any purpose. Facebook’s users did not, because they could not,
18 consent to such information being shared with third parties or used for targeted advertising.
19 Thus, Facebook’s users did not implicitly or explicitly consent to Facebook’s practices.

20 **3. The Spanish Agency for Data Protection Fined Facebook €1.2 Million 21 Euros in 2017**

22 329. On September 11, 2017, the Spanish Agency for Data Protection (“AEPD”)
23 announced that it had fined Facebook €1.2 million euros for violating data protection
24 regulations following its investigation to determine whether the data processing carried out by
25 the Company complied with the data protection regulations. The AEPD stated that its
26 investigation made it possible to verify that Facebook does not inform the users in a
27 comprehensive and clear way about the data that it will collect and the treatments that it will
28 carry out with them, but that it is limited to giving some examples. In particular, the AEPD
found that Facebook collects other data derived from the interaction carried out by users on the

1 platform and on third-party sites without them being able to clearly perceive the information
2 that Facebook collects about them or with what purpose they are going to use it.

3 330. The AEPD also found that the privacy policy of Facebook contains generic and
4 unclear expressions, and requires access to a multitude of different links to know it. Further,
5 the AEPD concluded that the Company makes an inaccurate reference to the use it will make of
6 the data it collects, so that a Facebook user with an average knowledge of the new technologies
7 does not become aware of the data collection or storage and subsequent treatment, or what they
8 will be used for.

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

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

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

19 332. On February 12, 2018, a German court found that Facebook’s failure to obtain
20 users’ informed consent before collecting their data was illegal. The Berlin Regional Court
21 found that Facebook flouted Germany’s data protection law by turning data sharing settings on
22 by default. One preactivated setting on Facebook’s smartphone app shared users’ locations to
23 the people they are chatting with, the court said. The Company also preticked a box
24 authorizing search engines to show links to user profiles in search results, making it easier for
25 anyone to find someone’s personal profile, the ruling said.

26 333. The court found that eight clauses in Facebook’s terms of service were invalid,
27 including a declaration that users consented to the company using their names and profile
28 pictures “for commercial, sponsored or related content” or sending their data to the United
States.

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

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

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

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

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

24 337. The Exchange Act requires publicly traded companies to disclose to shareholders
 25 “material information,” the kind of information that an investor would want to know to protect
 26 their investment. The SEC issued guidance on public reporting of cybersecurity incidents,
 27 noting that the commission “encourages companies to continue to use Form 8-K or Form 6-K
 28

1 to disclose material information promptly, including disclosure pertaining to cybersecurity
2 matters.”

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

6 **A. THE BOARD ISSUED THE MATERIALLY MISLEADING PROXY STATEMENTS IN**
7 **RECOMMENDING A VOTE AGAINST SHAREHOLDER PROPOSALS ON THE**
8 **BASIS OF THE DIRECTORS’ MISSTATEMENTS ABOUT FACEBOOK’S PRIVACY**
9 **PRACTICES AND BOARD OVERSIGHT**

10 339. Facebook’s Board, including all of the Defendants, caused Facebook to issue and
11 file with the SEC materially misleading Proxy Statements soliciting their vote against various
12 matters proposed by shareholders.

13 340. In soliciting a no vote, the Proxy Statements contained misrepresentations
14 concerning the Board’s role in risk oversight. For example, on page 16 of the 2018 Proxy
15 Statement, Defendants stated:

16 **“Board Role in Risk Oversight”**

17 Our board of directors as a whole has responsibility for overseeing our risk
18 management and believes that a thorough and strategic approach to risk
19 oversight is critical. The board of directors exercises this oversight
20 responsibility directly and through its committees. The oversight
21 responsibility of the board of directors and its committees is informed by
22 regular reports from our management team, including senior personnel that
23 lead a variety of functions across the business, and from our internal audit
24 department, as well as input from external advisors, as appropriate. These
25 reports are designed to provide timely visibility to the board of directors and
26 its committees about the identification and assessment of key risks, our risk
27 mitigation strategies, and ongoing developments.

28 The full board of directors has primary responsibility for evaluating
strategic and operational risk management, and for CEO succession
planning. Our audit committee has the responsibility for overseeing our
major financial, legal, and regulatory risk exposures, which span a variety
of areas including litigation, regulatory compliance, reputational and policy
matters, platform integrity efforts, financial reporting, cybersecurity, and
international operations. Our audit committee also oversees the steps our
management has taken to monitor and control these exposures, including
policies and procedures for assessing and managing risk and related
compliance efforts. Finally, our audit committee oversees our internal audit
function. Our compensation & governance committee evaluates risks

1 arising from our corporate governance and compensation policies and
2 practices, as more fully described in “Executive Compensation—
3 Compensation Discussion and Analysis—Compensation Risk
4 Assessment.” The audit committee and the compensation & governance
5 committee provide reports to the full board of directors regarding these and
6 other matters.

7 341. The Proxy Statements misled shareholders to vote against “Stockholder
8 Proposals” meant to improve the Board’s governance, failing to disclose negative, true facts
9 about the Defendants’ performance described above.

10 **B. THE BOARD ISSUED THE MATERIALLY MISLEADING PROXY STATEMENT IN**
11 **SOLICITING THE DIRECTORS’ RE-ELECTION TO FACEBOOK’S BOARD AND**
12 **COMPENSATION PACKAGES**

13 342. Defendants also violated Section 14(a) of the Exchange Act and SEC Rule 14a-9
14 by causing Facebook to issue Proxy Statements soliciting their re-election to the Board, failing
15 to disclose the Cambridge Analytica incident and deliberately concealing Facebook’s
16 advertising practices and corporate policies that which allowed and perpetuated Facebook’s
17 violations of user privacy and other laws. Defendants’ failure to disclose those material facts
18 likewise constitutes a breach of their fiduciary duties.

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

24 344. The Proxy Statements omitted any disclosures regarding (i) the Cambridge
25 Analytica leak; (ii) Defendants’ knowledge that Facebook’s internal controls and systems were
26 inadequate and ineffective to protect user information; (iii) Defendants’ knowledge of data
27 security failures that had actually materialized and had not been disclosed; (iv) the fact that
28 Facebook’s internal controls and systems were inadequate to ensure that the Company
29 complied with applicable notification and disclosure requirements concerning the Cambridge
30 Analytica leak; (v) the fact that Defendants failed to maintain appropriate policies and
31 procedures to detect and prevent data security leaks and to protect user information; and (vi)

1 the fact that Defendants failed to appropriately address Facebook’s privacy practices and
2 misleading claims regarding same as required by the FTC Consent Decree; and (vii) as a result,
3 Facebook may be in violation of the Consent Decree.

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

8 346. The statements in the Proxy Statements conveyed that the Company’s corporate
9 governance structure was “effective” and provided “oversight of management and Board
10 accountability.” In reality, Facebook’s corporate government structure allowed senior
11 executives and the Board to sidestep real accountability and instead continue perpetuating the
12 data security practices that led to the Cambridge Analytica leak, and fail to disclose or notify
13 users of the leak.

14 347. The Proxy Statements, which contained materially misleading statements and
15 thus deprived shareholders of adequate information necessary to make a reasonably informed
16 decision, caused the Company’s stockholders to re-elect all of the Defendants to the Board and
17 approve their compensation while they were breaching their fiduciary duties to Facebook and
18 deliberately concealing material information concerning the Cambridge Analytica leak and its
19 effects on the Company’s business and reputation.

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

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

349. On November 18, 2016, with full knowledge of the exfiltration and unauthorized

1 use of user data and the undisclosed deviation of its policies, as described above, Facebook's
2 Board authorized the Company to repurchase \$6 billion of its own shares of common stock.
3 The share repurchases were the first in Facebook's history since becoming a public company.

4 350. Between 2017 and March 31, 2018, with the Board's authorization and consent,
5 Facebook repurchased billions worth of Facebook stock. According to Facebook's 2017
6 Annual Report, Facebook repurchased approximately 13 million Class A common shares for an
7 aggregate amount of approximately \$2.07 billion in 2017 alone. In conducting these share
8 repurchases, Defendants falsely signaled to the public that they believed Facebook shares were
9 undervalued and that the repurchases were the best use of the Company's cash. The share
10 repurchases also had the effect of growing the Company's earnings per share—as share
11 repurchases lower the number of shares outstanding, on which earnings per share are based—as
12 well as its return on assets, return on equity, and other metrics. Together, these actions helped
13 inflate Facebook's share price.

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

17 352. During the time of the repurchase transactions, Defendants knowingly or
18 recklessly made materially false or misleading statements and/or failed to disclose material
19 information regarding the Company's user privacy practices, including the failure to disclose
20 that Facebook had already experienced the exfiltration and unauthorized use of data impacting
21 millions of Facebook users, that Facebook had intentionally deviated from its own policy
22 supposedly implemented in 2015 to prevent access to user information, and that Facebook had
23 no internal processes in place to control, monitor or retrieve user data that had been sent from
24 Facebook servers. To the contrary, as revealed by Facebook's former platform operations
25 manager responsible for policing data breaches by third-party software developers, Facebook
26 had no such controls and millions of Facebook users had their data harvested by third parties
27 without their knowledge.

28 353. Defendants also made false or misleading statements or omissions relating to its

1 internal controls and risks in Facebook’s SEC filings. For example, Facebook’s 2015, 2016
2 and 2017 Annual Reports signed by Defendants each contain approximately 20 pages of risk
3 disclosures, yet the only reference to the unauthorized use of user information refers to the
4 mere risk of it happening in the future, obfuscating the fact that such unauthorized use had
5 already occurred and on a massive scale impacting tens of millions of Facebook users. The
6 Annual Reports falsely contain certifications that Facebook’s internal controls are effective.
7 Defendants’ SEC filings also falsely represented that Facebook maintained robust privacy
8 policies and risk management system to protect user data, and that the Board and senior
9 executives had overall and ultimate responsibility for the management of risk.

10 354. Defendants’ statements (including those contained in Facebook’s SEC filings
11 described above) were materially false and misleading, and failed to disclose material
12 information, for the reasons stated above, including the fact that Facebook had already
13 experienced the unauthorized access and use of user information, deviated from its own policy
14 to restrict access to user information, and failed to implement and maintain adequate risk
15 controls at the Company.

16 355. In repurchasing shares in connection with the stock repurchase program,
17 Facebook relied on Defendants’ false or misleading statements, either directly or through the
18 “fraud on the market” doctrine.

19 356. Facebook justifiably expected Defendants to disclose material information as
20 required by law and SEC regulations in the Company’s periodic filings with the SEC.
21 Facebook would not have repurchased its securities at artificially inflated prices had
22 Defendants disclosed all material information then known to them, as detailed in this
23 Complaint. Thus, reliance by Facebook should be presumed with respect to Defendants’
24 omissions of material information as established under the Affiliated Ute presumption of
25 reliance.

26 357. Additionally, the “fraud on the market” presumption applies to Defendants’
27 misstatements of material fact or failures to disclose material facts.

28 358. At all relevant times, the market for Facebook’s common stock was efficient, for

1 the following reasons, among others:

- 2 a. Facebook's stock met the requirements for listing, and was listed and actively
3 traded on a highly efficient and automated market;
- 4 b. As a regulated issuer, Facebook filed periodic reports with the SEC and the
5 automated market;
- 6 c. Facebook's common-stock trading volume was substantial on a daily basis;
- 7 d. Facebook regularly communicated with public investors via established market
8 communication mechanisms, including through regular disseminations of press
9 releases on the national circuits of major newswire services and through other
10 wide-ranging public disclosures, such as communications with the financial
11 press and other similar reporting services;
- 12 e. Facebook was followed by numerous securities analysts employed by major
13 brokerage firms, who wrote reports that were distributed to those brokerage
14 firms' sales force and certain customers, and each of those reports was publicly
15 available and entered the public market place; and

16 359. The market price of Facebook's stock reacted rapidly to new information entering
17 the market.

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

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

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

1 363. Neither the safe-harbor provision of the Private Securities Litigation Reform
2 Act of 1995 (“PSLRA”) nor the judicially created “bespeaks caution” doctrine applicable to
3 forward-looking statements under certain circumstances applies to any of the false or
4 misleading statements pleaded in this Complaint. None of the subject statements constituted a
5 forward-looking statement; rather, they were historical statements or statements of
6 purportedly current facts and conditions at the time the statements were made, including
7 statements about Facebook’s present practices, risks and internal controls, among other
8 things.

9 364. Alternatively, to the extent any of the false or misleading statements pleaded in
10 this Complaint could be construed as forward-looking statements, they were not accompanied by
11 any meaningful cautionary language identifying important facts that could cause actual results to
12 differ materially from those in the purportedly forward-looking statements. Further, to the extent
13 the PSLRA’s safe harbor would otherwise apply to any forward-looking statements pleaded in
14 this Complaint, Defendants are liable for those false or misleading statements because at the
15 time each of those statements was made, the speaker(s) knew the statement was false or
16 misleading, or the statement was authorized or approved by an executive officer of Facebook
17 or a Defendant who knew the statement was materially false or misleading when made.

18 365. While this Complaint identifies Defendant signatories or speakers with
19 respect to the false or misleading statements identified above, the group pleading doctrine
20 also applies to render Defendants responsible for statements as to which they are not
21 explicitly identified as the speaker or signatory. Defendants participated in the drafting,
22 preparation, or approval of the various shareholder and investor reports and other
23 communications concerning Facebook identified in this Complaint and were aware of or
24 recklessly disregarded the misstatements contained in those reports and other
25 communications as well as the omissions from them, and were aware of their materially false
26 and misleading nature. Each Defendant, by virtue of his or her position(s) at Facebook, had
27 access to adverse undisclosed information about the Company’s condition and performance
28

1 as alleged in this Complaint, and knew or recklessly disregarded that those adverse facts
2 rendered the subject statements materially false or misleading when made.

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

11 367. The price of Facebook's common stock was artificially inflated as a result of
12 Defendants' materially false and misleading statements and omissions identified above.
13 Defendants engaged in a scheme to deceive the market and a course of conduct that operated as a
14 fraud or deceit on Facebook, which repurchased shares at artificially inflated prices. When
15 Defendants' prior misrepresentations and fraudulent conduct were disclosed and became
16 apparent to the market, the price of Facebook stock fell as the prior artificial inflation
17 dissipated. As a result of its purchases of Facebook shares, the Company suffered damages
18 under the federal securities laws.

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

21 368. During the relevant period, certain of the Defendants took advantage of the
22 artificial inflation of Facebook's shares caused by the Defendants' false or misleading
23 statements and omissions that failed to disclose the Cambridge Analytica incident or the nature
24 and extent to which the Company's internal controls and policies had permitted the breach to
25 occur. Specifically, Defendants Zuckerberg, Sandberg, and Koum (the "Insider Selling
26 Defendants") collectively sold or otherwise disposed of nearly \$1.5 billion worth of their
27 personally-held shares of Facebook stock during that time, all while in the possession of
28 material, non-public information. At the time of these stock transactions in 2018, all of the

1 Insider Selling Defendants knew about or recklessly disregarded material, non-public
2 information regarding the Cambridge Analytica scandal and Facebook’s advertising practices,
3 violations of user privacy and data security laws, and other damages to Facebook caused by
4 Defendants’ actions (or conscious inaction) in connection with the practices described above.

5 369. For example, the IRS summons indicates that Facebook executives testified
6 under oath about their communications and presentations to the Board beginning in at least
7 2009 regarding “advertising operations and revenues[.]”

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

13 371. All of the Defendants knew or recklessly disregarded that these and other
14 relevant facts were necessary to make Defendants’ statements truthful and not misleading, but
15 were not disclosed by Defendants. While these and other material facts were concealed from
16 Facebook shareholders and the public, the Insider Selling Defendants sold or otherwise
17 disposed of Facebook common stock on the basis of that information, thereby breaching their
18 fiduciary duties. In particular,

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

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

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

25 372. The Exchange Act requires publicly traded companies to disclose to shareholders
26 “material information,” the kind of information that an investor would want to know to protect
27 their investment. The SEC issued guidance on public reporting of cybersecurity incidents,
28 noting that the commission “encourages companies to continue to use Form 8-K or Form 6-K

1 to disclose material information promptly, including disclosure pertaining to cybersecurity
2 matters.” In the 2017 and 2018 Proxy Statements, Facebook did not mention the Cambridge
3 Analytica incident, and also did not mention these facts in any of its Form 8-K or Form 6-K
4 filings. Instead, Facebook made general statements in their most recent proxy statement and
5 annual report on Form 10-K about potential, not actual, user privacy and data security risks,
6 and certified that the Company’s internal controls were adequate and complied with applicable
7 laws (which necessarily include the FTC Consent Decree). By trading while in possession of
8 this material, non-public information, the Insider Selling Defendants breached their fiduciary
9 duties.

10 **IX. DAMAGES TO FACEBOOK**

11 373. Defendants’ misconduct has wrought extreme reputational damage upon the
12 Company. This is especially harmful to Facebook because the Company is built on customer
13 trust.

14 374. Defendants breached this trust by acting in direct contravention of the
15 Company’s publicly-touted credo. This reputational harm undoubtedly translates into long-
16 term damage to the Company.

17 375. The illegal practices and Defendants’ gross failures to timely address, remedy, or
18 disclose them also severely damaged Facebook’s reputation within the business community
19 and in the capital markets, as evidenced by, for example, the more than \$50 billion loss in
20 market capitalization after the Cambridge Analytica incident, and Defendants’ knowledge of or
21 conscious disregard of it, were revealed. Further, Facebook’s customers and current and
22 potential investors consider the Company’s ability to protect its users’ personal information,
23 and implement adequate controls to ensure practices that may violate user privacy are timely
24 discovered and properly addressed. This has harmed Facebook, as customers are less likely to
25 use websites that knowingly permit or encourage unscrupulous behavior, and investors are less
26 likely to invest in companies that lack internal controls and fail to timely disclose material
27 information. Thus, Facebook’s ability to attract customers and investors is now impaired.

28 376. Further, as a direct and proximate result of Defendants’ actions, Facebook has

1 expended and will continue to expend significant additional money, including: costs incurred in
2 defending against, and the potential settlement of, civil and criminal legal proceedings brought
3 against the Company related to the unauthorized sharing and use of users' personal
4 information; and costs incurred from the substantial compensation and benefits paid to
5 Defendants, who are responsible for the scheme.

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

13 **X. DEMAND ON FACEBOOK'S BOARD WAS FUTILE AND THUS, EXCUSED**

14 378. Plaintiffs did not make a demand on Facebook's Board of Directors to institute
15 this action against Defendants because, for the reasons detailed above and as set forth further
16 below, any such demand would have been futile.

17 379. The facts detailed in this Complaint demonstrate that the Defendants
18 affirmatively adopted, implemented, and condoned a business strategy based on deliberate and
19 widespread violations of applicable law, which is not a legally protected business decision and
20 can in no way be considered a valid exercise of business judgment, and/or consciously
21 disregarded numerous red flags of misconduct throughout the relevant period, subjecting them
22 to a substantial likelihood of liability as to Plaintiffs' claims against them in this action.
23 Moreover, defendant Zuckerberg dominates and controls the Board, and a majority of the
24 directors are beholden to Zuckerberg and lack independence from him. For all of these
25 reasons, a demand on the Board would have been futile.

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

1 **A. DEMAND IS EXCUSED BECAUSE THE BOARD’S CONDUCT DID NOT**
 2 **CONSTITUTE A VALID EXERCISE OF BUSINESS JUDGMENT**

3 381. Plaintiffs did not make a demand on the Facebook Board prior to instituting this
 4 action because the Board pursued profits at the expense of complying with applicable law,
 5 including the 2011 Consent Decree, and abdicated their duty to the Company and its users to
 6 protect user information. A fiduciary of a Delaware corporation cannot act loyally by causing
 7 the Company to violate the laws of the United States and other countries, thereby exposing the
 8 Company to billions of dollars of liability and regulatory action. These acts, and the other
 9 improper acts set forth in this Complaint which demonstrate a pattern of misconduct, were not
 10 the product of a valid or good faith exercise of business judgment, nor could they have been.

11 382. Defendants’ misconduct at the heart of this case constitutes the direct facilitation
 12 of violations of federal, state, and international laws, including knowingly and consciously
 13 presiding over the Company’s systematic deficiencies and unsound user privacy practices and
 14 concealing . Among other things, the Defendants made, or caused Facebook to make,
 15 materially false or misleading statements and omissions, including in Facebook’s 2017 and
 16 2018 Proxy Statements filed with the SEC.

17 383. Defendants’ blatant and repeated disregard of their responsibility to safeguard the
 18 Company against wrongdoing indicate they knowingly adopted, endorsed, condoned or
 19 promoted illegal business practices, which cannot be considered a legitimate exercise of
 20 business judgment. Demand is therefore excused.

21 **B. DEMAND IS EXCUSED BECAUSE DEFENDANTS FACE A SUBSTANTIAL**
 22 **LIKELIHOOD OF LIABILITY FOR THEIR ROLES IN PERPETUATING FACEBOOK’S**
 23 **ILLEGAL BUSINESS PRACTICES**

24 384. Demand is excused as futile because each of the Defendants faces a substantial
 25 likelihood of liability for the claims alleged against them in this Complaint, given their roles in
 26 perpetuating Facebook’s illegal business practices.

27 385. The Board was well aware of how the Company was monetizing user data. The
 28 Board approved acquisitions that expanded the functionality and reach of the Facebook
 platform and enables it to obtain additional user data. Facebook executives apprised the Board

1 at least quarterly regarding Facebook’s “advertising operations and revenues.” In addition,
 2 certain directors’ affiliated companies, including WhatsApp (defendant Koum) and Netflix
 3 (defendant Hastings) entered into partnerships with Facebook that included the sharing of
 4 Facebook information.

5 386. Defendants also obtained personal financial benefits that were material to
 6 Defendants, and that were not equally shared by other Facebook stockholders, that directly
 7 relate to Facebook’s advertising practices and revenues derived from the illegal business
 8 strategy.

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

11 387. In 2017, Facebook’s Compensation & Governance Committee created a new
 12 “Equity Subcommittee” comprised of defendant Sandberg and Facebook’s Chief Financial
 13 Officer, Wehner, which has the “authority to review and approve grants of RSUs to employees
 14 and consultants” that is traditionally granted to the Board.

15 388. According to the 2018 Proxy Statement, Facebook’s “[e]xecutive compensation
 16 is based on contributions to *number of advertisers*, delivery of a strategic long-range plan,
 17 growth in user engagement, recruiting and developing teams to drive product development in
 18 “new initiatives.” (2018 Proxy Statement at 24) (emphasis added). Accordingly, by creating
 19 the Equity Subcommittee comprised entirely of members of management who determine their
 20 own compensation based on metrics that encourage Facebook’s unlawful business strategy, the
 21 Compensation & Governance Committee members have effectively ceded their oversight
 22 responsibilities to the very members of management who are responsible wrongdoers, while at
 23 the same time rewarding them for achieving performance goals that encourage the same
 24 wrongdoing and advertising practices based on violating user privacy and other laws.

25 389. Accordingly, there is significant doubt that the Defendants are disinterested
 26 because they face a substantial likelihood of liability for their breaches of fiduciary duties,
 27 including their duties of good faith, fair dealing, and loyalty, as well as other violations of law.

28 390. The entire Board had the duty to ensure Facebook’s privacy practices were
 designed to protect user information and disclose any violations of user privacy in accordance

1 with applicable law. Facebook’s internal controls and systems had the ability to detect and
2 report suspicious activity at the developer level, yet failed to prevent violations of user privacy
3 on multiple occasions, in violation of various applicable laws, regulations, and the FTC
4 Consent Decree. The Board’s duty was heightened by the fact that the FTC imposed
5 affirmative obligations with respect to the Company’s user privacy practices in the 2011
6 Consent Decree.

7 391. The Board failed to fulfill that duty, and its failure is even more egregious in light
8 of the many blatant warnings both before and during the relevant period that Facebook’s
9 privacy policies did not comply with applicable laws, and moreover, that the same practices
10 which violated the law and user trust was the Company’s primary source of revenue.

11 392. During a May 27, 2015 presentation to the IRS, a Facebook representative
12 indicated that “[Facebook] built ‘forecasts,’ from internal and external data, projecting
13 [Facebook]’s [REDACTED] on a country-by-country basis, so that Facebook could look at the
14 forecasts, ‘U.S. versus international.’” The representative stated that she has seen both year-
15 long and three year forecasts, and the IRS subsequently asked Facebook to provide all
16 Documents constituting, reflecting or referring to any such “forecasts” of growth of [redacted],
17 created, obtained or circulated from 2008 until 2012. If, as the IRS disclosures suggest,
18 Facebook forecasted growth based on national and international rights to exploit Facebook’s
19 “platform technology,” there can be no doubt that the Board knew of such exploitation of user
20 data, and that it has been a core aspect of Facebook’s business since well before the Company’s
21 initial public offering in 2012.

22 393. In the June 8, 2016 summons, the IRS noted that a former Facebook executive
23 who was examined under oath by the IRS on May 17, 2016, “made quarterly presentations to
24 [Facebook]’s Board of Directors regarding user growth, projected and actual; (b) other
25 executives of [Facebook] also made quarterly presentations to [Facebook]’s Board of Directors
26 on topics or areas covered by the divisions they supervised; and (c) quarterly financials were
27 presented to the Board of Directors as part of the quarterly board meetings.”
28

1 394. Given the Board’s awareness and deliberate concealment of the extent to which
2 Facebook’s business model and revenue depends upon its targeted advertisements, which
3 requires the Company to collect, store, and share massive amounts of user data, and
4 Facebook’s failure to disclose or notify users of these practices, it is clear the Board either
5 deliberately or recklessly permitted the Company to pursue profit at the expense of complying
6 with the law.

7 395. Defendants directed, authorized, and oversaw the misconduct alleged herein, and
8 they regularly monitored Facebook’s user and revenue growth. Defendant Zuckerberg was
9 personally involved in developing Facebook’s platform and was responsible for its
10 implementation. the activity, to a degree that reflects far more than his supervisory role of the
11 Company as CEO. In that role, Zuckerberg specifically instructed Facebook employees to
12 prepare for and circumvent the blocks that he anticipated other websites would implement.

13 396. Defendants maintained executive compensation practices that improperly
14 incentivized Facebook’s growth, and the illegal activity, throughout the relevant period.

15 397. The Board’s actions and decisions are not entitled to the presumption of the
16 business judgment rule because Defendants failed to act in good faith and put their own
17 personal and financial interests above those of Facebook and its shareholders. Demand is,
18 therefore, futile (and excused).

19 **2. The Board Failed to Comply with the 2011 FTC Consent Decree and**
20 **Has Exposed Facebook to Further Sanctions**

21 398. Defendants were aware of yet disregarded their affirmative obligations to oversee
22 Facebook’s compliance with the 2011 Consent Decree entered into with the FTC.

23 399. Because a majority of the directors face a substantial risk of liability for
24 Facebook’s violations of law, or at a minimum, for exposing Facebook to sanctions for
25 violating the FTC Consent Decree, demand is futile.

26 400. Section VII of the Consent Decree provides, in relevant part, that “[Facebook]
27 shall deliver a copy of this order to all current and future principals, officers, directors, and
28 managers; (2) all current and future employees, agents, and representatives having supervisory

1 responsibilities relating to the subject matter of this order, and (3) any business entity resulting
2 from any change in structure.... [Facebook] shall deliver this order to such current personnel
3 within thirty (30) days after service of this order, and to such future personnel within thirty (30)
4 days after the person assumes such position or responsibilities.”

5 401. Thus, each of the Defendants received the Consent Decree, pursuant to Section
6 VII, and therefore had knowledge of the issues addressed therein and the Company’s
7 affirmative obligations under the agreement. Yet, Defendants failed to act to ensure the
8 Company complied with the Consent Decree.

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

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

19 404. Further, the Audit Committee members were charged with assisting the Board in
20 overseeing the integrity of the Company’s financial statements and the adequacy and reliability
21 of disclosures to its stockholders, including the Company’s internal controls.

22 405. But Facebook’s internal and disclosure controls were deficient, causing Facebook
23 to issue materially false and misleading information regarding the Company’s practices. The
24 Audit Committee was directly responsible for approving the Company’s materially false and
25 misleading SEC filings including the 2017 and 2018 Proxy Statements.

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

28 407. In its 2011 consent decree, the FTC said Facebook told users that third party apps

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

9 408. PwC’s improper certification and failure to detect the serious internal controls
10 deficiencies at the Company in conducting its audits of Facebook may be related to its ties with
11 members of Facebook’s audit committee. In particular, defendant Desmond-Hellman has close
12 ties to PwC that extend beyond her tenure on Facebook’s Board and may have had an impact
13 on why PwC continually certified that the Company’s privacy controls were effective in
14 accordance with the FTC Consent Decree. Desmond-Hellman became the Chancellor of UCSF
15 on August 3, 2009 and served in that position until 2014. In 2012, UCSF’s Global Health
16 Group partnered with PwC Global Healthcare to form a joint fellowship, under Desmond-
17 Hellman’s watch.

18 409. All of the Defendants failed to exercise any oversight over the insider sales
19 transactions and failed to implement reasonable internal controls with respect to same.
20 Accordingly, a clear majority of the Board is unable to consider a demand to investigate
21 Plaintiff’s allegations that the Insider Selling Defendants engaged in illegal insider selling of
22 Company stock, committed other wrongdoing in violation of their fiduciary duties, and
23 artificially inflated the Company’s stock price for their own personal gain. Defendants cannot
24 investigate allegations of the other Defendants’ wrongdoing in a disinterested and independent
25 manner.

26 410. In light of the foregoing facts, Defendants face a substantial likelihood of liability
27 in this case, thus rendering demand on them futile (and excused).

28 **C. FACEBOOK IS “CONTROLLED” BY ZUCKERBERG AND HE DOMINATES THE BOARD**

1 411. Demand was also futile, and therefore excused, because defendant Zuckerberg
2 dominates and controls the entire Board by virtue of his controlling voting power, and because
3 a majority of the directors are beholden to him, and lack independence from him, as explained
4 further below.

5 412. There is no question that defendant Zuckerberg controls the Board and the entire
6 Company in his role as CEO of Facebook, which he founded. Facebook’s status as a
7 “controlled” company is inherent in its corporate governance (Dual-Class) structure, and the
8 role Zuckerberg has played in recruiting and retaining the current directors cannot be
9 understated – it is Zuckerberg alone who has the power to elect (and remove) any director from
10 Facebook’s Board, by virtue of his share ownership, controls a majority of Facebook’s
11 outstanding voting power, or 53.3 percent of the total voting power, according to the
12 Company’s most recent 2018 Proxy Statement. Zuckerberg’s control of Facebook is like a
13 dictatorship, and he directs and is responsible for the activities of Facebook’s employees.

14 413. According to Facebook’s 2017 Proxy Statement:

15 Because Mr. Zuckerberg controls a majority of our outstanding voting power, *we are a*
16 *“controlled company”* under the corporate governance rules of the NASDAQ Stock
17 Market LLC (NASDAQ). Therefore, *we are not required to have a majority of our*
18 *board of directors be independent*, nor are we required to have a compensation
19 committee or an independent nominating function. In light of our status as a controlled
20 company, our board of directors has determined not to have an independent nominating
21 function and to have the full board of directors be directly responsible for nominating
22 members of our board.

23 414. Defendant Zuckerberg directs and controls the Company’s business and is
24 personally responsible for the damage caused to Facebook as a result of the illegal business
25 practices and data sharing that led to the Cambridge Analytica scandal. Accordingly,
26 Zuckerberg lacks the requisite “disinterestedness” to consider a demand.

27 415. Former Facebook employee Parakilas confirmed that defendant Zuckerberg has
28 always been responsible for Facebook’s policies, noting that shortly after he arrived at the
company’s Silicon Valley headquarters in 2011, Parakilas was told that any decision to ban an
app required the *personal approval* of defendant Zuckerberg, although the policy was later
relaxed.

1 416. Facebook’s website states that “Mark [Zuckerberg] is responsible for setting the
2 overall direction and product strategy for the company. He leads the design of Facebook’s
3 service and development of its core technology and infrastructure.” Defendant Zuckerberg also
4 is responsible for Facebook’s policies, according to defendant Sandberg. In a May 30, 2018
5 interview with Recode Media, she stated, “**Mark has said very clearly on Cambridge**
6 **Analytica that he designed the platform and he designed the policies**, and he holds himself
7 responsible.” Defendant Zuckerberg directs and controls the Company’s business and is
8 personally liable for the wrongdoing and damage cause to Facebook as alleged herein.
9 Accordingly, defendant Zuckerberg lacks the requisite “disinterestedness” to consider a
10 demand.

11 417. In an interview with Recode Media on May 30, 2018, defendant Sandberg
12 acknowledged the entrenchment of defendant Zuckerberg and that he (and she) will make
13 decisions notwithstanding any criticism. “You know, in terms of the business, we don’t make
14 decisions for the short run. We don’t have to and we shouldn’t. I don’t think any company
15 should have to. But **we have founder control and protections in place, and we’re very clear**
16 **that we’re gonna make the investments we need to make.**”

17 418. On June 26, 2018, a group of six of Facebook’s largest shareholders publicly
18 asked to remove Zuckerberg from his chairman position and to replace him with an
19 independent executive. The shareholders also want to get rid of Facebook’s dual-class share
20 structure, which they believe hands over too much power to Zuckerberg and his team of
21 executives. Facebook unsurprisingly objected, “We believe that our capital structure is in the
22 best interests of our stockholders and that our current corporate governance structure is sound
23 and effective.” This has been a common rhetoric from Zuckerberg and Facebook, as he has
24 long faced criticism over the dual-class share structure, but he has ultimately refused to even
25 consider making any changes. Even independent investors have called for Zuckerberg to step
26 down as chairman and for Facebook to dissolve its dual-class stock structure. Neither of these
27 has happened. Zuckerberg habitually ignores the protests, objections, and suggestions of both
28 shareholders and independent investors, and continues to benefit financially in the form of

1 billions of dollars due to Facebook’s top-heavy corporate governance structure. Clearly,
2 Zuckerberg’s decision-making rationale does not take into consideration the opinions of
3 shareholders, and he prioritizes his own power and control instead of the long-term interests of
4 the Company.

5 419. Defendant Zuckerberg has always dominated and controlled Facebook and its
6 Board, and his aspirations were even larger all the way back in 2005. Former Facebook
7 employee Kate Losse (“Losse”), a speechwriter for Zuckerberg until 2005, recalls that
8 Zuckerberg would end weekly Friday all-hands meeting by raising his fist with a slight smile
9 and saying, “Domination!”

10 420. Losse confirmed that Zuckerberg created an atmosphere at Facebook that
11 discouraged questioning power and standing up to management. Losse stated, “But the
12 question I was afraid to ask him was this: If we were to achieve our goal, why should the world
13 trust Facebook or Zuckerberg to shape and manage this new global meta-society? Could
14 Zuckerberg, who wields considerable power over Facebook’s share structure, develop the self-
15 awareness and responsibility to manage it? If my co-workers were asking themselves these
16 same questions, I didn’t see it being discussed on our internal forum pages or in conversations
17 around the office.”

18 421. Losse noted that most employees were afraid of losing their lucrative jobs and
19 that “internal conversations stayed focused on technical and growth questions; questions that
20 can be answered with metrics — how fast are we growing and what technical roadblocks can
21 we remove — rather than introspection.” While Losse recalls this being the atmosphere back
22 in 2005, it seems to have manifested into Zuckerberg’s push for the growth-at-all-costs model
23 introduced in 2008. Zuckerberg’s style of responding to questioning from members of the
24 U.S. Congress and the U.K. Parliament reflects this culture: rather than actually speaking about
25 possible internal improvement, Zuckerberg deflected questions and avoid answering them
26 directly by purposely focusing on explaining Facebook in technical terms.

27 422. The results of the 2018 stockholder meeting confirm that defendant Zuckerberg
28 continues to control the Board. He selected director Jeffrey Zients to replace defendant Koum

1 after the 2018 Proxy Statement was issued and before the stockholder meeting, but no vote was
2 required and defendant Zuckerberg thus effectively unilaterally appointed Zients to the Board
3 for the entire year.

4 423. All of the directors on Facebook’s Board lack independence from defendant
5 Zuckerberg, for these and other reasons explained below. Because he dominates and controls
6 the entire Board, demand was futile as to defendant Zuckerberg and is excused as to the entire
7 Board.

8 **1. Demand was Futile as to Defendant Thiel**

9 424. Defendant Thiel was one of the early investors in Facebook and is its longest-
10 standing Board member besides Zuckerberg. Thiel co-founded PayPal, Inc., and has been a
11 Partner of the Founders Fund, a venture capital firm that strives to keep founders in control of
12 the companies they have created, since 2005. Thiel also co-founded Palantir in 2003.

13 425. Defendant Thiel has been instrumental to Facebook’s business strategy over the
14 years. He has been known to personally engage in secretive politically-motivated litigation
15 tactics, most notably with regard to Gawker, a gossip website that owned Valleywag, a blog
16 specifically concerning Silicon Valley gossip. Angered by a 2007 post on Valleywag
17 headlined “Peter Thiel Is Totally Gay, People” and other stories published on Gawker’s
18 website, he secretly financed a lawsuit filed by Terry Bollea (the real name of the wrestler Hulk
19 Hogan) against Gawker for posting an excerpt from a sex tape showing Mr. Hogan with a
20 friend’s wife. After Hogan won a \$140 million judgment against Gawker, the site went
21 bankrupt. Gawker founder Nick Denton described Thiel to *Vanity Fair* as “interesting — and
22 scary.”

23 426. *The New York Times* reported on Thiel’s connections to Palantir and Cambridge
24 Analytica in an article published on January 11, 2017. According to *The Times*, Thiel was “a
25 member of the Trump transition team” and had “dressed as Hulk Hogan for the ‘Villains and
26 Heroes’ annual costume party last month, hosted on Long Island by the Mercer family, who
27 were big Trump donors.” Thiel, who was reportedly advising the Trump transition team on
28 “science,” had recently organized a meeting with tech executives, including Palantir’s CEO,

1 Alex Karp, and other executives who were described as “anti-Trump” but had “sort of changed
2 their minds.”

3 427. When asked by the reporter if he was concerned about conflicts of interest in
4 relation to Trump and the tech meeting, Thiel said: “I don’t want to dismiss ethical concerns
5 here, but I worry that ‘conflict of interest’ gets overly weaponized in our politics. I think in
6 many cases, when there’s a conflict of interest, it’s an indication that someone understands
7 something way better than if there’s no conflict of interest. ***If there’s no conflict of interest,***
8 ***it’s often because you’re just not interested.***” Thiel also reportedly said in response to a
9 comment by the reporter that Barack Obama had avoided “any ethical shadiness” during his
10 eight-year term as president, “But there’s a point where no corruption can be a bad thing. It
11 can mean that things are too boring.”

12 428. Defendant Thiel’s other comments during the interview are telling as to his
13 knowledge of Facebook’s illicit business practices and are similarly unsettling as to his
14 membership on Facebook’s Board. For instance, *The Times* reporter commented that “Mr.
15 Thiel and Mr. Trump are strange bedfellows, given that much of Mr. Thiel’s billions came
16 from being one of the original investors in Facebook and Mr. Trump recently said it’s better to
17 send important messages by courier.” In response, Thiel stated, “Well, ***one does have to be***
18 ***very careful with what one says in an email.***”

19 429. In the interview, Thiel acknowledged the reports of Russian hacking, stating,
20 “There’s a strong circumstantial case that Russia did this thing.” When asked if he worried
21 about the relationship between Vladimir V. Putin and then-President elect Trump, Thiel
22 responded, “But should Russia be allied with the West or with China?” “There are these really
23 bad dictators in the Middle East, and we got rid of them and in many cases there’s even worse
24 chaos.” Thiel also stated, “***It’s the people behind the red-eyed robots that you need to be***
25 ***scared of.***” When asked about the “incestuous amplification of the Facebook news feed,” Thiel
26 cryptically responded, “There’s nobody you know who knows anybody. There’s nobody you
27 know who knows anybody who knows anybody, ad infinitum.”

28 430. The *Times* reporter pointed out that Thiel is a “social-media visionary” yet he

1 “rarely updates his Facebook page and doesn’t tweet,” which Thiel reportedly said is “because
2 you always want to get things exactly right” and “if you start doing it, you have to do it a lot.”
3 According to the reporter, Thiel also “wondered if his most famous investment, Facebook,
4 *contributes to herd mentality.*”

5 431. Defendant Thiel will not institute any litigation against Zuckerberg because he is
6 beholden to him. Thiel has greatly benefited by his relationship with Zuckerberg and his seat
7 on the Facebook Board. The Founders Fund gets “good deal flow” from this high profile
8 association, and further demonstrates that Thiel has a personal bias in favor of keeping
9 founders in control of the companies they created and will not act to remove Zuckerberg from
10 his position. Thiel’s venture capital fund, The Founders Fund, is marketed on the principle that
11 company founders should have long-term control of the companies they create. In fact, the
12 Fund’s website touts Facebook as a primary example of that maxim, stating that “we have often
13 tried to ensure that founders can continue to run their businesses through voting control
14 mechanisms, as Peter Thiel did with Mark Zuckerberg and Facebook.”

15 432. In addition to the past connections which demonstrate that defendant Thiel lacks
16 independence from defendant Zuckerberg, Thiel has a current personal and financial interest in
17 remaining on Facebook’s Board. According to the 2018 Proxy Statement, the Facebook shares
18 owned by the Founders Fund – i.e., defendants Thiel and Andreesen – are to be released from
19 escrow in connection with the Oculus acquisition. Thiel stands to gain substantially from the
20 vesting of stock in connection therewith.

21 433. The foregoing facts demonstrate that defendant Thiel is interested and lacks
22 independence due to his close relationship with defendant Zuckerberg and will not take any
23 action against Zuckerberg or that will threaten his prestigious and lucrative position as a
24 Facebook director. Demand was futile as to defendant Thiel.

25 **2. Demand was Futile as to Defendant Andreesen**

26 434. Defendant Andreesen has demonstrated a deep-rooted personal bias in favor of
27 keeping founders in control of the companies they created. When he and his partner, Ben
28 Horowitz (“Horowitz”), were trying to get Loudcloud, a company that they co-founded, on its

1 feet, the venture capitalist providing their funding advised Horowitz to cut Andreessen out of
2 the project altogether. Based on this experience, when Andreessen and Horowitz founded their
3 own venture capital firm, Andreessen Horowitz, they “set out to design a venture capital firm
4 that would enable founders to run their own companies” without interference from the financial
5 backers.

6 435. Defendant Andreessen lacks independence from Zuckerberg. Andreessen has
7 greatly benefited by his relationship with Zuckerberg and his seat on the Facebook Board. The
8 Founders Fund gets “good deal flow” from this high profile association. Moreover, according
9 to the 2018 Proxy Statement, the Facebook shares owned by the Founders Fund – i.e.,
10 defendants Thiel and Andreessen – are to be released from escrow in connection with the
11 Oculus acquisition. (2018 Proxy Statement at 39)

12 436. Andreessen also lacks independence from Zuckerberg based on the highly
13 lucrative deals that Andreessen and his firm have made with Zuckerberg in the past few years.

14 437. Andreessen Horowitz has seen two of its portfolio companies purchased by
15 Facebook – Instagram and Oculus VR. Andreessen turned his firm’s \$250,000 investment in
16 Instagram into \$78 million when the \$1 billion acquisition by Facebook closed. Andreessen
17 would not have even been able to invest in Oculus VR without Zuckerberg. Andreessen had
18 declined to invest in the company previously, but desperately wanted to invest by the fall of
19 2013, according to an October 2015 Vanity Fair article. When Oculus VR’s CEO seemed
20 reluctant to allow the investment, Andreessen reportedly had Zuckerberg talk to the CEO about
21 Andreessen. Andreessen Horowitz got the deal and Andreessen became one of four board
22 members for the fledgling company. Not very long after, Zuckerberg offered \$2 billion for
23 Facebook to acquire Oculus VR.

24 438. Andreessen knows that his firm’s access to the best investments – its “deal flow”
25 – relies heavily on his relationship with Zuckerberg and Facebook. In a May 18, 2015 New
26 Yorker article titled “Tomorrow’s Advance Man,” Andreessen reportedly said that “Deal flow
27 is everything. If you’re in a second-tier firm, you never get a chance at that great company.”
28 Andreessen Horowitz saw its biggest successes after “logo shopping” to add Facebook to the

1 firm's portfolio in 2010. Within two years of that investment, "Andreessen Horowitz was the
2 talk of the town."

3 439. According to a December 8, 2016 article posted on Deal Breaker, "Marc
4 Andreessen and Mark Zuckerberg Are BFFs, and Pesky Board Negotiations Can't Change
5 That," Andreessen was one of Zuckerberg's first friends – and funders – in the Valley. In
6 return, Zuckerberg gave him a seat on the Board in 2008, and the two have remained tight
7 since. The dispute goes back to when Zuckerberg wanted to sell a bunch of shares but maintain
8 voting control of the company. To do so would require a stock split that would dilute other
9 voting shares, potentially to the detriment of other stakeholders. The proposal was
10 controversial, so the Board created a special committee to represent shareholders on the matter,
11 composed of Susan Desmond-Hellmann, Erskine Bowles and, of course, Zuckerberg close
12 friend Andreessen. While on the committee, Andreessen slipped Zuckerberg information about
13 their progress and concerns, helping Zuckerberg negotiate against them, according to court
14 documents.

15 440. When the time came for the committee to ask Zuckerberg questions on a
16 conference call, Andreessen warned the Facebook founder about what he would be asked
17 before directors posed the questions. While the committee grilled Zuckerberg about why he
18 wanted a special class of stock, Andreessen sent the CEO text messages to explain which of his
19 arguments weren't working and why, according to messages quoted in court filings. During
20 one March 4 call, Andreessen gave Zuckerberg live updates, both negative ("This line of
21 argument is not helping.") and positive ("NOW WE'RE COOKING WITH GAS"), according
22 to texts provided by Facebook's lawyers and cited in court filings. "Andreessen even told
23 Zuckerberg that he was working to protect Zuckerberg's personal interests through the Special
24 Committee process," according to the filings. When the two prevailed over defendant Bowles,
25 who reportedly had initially looked askance at the whole deal, defendant Andreessen texted
26 defendant Zuckerberg, "The cat's in the bag and the bag's in the river." "Does that mean the
27 cat's dead?" Zuckerberg replied, dumbfounded. Andreessen answered, "Mission accomplished
28 [smiley face]".

1 **3. Demand was Futile as to Defendant Hastings**

2 441. Defendant Hastings lacks independence from Zuckerberg. Defendant Hastings is
3 a co-founder of Netflix, and currently serves as its CEO and Chairman of its board of directors.
4 Netflix is one of Facebook's largest advertisers, and Defendants have disclosed that Netflix
5 purchased ads from Facebook during the relevant period through the Company's usual
6 procedures "including a competitive bid auction." (See 2018 Proxy Statement at 13)

7 442. In addition to being sympathetic to Zuckerberg's desire to maintain founder's
8 control due to his own founder role at Netflix, defendant Hastings has every incentive to cater
9 to Zuckerberg's desires at Facebook due to Facebook's business relationship with Netflix.
10 Through the "Friends and Community" initiative launched in March 2013, Netflix enjoyed
11 very valuable word-of-mouth type marketing because the initiative allows Facebook users to
12 share data about their Netflix viewing habits with their Facebook friends. Hastings would not
13 want to risk losing this relationship, as the initiative's launch caused Netflix's share price to
14 climb 6%, and displeasing Zuckerberg could mean an end to such valuable data.

15 443. Further, Facebook has not done much direct commerce historically, but now sells
16 virtual reality headsets through Oculus, and is planning to push into other home electronics,
17 like a video chat device. Although it has been noted that Facebook's push into original video
18 content could create a potential conflict of interest situation. Hastings, however, does not want
19 to risk losing his relationship with Facebook, or with Zuckerberg, given how lucrative these
20 relationships are for Netflix and for Hastings, personally, and he remains on Facebook's Board.

21 **4. Demand was Futile as to Defendant Sandberg**

22 444. Defendant Sandberg joined Facebook in 2008 as COO and took over business
23 operations. Sandberg oversees sales management, business development, human resources,
24 marketing, public policy, privacy and communications. Defendant Sandberg, in her role as
25 COO since 2008, is responsible for directing and approving the illegal acts committed by
26 Facebook employees. Moreover, Sandberg has been at Facebook since its early days, and has
27 overseen the Company's meteoric rise, based upon the illegal business practices she
28 implemented along with Zuckerberg since the launch of Facebook's platform in 2008.

1 445. Facebook was running a \$561 million deficit and struggling through a period of
2 stagnant growth at the time of Sandberg's hire in 2008. Her job, in essence, was to make the
3 company profitable and she accomplished this by directing Facebook toward advertising as its
4 main business. She took on the project of integrating ads into the News Feed on both the
5 desktop and mobile versions of Facebook. Since user data and advertising operations go hand
6 in hand, Sandberg has an elevated responsibility to protect user information, especially since
7 Facebook has incredible access to the user data of billions of customers. The data that
8 Facebook collects on users funnels directly toward targeted ads.

9 446. Before she was hired by defendant Zuckerberg, defendant Sandberg served as
10 Google's vice president of global online sales, where she learned how to profit from user data
11 through targeted advertising. When she was brought on at Facebook in 2008, Sandberg
12 advised Zuckerberg to either make users pay or to make advertisers pay, in regard to
13 Facebook's overarching business model. Together with the other Defendants, they decided that
14 advertisers would pay. From there, Sandberg determined that brand advertising would become
15 Facebook's sole source of revenue, demonstrating her close personal and business relationship
16 with Zuckerberg, and her significant influence on Facebook's business and decisions overall.
17 One year later, Facebook generated a profit for the first time.

18 447. In 2009, Facebook generated \$225 million in revenue from ad sales, and the
19 following year, brand advertising skyrocketed to \$2 billion in sales. This concept of
20 maximizing brand advertising that is attributable to Sandberg is consistent with Facebook's
21 growth-at-all costs strategy introduced in 2008 and cemented her dedication and loyalty to
22 defendant Zuckerberg.

23 448. Defendant Sandberg has well-established connections with defendant Zuckerberg
24 and has a significant influence on his decisions. When Zuckerberg was considering hiring
25 Sandberg, the two spent months speaking for several hours a week to determine whether she
26 would be a good fit for the position. To this day, Sandberg and Zuckerberg have twice-weekly
27 meetings to give each other feedback and to work through disagreements, which has been
28 going on for a decade now. She has been deemed Zuckerberg's second-in-command, giving

1 her significant control in the direction that Facebook takes.

2 449. Defendant Sandberg has admitted that she is personally responsible for
3 Facebook's lax data privacy controls. In an interview with Bloomberg, she stated, "I feel
4 deeply personally responsible, because a lot of mistakes were made...what we didn't do until
5 recently and what we are doing now is just take a broader view looking to be more restrictive in
6 ways data could be misused. We also didn't build our operations fast enough -- and that's on
7 me." Compounding this issue, Sandberg promises policy changes on data security but still
8 does not seem to have a grasp of the severity of the issue. On April 5, 2018, she told the
9 *Financial Times*, "To this day, we still don't know what data Cambridge Analytica has."

10 450. Recode Media interviewed defendant Sandberg and Mike Schroepfer,
11 Facebook's Chief Technology Officer, on May 30, 2018. When asked why nobody had been
12 fired, and who should have been fired, with regard to the Cambridge Analytica scandal,
13 Sandberg stated, "So, Mark has said very clearly on Cambridge Analytica that he designed the
14 platform and he designed the policies, and he holds himself responsible. ***The controls in the***
15 ***company and this are under me***, I hold myself responsible for the ones we didn't have. And
16 look, Schroep[fer] and I are here, we run the company." She acknowledged that the Company
17 had insufficient internal controls, stating, "we always had some controls in place but I don't
18 think they were enough." She further admitted that Facebook had not audited Cambridge
19 Analytica to ensure they had actually deleted the data. "***Looking back, we definitely wish we***
20 ***had put more controls in place***. We got legal certification that Cambridge Analytica didn't
21 have the data, ***we didn't audit them***," she admitted.

22 451. Despite admitting she was personally responsible for failing to establish adequate
23 internal controls, defendant Sandberg has continued to defend Facebook's advertising business
24 that relies on the mass collection of Facebook users' data, saying that it benefits consumers.
25 Sandberg uses "consumer benefit" as a guised rationale for continuing its overreaching
26 advertising business, when the de facto purpose is to generate profit. This is not surprising, as
27 Sandberg has demonstrated a track record of prioritizing profitability, and she was the direct
28 beneficiary of Facebook's manipulation of consumers' personal data in the Cambridge

1 Analytica incident.

2 452. Indeed, defendant Sandberg's compensation is based off of Facebook's
3 profitability, and specifically targets that are related to increasing advertising revenues.
4 According to Facebook's 2017 Proxy Statement, Sandberg received \$631,731 for the First Half
5 2016 bonus, which reflected her "overall leadership and execution on business priorities, her
6 contribution to growing revenue, continued strong growth in the number of advertisers on our
7 [Facebook's] platform, and her leadership in key policy matters." Sandberg received \$661,904
8 for the Second Half 2016 bonus. These bonuses were the highest among those handed out to
9 Facebook's Board of Directors, highlighting her influence in policy decisions and her
10 established power as a long-standing member of Facebook's Board.

11 453. More recently, in an interview with NBC's Today show, Sandberg said that users
12 who wanted to stop Facebook from making money off their personal data would have to pay
13 for the privilege. *Today's* Savannah Guthrie asked, "Could you come up with a tool that said,
14 'I do not want Facebook to use my personal profile data to target me for advertising.'? Could
15 you have an opt-out button – 'Please don't use my profile data for advertising'?" Sandberg
16 responded, "We have different forms of opt-out. We don't have an opt-out at the highest level.
17 That would be a paid product." Clearly, Sandberg has a personal financial interest in Facebook
18 continuing to earn revenues based on the personal information and data it obtains and generates
19 about Facebook's users and non-users and will not act to change its business model. Her
20 compensation is directly tied to Facebook's revenues that are generated from the sale of
21 targeted advertising services, and she has acted and will continue to prioritize profitability over
22 complying with the law. Demand is, therefore, futile as to defendant Sandberg.

23 **5. Demand was Futile as to Defendant Bowles**

24 454. Defendant Bowles is beholden to the entire Board for granting a waiver of the
25 mandatory retirement age for directors set forth in Facebook's Corporate Governance
26 Guidelines, so that defendant Bowles could stand for re-election to the Board despite having
27 attained the age of 70 years before the date of the Company's annual stockholder meeting on
28 May 31, 2018.

1 455. Section IX of Facebook’s Corporate Governance Guidelines, **Retirement Age**,
2 states, “It is the general policy of the company that no director having attained the age of 70
3 years (as of the date of Facebook’s annual stockholder meeting for such year), shall be
4 nominated for re-election or reappointment to the Board. However, the Board may determine to
5 waive this policy in individual cases.” Section XXIV, **Review, Amendment and Waiver of**
6 **Guidelines**, provides that “[t]he Board may amend these Corporate Governance Guidelines, *or*
7 *grant waivers in exceptional circumstances*, provided that any such modification or waiver
8 may not be a violation of any applicable law, rule or regulation, and, provided further, that any
9 such modification or waiver is appropriately disclosed.”

10 456. According to the 2018 Proxy Statement, defendant Bowles reached the
11 mandatory retirement age for directors this year, but Board granted a waiver of policy to permit
12 his re-election at the 2018 stockholder meeting. Defendants did not disclose any reason for the
13 waiver granted to defendant Bowles, let alone identify any “exceptional circumstances”
14 warranting the waiver, in the 2018 Proxy Statement.

15 457. Defendant Bowles is beholden to the entire Board for granting him the waiver
16 and allowing him to continue in his prestigious and lucrative position on Facebook’s Board.
17 Accordingly, he lacks independence from other interested directors, and demand was futile as
18 to defendant Bowles.

19 **6. Demand was Futile as to Defendant Desmond-Hellmann**

20 458. Defendant Desmond-Hellmann is chief executive of the Gates Foundation, and
21 formerly served as an executive at Genentech and as a director at Procter & Gamble. It is no
22 coincidence that she is one of the newest Facebook directors, and one of the only members of
23 Facebook’s Board that does not have extensive experience and a background in tech
24 entrepreneurship. Defendant Zuckerberg has surrounded himself with Silicon Valley
25 entrepreneurs on Facebook’s Board who have interests that are closely aligned with his,
26 making it extremely difficult for new directors and shareholders alike to protest his decisions,
27 because he usually does not face much if any opposition in policy matters.

28 459. Defendant Desmond-Hellman lacks independence from defendant Zuckerberg,

1 and she has already demonstrated that she will not take any action to oppose his wishes or the
2 other directors. In April 2016, when Zuckerberg announced a plan to issue new “Class C”
3 shares with no voting rights, that would allow him to sell the majority of his shares for billions
4 of dollars, while simultaneously retaining total control over decision-making, Desmond-
5 Hellmann initially objected to the share reclassification, legal briefs filed in the case show.
6 However, fellow board members eventually swayed her to vote in his favor, highlighting her
7 willingness to cede to Zuckerberg’s views even when they conflict with her own views of what
8 is best for the Company and its shareholders.

9 460. As the lead director of Facebook’s Board, defendant Desmond-Hellman made a
10 public statement following the break of the Cambridge Analytica story, saying that the Board
11 supported both defendants Zuckerberg and Sandberg. It was the Board’s only comment about
12 the revelations, confirming once again that Desmond-Hellman will not take any position
13 against Zuckerberg, even in a statement, let alone commence litigation against him.

14 **7. Demand was Futile as to Facebook Director Ken Chenault**

15 461. On January 18, 2018, Facebook announced that the Company added a new
16 member to its board of directors: Ken Chenault (“Chenault”), then CEO of American Express.
17 Chenault is the first new director since defendant Koum joined Facebook’s Board in 2014.

18 462. Defendant Zuckerberg announced the new appointment in a Facebook post,
19 claiming he’s been “trying to recruit Ken for years.” “He has unique expertise in areas I believe
20 Facebook needs to learn and improve — customer service, direct commerce, and building a
21 trusted brand,” Zuckerberg added. “Adding someone to our board is one of the most important
22 decisions our board makes. It’s a long process that I take very seriously since this is the group
23 that ultimately governs Facebook. Ken and I have had dinners discussing our mission and
24 strategy for years, and he has already helped me think through some of the bigger issues I’m
25 hoping we take on this year.”

26 463. For all of the foregoing reasons, demand on Facebook’s Board was futile, and
27 therefore, excused.
28

1 CAUSES OF ACTION

2 FIRST CAUSE OF ACTION

3 Violation of Section 14(a) of the Exchange Act and SEC Rule 14a-9

4 (Against the Individual Defendants)

5 464. Plaintiffs incorporate by reference and reallege each of the foregoing allegations
6 as though fully set forth in this paragraph, except to the extent those allegations plead knowing
7 or reckless conduct by the Defendants. This claim is based solely on negligence, not on any
8 allegation of reckless or knowing conduct by or on behalf of the Defendants. Plaintiffs
9 specifically disclaim any allegations of, reliance upon any allegation of, or reference to any
10 allegation of fraud, scienter, or recklessness with regard to this claim.

11 465. SEC Rule 14a-9 (17 C.F.R. § 240.14a-9), promulgated under Section 14(a) of the
12 Exchange Act, provides:

13 No solicitation subject to this regulation shall be made by means of any
14 proxy statement form of proxy, notice of meeting or other communication,
15 written or oral, containing any statement which, at the time and in the light
16 of the circumstances under which it is made, is false or misleading with
17 respect to any material fact, or which omits to state any material fact
18 necessary in order to make the statements therein not false or misleading
or necessary to correct any statement in any earlier communication with
respect to the solicitation of a proxy for the same meeting or subject
matter which has become false or misleading.

19 466. Defendants negligently issued, caused to be issued, and participated in the
20 issuance of materially misleading written statements to stockholders that were contained in
21 Facebook's Proxy Statements filed on Form DEF 14A on or about June 2, 2016 ("2016 Proxy
22 Statement"), April 14, 2017 ("2017 Proxy Statement"), and April 13, 2018 ("2018 Proxy
23 Statement") and in the supplements thereto.

24 467. The 2016, 2017 and 2018 Proxy Statements contained proposals to Facebook's
25 stockholders urging them to re-elect the members of the Board, approve executive
26 compensation, approve director compensation, approve adoption of an amended and restated
27 certificate of incorporation, and to vote against various stockholder proposals for Facebook's
28 Board, including to initiate and adopt a recapitalization plan and to take necessary steps to

1 change voting requirements, including in Facebook's charter and bylaws, for Facebook's Board
2 to issue a report discussing the merits of establishing a Risk Oversight Board Committee, for
3 the Company to appoint an independent Chair of the Board, and for the Company to issue a
4 report to shareholders regarding the efficacy of Facebook's enforcement of its terms of service
5 relating to content policies and assessing content-related risks. The 2016, 2017 and 2018 Proxy
6 Statements recommended a vote AGAINST each of the stockholder proposals, but misstated or
7 failed to disclose *any* facts whatsoever (i) regarding the Cambridge Analytica scandal,
8 including the fact that Defendants learned of the issue and related issues in 2015, and believed
9 that Facebook would face significant reputational harm if the truth were revealed; (ii) that
10 the Company's policies allowed certain third parties to access Facebook information including
11 user data and that of their friends, despite representations that the Company's policies
12 prohibited such practices; (iii) that the Company obtained information about Facebook users
13 and non-users from other sources besides Facebook's website; (iv) that the Company had failed
14 to enforce its platform policies or correct deficiencies in its internal controls that were known
15 to the Board when the Proxy Statements were filed, including its inability to track user data
16 once it left Facebook's servers; and (v) that the Company's corporate governance structure
17 was materially deficient. Thus, the 2016, 2017 and 2018 Proxy Statement soliciting materials
18 were materially false and misleading. By reasons of the conduct alleged in this Complaint, the
19 Defendants violated Section 14(a) of the Exchange Act and SEC Rule 14a-9. As a direct and
20 proximate result of the Defendants' wrongful conduct, Facebook misled or deceived its
21 stockholders by making misleading statements that were an essential link in stockholders
22 heeding Facebook's recommendation to re-elect the directors who are members of the current
23 Board, vote in favor of the Board's proposals, and vote against stockholder proposals identified
24 above.

25 468. The Board also knowingly agreed to include the false statements in the 2016,
26 2017 and 2018 Proxy Statements since it believed that, had it admitted its own ineffectiveness
27 in oversight of risk management, such admission would have led to the Defendants' own
28 personal liability for breaching their fiduciary duties as Board members. Thus, the Board acted

1 in bad faith and in a disloyal manner.

2 469. By reason of the conduct alleged herein, Defendants, who caused the issuance of
3 the 2016, 2017 and 2018 Proxy Statements, violated Section 14(a) of the Exchange Act. As a
4 direct and proximate result of these Defendants' wrongful conduct, Defendants misled and/or
5 deceived Facebook shareholders by falsely portraying material facts concerning the Company.
6 As a result of the false statements and material omissions, Facebook shareholders were
7 deceived. The false statements and material omissions were material because there is a
8 substantial likelihood that a reasonable shareholder would consider the information important
9 in deciding how to vote with respect to the matters contained in the Proxy Statements, which
10 were submitted for shareholder approval at the 2016, 2017 and 2018 annual meetings.

11 470. The misleading information contained in the 2016, 2017 and 2018 Proxy
12 Statements was material to Facebook's stockholders in determining whether or not to elect the
13 Defendants to the Board and how to vote with respect to the stockholder proposals, which was
14 material to the integrity of the directors that were proposed for election to the Board and their
15 oversight of the Company. The proxy-solicitation process in connection with the Proxy
16 Statements was an essential link in (i) the re-election of nominees to the Board and (ii) the
17 decision to approve the proposals recommended by the Board and not to approve the proposals
18 not recommended by the Board.

19 471. Plaintiff, on behalf of Facebook, thereby seeks relief for damages, as well as
20 injunctive and equitable relief, because the conduct of the Defendants named herein interfered
21 with Plaintiff's voting rights and choices at the 2016, 2017 and 2018 annual meetings.

22 472. This action was timely commenced within three years of the date of the 2016,
23 2017 and 2018 Proxy Statements and within one year from the time Plaintiff discovered or
24 reasonably could have discovered the facts on which this claim is based.

25
26
27
28

SECOND CAUSE OF ACTION

Violations of Section 10(b) of the Exchange Act

and SEC Rule 10b-5 Promulgated Thereunder

(Against All Defendants)

1
2
3
4
5 406. Plaintiffs incorporate by reference and reallege each and every
6 allegation contained above, as though fully set forth in this paragraph.

7 407. In connection with Facebook's repurchases of Facebook shares, Defendants
8 disseminated or approved false or misleading statements about Facebook as described above,
9 which they knew or recklessly disregarded were false or misleading and were intended to
10 deceive, manipulate, or defraud. Those false or misleading statements and Defendants'
11 course of conduct were designed to artificially inflate the price of the Company's common
12 stock.

13 408. At the same time that the price of the Company's common stock was inflated
14 due to the false or misleading statements made by Defendants, Defendants caused the
15 Company to repurchase millions of shares of its own common stock at prices that were
16 artificially inflated due to Defendants' false or misleading statements. Defendants engaged in
17 a scheme to defraud Facebook by causing the Company to purchase at least \$2 billion in
18 shares of Facebook stock at artificially inflated prices.

19 409. Defendants violated Section 10(b) of the Exchange Act and SEC Rule 10b-5 in
20 that they (a) employed devices, schemes, and artifices to defraud; (b) made untrue statements
21 of material facts or omitted to state material facts necessary in order to make the statements
22 made, in light of the circumstances under which they were made, not misleading; and/or (c)
23 engaged in acts, practices, and a course of business that operated as a fraud or deceit upon
24 Facebook in connection with the Bank's purchases of Facebook stock during the Relevant
25 Period.

26 410. Defendants, individually and in concert, directly and indirectly, by the use of
27 means or instrumentalities of interstate commerce or of the mails, engaged and participated
28 in a continuous course of conduct that operated as a fraud and deceit upon the Company;

1 made various false or misleading statements of material facts and omitted to state material
2 facts necessary in order to make the statements made, in light of the circumstances under
3 which they were made, not misleading; made the above statements intentionally or with a
4 severely reckless disregard for the truth; and employed devices and artifices to defraud in
5 connection with the purchase and sale of Facebook stock, which were intended to, and did,
6 (a) deceive Facebook; (b) artificially inflate and maintain the market price of Facebook
7 stock; and (c) cause Facebook to purchase the Company's stock at artificially inflated prices
8 and suffer losses when the true facts became known. Throughout the Relevant Period,
9 Defendants were in possession of material, adverse non-public information.

10 411. Defendants were among the senior management and the directors of the
11 Company, and were therefore directly responsible for, and are liable for, all materially false
12 or misleading statements made during the Relevant Period, as alleged above.

13 412. As described above, Defendants acted with scienter throughout the Relevant
14 Period, in that they acted either with intent to deceive, manipulate, or defraud, or with severe
15 recklessness. The misstatements and omissions of material facts set forth in this Complaint
16 were either known to Defendants or were so obvious that Defendants should have been
17 aware of them. Throughout the Relevant Period, Defendants also had a duty to disclose new
18 information that came to their attention and rendered their prior statements to the market
19 materially false or misleading.

20 413. Defendants' false or misleading statements and omissions were made in
21 connection with the purchase or sale of the Company's stock.

22 414. As a result of Defendants' misconduct, Facebook has and will suffer damages
23 in that it paid artificially inflated prices for Facebook common stock purchased as part of the
24 repurchase program and suffered losses when the previously undisclosed facts were disclosed
25 beginning in March 2018. Facebook would not have purchased these securities at the prices it
26 paid, or at all, but for the artificial inflation in the Company's stock price caused by
27 Defendants' false or misleading statements.
28

1 415. As a direct and proximate result of Defendants’ wrongful conduct, the
2 Company suffered damages in connection with its purchases of Facebook stock. By reason
3 of such conduct, Defendants are liable to the Company pursuant to Section 10(b) of the
4 Exchange Act and SEC Rule 10b-5.

5 416. Plaintiffs brought this claim within two years of their discovery of the facts
6 constituting the violation and within five years of the violation.

7 **THIRD CAUSE OF ACTION**

8 **Misappropriation of Information and Breach of Fiduciary Duty for Insider Sales**

9 **(Against the Insider Selling Defendants)**

10 473. Plaintiffs incorporate by reference and reallege each of the foregoing allegations
11 as though fully set forth in this paragraph.

12 474. At the time of the stock sales set forth above, each of defendants Zuckerberg,
13 Sandberg, and Koum (the “Insider Selling Defendants”) knew or recklessly disregarded the
14 information described in this Complaint regarding the breach and illicit data sharing and sold
15 Facebook common stock on the basis of that information.

16 475. The information described above was non-public information concerning the
17 Company’s unlawful conduct associated with its business strategy to generate revenues through
18 targeted advertising. The information was a proprietary asset belonging to the Company,
19 which the Insider Selling Defendants used for their own benefit when they sold Facebook
20 common stock.

21 476. The Insider Selling Defendants’ sales of their shares of Facebook common stock
22 while in possession and control of this material adverse non-public information was a breach of
23 their fiduciary duties of loyalty and good faith.

24 477. Because the use of the Company’s proprietary information for their own gain
25 constitutes a breach of the Defendants’ fiduciary duties, the Company is entitled to the
26 imposition of a constructive trust on any profits the Insider Selling Defendants obtained
27 thereby.

28

1 as though fully set forth in this paragraph.

2 484. Defendants, through their positions, possessed control and influence over the
3 Insider Selling Defendants' sale of Facebook common stock in violation of the California
4 Corporations Code. Defendants are statutorily liable to the same extent as the Insider Selling
5 Defendants under California Corporations Code § 25403.

6 485. Defendants were aware of the Insider Selling Defendants' knowledge of the
7 material adverse non-public information, and the Defendants were aware of the Insider Selling
8 Defendants' intent to sell Facebook common stock while in possession of material adverse
9 non-public information.

10 486. Defendants are culpable for the Insider Selling Defendants' underlying violations
11 of California Corporations Code § 25402 because of their knowledge and ability to control and
12 influence the Insider Selling Defendants and due to their involvement in preparing, approving,
13 and signing the Company's false or misleading Form 10-Ks, and Proxy Statements during the
14 relevant period.

15 487. Under California Corporations Code § 25403, each of the Defendants is liable to
16 Facebook for damages in an amount up to three times the difference between the price at which
17 Facebook common stock was sold by the Defendant and the market value that stock would
18 have had at the time of the sale if the information known to the Defendants had been publicly
19 disseminated prior to that time and a reasonable time had elapsed for the market to absorb the
20 information.

21 **SIXTH CAUSE OF ACTION**

22 **Breach of Fiduciary Duty**

23 **(Against All Defendants)**

24 488. Plaintiffs incorporate by reference and reallege each of the foregoing allegations
25 as though fully set forth in this paragraph.

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

1 administration and management of the affairs of the Company, including the Company's
2 financial reporting, internal controls, and compensation practices.

3 490. Additionally, the Defendants have affirmative obligations under the FTC Consent
4 Decree, as well as specific fiduciary duties as defined by the charters of various Board
5 committees that, had they been discharged in accordance with the Defendants' obligations,
6 would have necessarily prevented the misconduct and the consequent harm to the Company
7 alleged in this Complaint.

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

12 492. Each of the Defendants had actual or constructive knowledge that they had
13 caused the Company to improperly misrepresent the nature of its advertising services, user
14 privacy practices, and the extent of the its data sharing operations, and they failed to correct the
15 Company's public statements. Defendants had actual knowledge of the misstatements and
16 omissions of material facts set forth in this Complaint, or acted with reckless disregard for the
17 truth, in that they failed to ascertain and to disclose such facts, even though such facts were
18 available to them. Such material misrepresentations and omissions were committed knowingly
19 or recklessly and for the purpose and effect of increasing Facebook's revenues at the artificially
20 inflating the price of Facebook's securities.

21 493. Defendants breached their fiduciary duties to Facebook by their actions and
22 inactions, including, without limitation, by: (i) by implementing and overseeing Facebook's
23 illegal business strategy of pursuing profits and revenue growth through violations of various
24 laws, and conduct which was unethical or was designed to achieve an improper result or for an
25 improper purpose that was not in the Company's best interests; (ii) by suppressing, concealing,
26 and engaging in conduct designed to suppress, conceal, hide, or avoid detection or disclosure of
27 information about any illegal activity or wrongdoing; (iii) by omitting and failing to disclose
28 material information or facts concerning illegal activity or wrongdoing in any public

1 statements, or in connection with any request for information in any investigation, inquiry, or
2 litigation by any government entity or regulator, and in discovery in any civil or criminal
3 litigation; (iv) by consciously permitting, allowing, and encouraging business practices that
4 were unfair and violated the expectations and trust of Facebook's stockholders, users of
5 Facebook's social networking website, smartphone users and users of mobile devices, U.S.
6 citizens, government officials, and the public at large; (v) by turning a blind eye to the
7 Company's illegal activity and any persons who were employees, attorneys, and advisors or
8 had any similar relationship with the Company who engaged in wrongdoing or any illegal
9 activity relating to their position, responsibilities and duties respecting the Company, pursued
10 profits or revenue growth, or who obtained any personal financial gain, at the expense of any of
11 Facebook's users, stockholders, or any other person, or instead of complying, causing or failing
12 to act or prevent others from failing to comply or to act to cause Facebook's compliance with
13 applicable laws; (vi) by failing to be reasonably informed about the source of the Company's
14 revenues and the nature of its core advertising business; (vii) by failing to implement policies
15 and procedures for enforcement of any Company policies, or failing to be reasonably informed
16 about the Company's policies and procedures for enforcement, or any Company policies that
17 violated the law or that were not enforced, or any employee actions and activities at the
18 Company that violated the law and complied with any Company policy; (viii) by failing to
19 ensure that the Company was in compliance with any of its duties or obligations of the
20 Company set forth in any agreements with U.S. and foreign governments and any regulators, or
21 by allowing or permitting the Company's policies and any activities or taking of any actions
22 that failed to comply with such duties, obligations, and agreements, including, without
23 limitation, the FTC Consent Decree entered in 2011; and (viii) by failing to monitor and
24 oversee low-level employee misconduct, either by (a) failing to implement a reasonable system
25 of internal controls and reporting procedures designed to detect and prevent wrongdoing; or (b)
26 failing to adequately supervise and monitor the Company's internal controls and reporting
27 systems and taking no action or inadequate action upon receiving red flag warnings of
28 deficiencies in the Company's internal controls or of illegal activity occurring at the Company.

1 494. Defendants, individually and in concert, engaged in the above referenced conduct
2 in intentional, reckless, or grossly negligent breaches of the fiduciary duties they owed to
3 Facebook to protect its rights and interests.

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

10 496. Each of the Defendants deliberately concealed this information for improper
11 purposes and failed to disclose material facts or to correct the Company's public statements as
12 necessary so as to not be misleading, or alternatively, failed to be reasonably informed about
13 the Company's business and failed to fully inform themselves sufficiently when making,
14 signing, and approving public statements and prior to making decisions as directors and
15 officers, either of which is sufficient to render them personally liable to the Company for
16 breaching their fiduciary duties.

17 497. Defendants' actions detailed in this Complaint were not a good-faith exercise of
18 prudent business judgment to protect and promote the Company's corporate interests.

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

21 499. As a result of the misconduct alleged in this Complaint, the Defendants are liable
22 to the Company.

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

28 501. Plaintiffs, as shareholders and representatives of Facebook, seeks restitution from

1 Defendants and seek an order of this Court disgorging all profits, benefits, and other
2 compensation—including any salary, options, performance-based compensation, and stock—
3 obtained by Defendants due to their wrongful conduct alleged in this Complaint.

4 502. Defendants' actions and conduct described herein was not only a breach of their
5 fiduciary duties, but also constitute violations of law for which they are personally liable,
6 separately and apart from their liability for breaches of fiduciary duties owed to Facebook.
7 Although the violations of federal and state statutes are evidence of their breaches of fiduciary
8 duty, and constitute breaches of fiduciary duty, they are based upon violations arising under
9 those federal and state laws, and the claims asserted herein against Defendants for such
10 violations of law are separate from the claims against Defendants for breach of their fiduciary
11 duties, and the Company may recover damages under those statutes that are specifically
12 provided for by those statutes, separately and apart from any recovery for the breach of
13 fiduciary duty claims for which Plaintiffs seek restitution, disgorgement of profits, and other
14 equitable remedies. Any damages that are recoverable under the statutes are for violations of
15 those statutes, for which Defendants are separately liable to the Company, and they provide
16 additional bases for Defendants' liability and the Company may recover damages pursuant to
17 those statutes that are separate from and may not be recoverable by the Company apart from
18 under the statutes for Defendants' breaches of fiduciary duties that caused the violations and
19 are asserted as separate claims by Plaintiffs derivatively on the Company's behalf.

20 **SEVENTH CAUSE OF ACTION**

21 **Contribution and Indemnification**

22 **(Against All Defendants)**

23 503. Plaintiffs incorporate by reference and reallege each of the foregoing allegations
24 as though fully set forth in this paragraph.

25 504. This claim is brought derivatively on behalf of the Company against Defendants
26 for contribution and indemnification.

27 505. Facebook is named as a defendant in a putative shareholder class action filed in
28 this District on March 20, 2018, asserting claims under the federal securities laws for, inter alia,

1 false and misleading statements related to the Company's user privacy practices. In the event
2 the Company is found liable for violating the federal securities laws, the Company's liability
3 will arise, in whole or in part, from the intentional, knowing, or reckless acts or omissions of
4 some or all of the Defendants as alleged herein. The Company is entitled to receive
5 contribution from those Defendants in connection with the securities fraud class action against
6 the Company currently pending in this District.

7 506. Facebook is named as a defendant in other putative class actions filed on behalf
8 of certain Facebook users that have been coordinated in a multidistrict litigation (MDL)
9 proceeding that is pending in this District, asserting claims under various states' laws for, inter
10 alia, violations of privacy. In the event the Company is found liable for violating those laws,
11 the Company's liability will arise, in whole or in part, from the intentional, knowing, or
12 reckless acts or omissions of some or all of the Defendants as alleged herein. The Company is
13 entitled to receive contribution from those Defendants in connection with the class actions filed
14 against the Company in the MDL proceeding currently pending in this District.

15 507. Accordingly, Facebook is entitled to all appropriate contribution or
16 indemnification from Defendants.

17 **EIGHTH CAUSE OF ACTION**

18 **Aiding and Abetting Breaches of Fiduciary Duty**

19 **(Against All Defendants)**

20 508. Plaintiffs incorporate by reference and reallege each of the foregoing allegations
21 as though fully set forth in this paragraph.

22 509. Defendants Zuckerberg, Sandberg, Thiel, Andreessen, Hastings, Koum,
23 Desmond-Hellmann, and Bowles owed and owe fiduciary duties to Facebook and its
24 stockholders, as set forth above.

25 510. Each of the Defendants, Zuckerberg, Sandberg, Thiel, Andreessen, Hastings,
26 Koum, Desmond-Hellmann, and Bowles knows and knew or consciously disregarded that at all
27 relevant times the other Defendants owed fiduciary duties to Facebook.

28 511. Each of the Defendants either personally engaged in or caused by their actions

1 and inactions the wrongful conduct and violations of law which constituted a breach and
2 thereby breached their fiduciary duties as set forth above, or alternatively, they aided and
3 abetted the other Defendants who are Facebook officers, directors, and employees who owed
4 fiduciary duties to Facebook at all relevant times, and who breached their fiduciary duties to
5 Facebook, in their breaches of fiduciary duty as described herein.

6 512. Defendants knowingly assisted, facilitated, and permitted one or more of the
7 other Defendants to engage in or cause by their actions and inactions the wrongful conduct and
8 violations of law which constituted a breach of their fiduciary duties owed to Facebook, as
9 described herein, by their actions and inactions which failed to prevent the other Defendants
10 and Doe Defendants from engaging in the wrongful conduct and their actions or inactions that
11 caused the violations of law, as described herein, and thereby aided and abetted those
12 Defendants and Doe Defendants in breaching their fiduciary duties owed to Facebook,
13 including, without limitation, by: (i) failing to implement a reasonable system of internal
14 controls and reporting procedures designed to detect and prevent wrongdoing at Facebook; (ii)
15 failing to adequately supervise and monitor the Company's internal controls and reporting
16 systems and taking no action or inadequate action upon receiving red flag warnings of
17 deficiencies in the Company's internal controls or of illegal activity occurring at the Company;
18 (iii) failing to exercise reasonable oversight of the Company's illegal business, employee
19 actions and activities at the Company which violated or failed to comply with any of the
20 Company's agreements, obligations, and the law of the U.S. or any state, foreign country, or
21 government and any of their statutes, regulations, and agreements with Facebook setting forth
22 obligations of the Company or that the Company has failed to comply with, including the FTC
23 Consent Decree entered in 2011; (iv) by failing to be reasonably informed about the
24 Company's revenues and the nature of its core advertising business; (v) by implementing and
25 overseeing Facebook's illegal business strategy of pursuing profits and revenue growth through
26 violations of various laws, and conduct which was unethical or was designed to achieve an
27 improper result or for an improper purpose that was not in the Company's best interests; (vi) by
28 suppressing, concealing, and engaging in conduct designed to suppress, conceal, hide, or avoid

1 detection or disclosure of information about any illegal activity or wrongdoing; (vii) by
2 omitting and failing to disclose material information or facts concerning illegal activity or
3 wrongdoing in any public statements, or in connection with any request for information in any
4 investigation, inquiry, or litigation by any government entity or regulator, and in discovery in
5 any civil or criminal litigation; (vi) by consciously permitting, allowing, and encouraging
6 business practices that were unfair and violated the expectations and trust of Facebook's
7 stockholders, users of Facebook's social networking website, smartphone users and users of
8 mobile devices, U.S. citizens, government officials, and the public at large; and (vii) by turning
9 a blind eye to the Company's illegal activity and any persons at the Company who engaged in
10 wrongdoing or any illegal activity, pursued profits or revenue growth, or who obtained any
11 personal financial gain, at the expense of any of Facebook's users, stockholders, or any other
12 person, instead of complying, causing or failing to act or prevent others from failing to comply
13 or to act to cause Facebook's compliance with applicable laws.

14 513. Each of the Defendants knowingly and substantially assisted the other
15 Defendants, by and through their own actions and inactions that allowed, facilitated, or
16 permitted the Defendants to engage in the wrongful acts and conduct that violated various laws
17 and which constituted a breach of their fiduciary duties to Facebook, as described herein.

18 514. Defendants, at all relevant times, were fiduciaries of the Company, and knew that
19 each of the other Defendants are persons who owed and owe fiduciary duties to Facebook and
20 participated, aided, abetted, and substantially assisted in intentional, reckless, or grossly
21 negligent breaches of the fiduciary duties they owed to Facebook to protect its rights and
22 interests. In breach of their fiduciary duties owed to Facebook, the Defendants willfully
23 participated in misrepresentations related to the Company's targeted advertising services,
24 privacy practices, internal controls, and compliance with the FTC Consent Decree and other
25 laws, failed to correct the Company's public statements, and failed to fully inform themselves
26 prior to making decisions as directors and officers, rendering them personally liable to the
27 Company for breaching their fiduciary duties and for aiding and abetting breaches of fiduciary
28 duty by the other Defendants.

- 1 i. a proposal to strengthen Board oversight and supervision of
- 2 Facebook’s data security practices;
- 3 ii. a proposal to strengthen the Company’s disclosure controls to
- 4 ensure material information is adequately and timely disclosed to
- 5 the SEC and the public; and
- 6 iii. a proposal to strengthen the Board’s supervision of operations and
- 7 develop and implement procedures for greater stockholder input into
- 8 the policies and guidelines of the Board;
- 9 E. Extraordinary equitable or injunctive relief as permitted by law or equity, including
- 10 attaching, impounding, imposing a constructive trust on, or otherwise restricting
- 11 Defendants’ assets so as to assure that Plaintiffs, on behalf of Facebook, have an
- 12 effective remedy;
- 13 F. Awarding to Facebook restitution from Defendants, and each of them, and ordering
- 14 disgorgement of all profits, benefits, and other compensation obtained by
- 15 Defendants, including the proceeds of insider transactions made in violation of
- 16 state securities laws;
- 17 G. Declaring that the 2017 and 2018 Proxy Statements contained materially false and
- 18 misleading statements;
- 19 H. Canceling the votes to re-elect the Defendants to the Board in connection with the
- 20 annual shareholder meeting in 2017 and 2018, and ordering Defendants to disgorge
- 21 to the Company all compensation they received for service on the Board following
- 22 the invalid election;
- 23 I. Awarding to Plaintiffs costs and disbursements related to this action, including
- 24 reasonable attorneys’ fees, consultant and expert fees, costs, and expenses; and
- 25 J. Granting such other and further relief as the Court deems just and proper.

JURY DEMAND

Plaintiffs respectfully demands a trial by jury on all issues so triable.

Dated: July 2, 2018

COTCHETT, PITRE & McCARTHY, LLP

/s/ Joseph W. Cotchett

JOSEPH W. COTCHETT

Lead Counsel for Plaintiffs

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

BOTTINI & BOTTINI, INC.
FRANCIS A. BOTTINI
fbottini@bottinilaw.com
YURY A. KOLESNIKOV
ykolesnikov@bottinilaw.com
BOTTINI & BOTTINI, INC.
7817 Ivanhoe Avenue, Suite 102
La Jolla, CA 92037
Telephone: (858) 914-2001
Facsimile: (858) 914-2002

Attorneys for Plaintiff Natalie Ocegueda
BERMAN TABACCO
JOSEPH J. TABACCO, JR. (SBN 75484)
jtabacco@bermantobacco.com
DANIEL E. BARENBAUM (SBN 209261)
dbarenbaum@bermantabacco.com
A. CHOWING POPPLER (SBN 272870)
cpoppler@bermantabacco.com
BERMAN TOBACCO
44 Montgomery Street, Suite 650
San Francisco, CA. 94104
Tel: (415) 433-3200
Fax: (415) 433-6382

Attorneys for Plaintiff Gloria Stricklin Trust

DEREK G. HOWARD LAW FIRM, INC.
DEREK G. HOWARD (SBN 118082)
derek@derekhowardlaw.com
DEREK G. HOWARD LAW FIRM, INC.
42 Miller Avenue
Mill Valley, CA. 94941
Telephone: (415) 432-7192
Facsimile: (415) 524-2419

Attorneys for Plaintiff James Karon

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

STULL, STULL & BRODY
PATRICE L. BISHOP
pbishop@ssbla.com
STULL, STULL & BRODY
9430 W. Olympic Blvd., Suite 400
Beverly Hills, CA. 90212
Telephone: (3310) 209-2468
Facsimile: (310) 209-2087

Attorney for Plaintiff Ronald

JENKINS MULLIGAN & GABRIEL LLP
DANIEL J. MULLIGAN (SBN 103129)
dan@jmglawoffice.com
LARRY W. GABRIEL (SBN 68329)
lgabriel@bg.law
JENKINS MULLIGAN & GABRIEL LLP
10085 Carroll Canyon Road, Suite 210
San Diego, CA. 92131
Telephone: (858) 527-1792
Facsimile: (858) 527-1793

Attorneys for Plaintiff James Karo

EXHIBIT 1

0923184

**UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION**

COMMISSIONERS: **Jon Leibowitz, Chairman**
 J. Thomas Rosch
 Edith Ramirez
 Julie Brill
 Maureen K. Ohlhausen

| | | |
|-------------------------|---|--------------------------|
| |) | |
| <i>In the Matter of</i> |) | |
| |) | |
| |) | DOCKET NO. C-4365 |
| FACEBOOK, INC., |) | |
| <i>a corporation.</i> |) | |
| |) | |

DECISION AND ORDER

The Federal Trade Commission, having initiated an investigation of certain acts and practices of the Respondent named in the caption hereof, and the Respondent having been furnished thereafter with a copy of a draft Complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued, would charge the Respondent with violation of the Federal Trade Commission Act, 15 U.S.C. § 45 *et seq.*;

The Respondent and counsel for the Commission having thereafter executed an Agreement Containing Consent Order (“Consent Agreement”), an admission by the Respondent of all the jurisdictional facts set forth in the aforesaid draft Complaint, a statement that the signing of said Consent Agreement is for settlement purposes only and does not constitute an admission by the Respondent that the law has been violated as alleged in such Complaint, or that the facts as alleged in such Complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission’s Rules; and

The Commission having thereafter considered the matter and having determined that it has reason to believe that the Respondent has violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such Consent Agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, and having carefully considered the comments filed by interested persons, now in further conformity with

the procedure described in Commission Rule 2.34, 16 C.F.R. § 2.34, the Commission hereby issues its Complaint, makes the following jurisdictional findings, and enters the following order:

1. Respondent Facebook, Inc. (“Facebook”) is a Delaware corporation with its principal office or place of business at 1601 Willow Road, Menlo Park, California 94025.
2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondent, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. Unless otherwise specified, “Respondent” shall mean Facebook, its successors and assigns. For purposes of Parts I, II, and III of this order, “Respondent” shall also mean Facebook acting directly, or through any corporation, subsidiary, division, website, or other device.
2. “Commerce” shall be defined as it is defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.
3. “Clear(ly) and prominent(ly)” shall mean:
 - A. in textual communications (*e.g.*, printed publications or words displayed on the screen of a computer or mobile device), the required disclosures are of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts highly with the background on which they appear;
 - B. in communications disseminated orally or through audible means (*e.g.*, radio or streaming audio), the required disclosures are delivered in a volume and cadence sufficient for an ordinary consumer to hear and comprehend them;
 - C. in communications disseminated through video means (*e.g.*, television or streaming video), the required disclosures are in writing in a form consistent with subpart (A) of this definition and shall appear on the screen for a duration sufficient for an ordinary consumer to read and comprehend them, and in the same language as the predominant language that is used in the communication; and
 - D. in all instances, the required disclosures: (1) are presented in an understandable language and syntax; and (2) include nothing contrary to, inconsistent with, or in

mitigation of any statement contained within the disclosure or within any document linked to or referenced therein.

4. “Covered information” shall mean information from or about an individual consumer including, but not limited to: (a) 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.
5. “Nonpublic user information” shall mean covered information that is restricted by one or more privacy setting(s).
6. “Privacy setting” shall include any control or setting provided by Respondent that allows a user to restrict which individuals or entities can access or view covered information.
7. “Representatives” shall mean Respondent’s officers, agents, servants, employees, attorneys, and those persons in active concert or participation with them who receive actual notice of this Order by personal service or otherwise.
8. “Third party” shall mean any individual or entity that uses or receives covered information obtained by or on behalf of Respondent, other than: (1) a service provider of Respondent that (i) uses the covered information for and at the direction of Respondent and no other individual or entity and for no other purpose; and (ii) does not disclose the covered information, or any individually identifiable information derived from such covered information, except for, and at the direction of, Respondent, for the purpose of providing services requested by a user and for no other purpose; or (2) any entity that uses the covered information only as reasonably necessary: (i) to comply with applicable law, regulation, or legal process, (ii) to enforce Respondent’s terms of use, or (iii) to detect, prevent, or mitigate fraud or security vulnerabilities.
9. “User” shall mean an identified individual from whom Respondent has obtained information for the purpose of providing access to Respondent’s products and services.

I.

IT IS ORDERED that Respondent and its representatives, in connection with any product or service, in or affecting commerce, 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:

- A. its collection or disclosure of any covered information;

- B. the extent to which a consumer can control the privacy of any covered information maintained by Respondent and the steps a consumer must take to implement such controls;
- C. the extent to which Respondent makes or has made covered information accessible to third parties;
- D. the steps Respondent takes or has taken to verify the privacy or security protections that any third party provides;
- E. the extent to which Respondent makes or has made covered information accessible to any third party following deletion or termination of a user's account with Respondent or during such time as a user's account is deactivated or suspended; and
- F. the extent to which Respondent 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.

IT IS FURTHER ORDERED that Respondent and its representatives, in connection with any product or service, in or affecting commerce, prior to any sharing of a user's nonpublic user information by Respondent 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," "statement of rights and responsibilities" page, 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 such sharing exceeds the restrictions imposed by the privacy setting(s) in effect for the user; and
- B. obtain the user's affirmative express consent.

Nothing in Part II will (1) limit the applicability of Part I of this order; or (2) require Respondent to obtain affirmative express consent for sharing of a user's nonpublic user information initiated by another user authorized to access such information, provided that such sharing does not materially exceed the restrictions imposed by a user's privacy setting(s). Respondent may seek modification of this Part pursuant to 15 U.S.C. §45(b) and 16 C.F.R. 2.51(b) to address relevant developments that affect compliance with this Part, including, but not limited to, technological changes and changes in methods of obtaining affirmative express consent.

III.

IT IS FURTHER ORDERED that Respondent and its representatives, in connection with any product or service, in or affecting commerce, shall, no later than sixty (60) days after the date of service of this order, implement procedures reasonably designed to ensure that covered information cannot be accessed by any third party from servers under Respondent's control after a reasonable period of time, not to exceed thirty (30) days, from the time that the user has deleted such information or deleted or terminated his or her account, except as required by law or where necessary to protect the Facebook website or its users from fraud or illegal activity. Nothing in this paragraph shall be construed to require Respondent to restrict access to any copy of a user's covered information that has been posted to Respondent's websites or services by a user other than the user who deleted such information or deleted or terminated such account.

IV.

IT IS FURTHER ORDERED that Respondent shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information. Such program, the content and implementation of which must be documented in writing, shall contain controls and procedures appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the covered information, including:

- A. the designation of an employee or employees to coordinate and be responsible for the privacy program.
- B. the identification of reasonably foreseeable, material risks, both internal and external, that could result in Respondent's unauthorized collection, use, or disclosure of covered information and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research.
- C. 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.
- D. 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 Respondent and requiring service providers, by contract, to

implement and maintain appropriate privacy protections for such covered information.

- E. the evaluation and adjustment of Respondent's privacy program in light of the results of the testing and monitoring required by subpart C, any material changes to Respondent's operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have a material impact on the effectiveness of its privacy program.

V.

IT IS FURTHER ORDERED that, in connection with its compliance with Part IV of this order, Respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. A person qualified to prepare such Assessments shall have a minimum of three (3) years of experience in the field of privacy and data protection. All persons selected to conduct such Assessments and prepare such reports shall be approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, in his or her sole discretion. Any decision not to approve a person selected to conduct such Assessments shall be accompanied by a writing setting forth in detail the reasons for denying such approval. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

- A. set forth the specific privacy controls that Respondent has implemented and maintained during the reporting period;
- B. explain how such privacy controls are appropriate to Respondent's size and complexity, the nature and scope of Respondent'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.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by Respondent until the order is

terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

VI.

IT IS FURTHER ORDERED that Respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of:

- A. for a period of three (3) years from the date of preparation or dissemination, whichever is later, all widely disseminated statements by Respondent or its representatives that describe the extent to which Respondent maintains and protects the privacy, security, and confidentiality of any covered information, including, but not limited to, any statement related to a change in any website or service controlled by Respondent that relates to the privacy of such information, along with all materials relied upon in making such statements, and a copy of each materially different privacy setting made available to users;
- B. for a period of six (6) months from the date received, all consumer complaints directed at Respondent or forwarded to Respondent by a third party, that relate to the conduct prohibited by this order and any responses to such complaints;
- C. for a period of five (5) years from the date received, any documents, prepared by or on behalf of Respondent, that contradict, qualify, or call into question Respondent's compliance with this order;
- D. for a period of three (3) years from the date of preparation or dissemination, whichever is later, each materially different document relating to Respondent's attempt to obtain the consent of users referred to in 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 Respondent has attempted to obtain and/or been required to obtain such consent; and
- E. 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 Respondent, 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.

IT IS FURTHER ORDERED that Respondent 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 structure set forth in Part VIII. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VIII, delivery shall be at least ten (10) days prior to the change in structure.

VIII.

IT IS FURTHER ORDERED that Respondent shall notify the Commission within fourteen (14) days of any change in Respondent that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of Facebook, Inc.*, FTC File No.[]. *Provided, however*, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

IX.

IT IS FURTHER ORDERED that Respondent, within ninety (90) days after the date of service of this order, 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, Respondent shall submit additional true and accurate written reports.

X.

This order will terminate on July 27, 2032, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. any Part of this order that terminates in fewer than twenty (20) years; and
- B. this order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that Respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that this order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission, Commissioner Rosch dissenting and Commissioner Ohlhausen not participating.

Donald S. Clark
Secretary

SEAL
ISSUED: July 27, 2012

EXHIBIT 2

Digital, Culture, Media and Sport Committee

House of Commons, London SW1A 0AA
Tel 020 7219 6120 website www.parliament.uk/cms

Rebecca Stimson
Head of Public Policy
Facebook UK
1 Rathbone Place
London W1T 1FB

1 May 2018

Dear Ms Stimson

Oral evidence from Facebook

Thank you for helping to arrange Mike Schroepfer's appearance in front of the Committee yesterday. As you may have seen from my press statement, the Committee feels that the evidence lacked many of the important details that we need. We therefore re-state our invitation to Mark Zuckerberg. Following reports that he will be giving evidence to the European Parliament in May, we would like Mr Zuckerberg to come to London during his European trip. We would like the session here to take place by 24 May.

It is worth noting that, while Mr Zuckerberg does not normally come under the jurisdiction of the UK Parliament, he will do so the next time he enters the country. We hope that he will respond positively to our request, but if not the Committee will resolve to issue a formal summons for him to appear when he is next in the UK.

Mr Schroepfer failed to answer fully on nearly 40 separate points. This is especially disappointing to the Committee considering that in his testimony to Congress Mark Zuckerberg also failed to give convincing answers to some questions. Mr Schroepfer agreed that his team would follow up on the questions included below. For clarity, we include a list of the questions below, and attach a transcript of yesterday's session to this letter. We would like the replies by 11 May so that we can factor the answers into planning for the evidence we hope to take from Mr Zuckerberg a fortnight later.

As I said yesterday, there are over 40 million Facebook users in the UK and they deserve to hear accurate answers from the company he created and whether it is able to keep their users' data safe. We look forward to receiving your answers by 11 May. We would like confirmation of Mr Zuckerberg's attendance by the same date.

Yours sincerely,



DAMIAN COLLINS MP

CHAIR, DCMS COMMITTEE

Unanswered questions/points for follow up from Mike Schroepfer

1. What is the percentage of sites on the internet on which Facebook tracks users?
2. Did the Internet Research Agency use custom audiences? What targeting tools did the IRA use for their advertising? Did they have a custom audience for state-by-state campaigns/races in the USA? Did they use look-alike audiences from Facebook as part of their advertising spend?
3. What is Facebook's definition of a political advertisement? What budget does Facebook put behind examining the parameters and use of political adverts?
4. How many developers did your enforcement team at Facebook take action against between 2011-2014?
5. Does the NDA signed with Dr Kogan prevent legal action being taken? What was the date of the agreement? Was there a payment made to Dr Kogan? [NB later in the session Mr Schroepfer said that a) the date was June 2016 and that b) no payment was made, but it would be useful to have these points confirmed in writing. Confirmation was given in the session that the full NDA document would be provided to the Committee.]
6. Who was the person at Facebook responsible for the decision not to tell users affected in 2015?
7. Who at Facebook heads up the investigation into Cambridge Analytica, including all the strands of the investigation?
8. Has Joseph Chancellor signed an NDA?
9. Agreement to provide documentation that Cambridge Analytica had certified the deletion of the data.
10. What was the number of paid adverts from the IRA during the US election?
11. From which country did the \$2million that AIQ spent on ads come?
12. How many UK Facebook users and Instagram users were contacted by non-UK entities during the EU referendum?
13. How many clicks or swipes does it take to alter your Facebook privacy settings on a smartphone? What steps are you taking to reduce the lengthy process of changing one's privacy settings?
14. What proportion of political campaigning ads globally are run on your platform? Do you have a rough estimate, based on average political campaign spend data?
15. What data on dark ads do you have?
16. Is it possible for Facebook to view pages set up during elections (e.g. the EU Referendum campaign) that host dark ads, and then are taken down a day later? Is it possible that no-one would ever be able to audit these dark ads, as no one (not even Facebook) would see them during the time they are online?
17. Was there any link between the US elections and the 2017 purge of fake accounts?

18. What proportion of the fake accounts you purged had any involvement from Russia?
19. Do you know how many developers were using and selling data on to third parties such as GSR? Is GSR the only company that has received letters from Facebook, demanding that they delete their Facebook data?
20. What kind of developer activity leading up to 2014 led to Facebook's major policy changes related to sharing friends' data? (Please give specific examples.) Were these changes responding to genuine concerns among Facebook users?
21. How many Facebook staff have been added to the app review team since 2014?
22. What is the legal situation regarding Facebook storing non-Facebook users' data?
23. Did Facebook pass user information to Cambridge Analytica or to Aleksandr Kogan?
24. At the 8 February evidence session, Chris Matheson asked Simon Milner, "Have you ever passed any user information over to Cambridge Analytica or any of its associated companies?" Simon Milner replied "No". Chris Matheson asked, "But they do hold a large chunk of Facebook's user data, don't they?" Simon Milner said, "No. They may have lots of data, but it will not be Facebook user data. It may be data about people who are on Facebook that they have gathered themselves, but it is not data that we have provided." [Qq 447-448] Do you agree with this answer?
25. At the time of Simon Milner's testimony in February 2018, who at Facebook knew about Cambridge Analytica? Who was in charge?
26. When did Mark Zuckerberg know about Cambridge Analytica?
27. Can you tell us about the financial links between SCL and Cambridge Analytica? (In evidence Mr Schroepfer said he had knowledge to share about this.)
28. How much money has been made from fraudulent ads (for example - but not limited to - the recent case of financial expert Martin Lewis?) When you find out they have been fraudulent, do you return the money to the purchaser of the ads?
29. Can we see copies of adverts from AIQ? Who saw these adverts shown to? Who paid for them?
30. Why wasn't GSR identified during audits of third party developers?
31. How can the feature allowing users to edit previews of article (in response to concerns over Fake News) be removed?
32. What work is Joseph Chancellor doing right now for Facebook? What is his job title? Was Facebook aware of Joseph Chancellor's involvement in GSR at the time of his application to the company, or during his employment?
33. Mr Schroepfer said that recruitment is taking place to boost work being done in Myanmar. When is this happening and can you provide more details?
34. What is the average time taken to respond to content that has been reported to Facebook in the region?
35. How many fake accounts have been identified and removed in Myanmar?
36. How much of your revenue is derived from Myanmar?

37. Are custom audiences used as a tool by AIQ using the GSR data from the US? What was the total value of AIQ/Vote Leave spend on Facebook? Can we see examples and copies of adverts that they used? To whom were they sent, and who decided what kind of targeting to use?
38. Is there evidence that CA/SCL shared data with AIQ?
39. Why was data responsibility moved from Facebook Irl to Facebook Inc in California just one month before GDPR kicks in?

EXHIBIT 3



United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Mike Swift
MLex Market Intelligence
324 Metzgar Street
Half Moon Bay, CA 94019

FEB 13 2013

Re: FOIA-2013-00197
Facebook

Dear Mr. Swift:

This is in response to your request dated November 28, 2012 under the Freedom of Information Act seeking access to documents regarding the 90-day Facebook compliance report. In accordance with the FOIA and agency policy, we have searched our records, as of November 28, 2012, the date we received your request in our FOIA office. We have located the responsive record which is granted in full and is enclosed.

If you are not satisfied with this response to your request, you may appeal by writing to Freedom of Information Act Appeal, Office of the General Counsel, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington D.C. 20580 or by facsimile at (202) 326-2477, within 30 days of the date of this letter. Please enclose a copy of your original request and a copy of this response.

If you have any questions about the way we are handling your request or about the FOIA regulations or procedures, please contact Elena Vera at (202) 326-3368.

Sincerely,

A handwritten signature in blue ink, appearing to read "Dione J. Stearns".

Dione J. Stearns
Assistant General Counsel

Enclosed:
15 pages

facebook

Submitted to: Debrief@ftc.gov

Associate Director of Enforcement
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, D.C. 20580

November 13, 2012

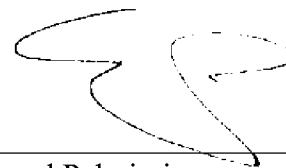
Re: In the Matter of Facebook, Inc., FTC Docket No. C-4365

To the Associate Director of Enforcement:

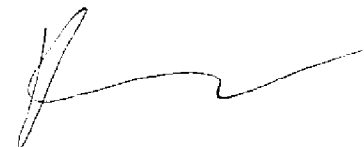
Facebook Inc. ("Facebook") submits the attached Report pursuant to Part IX of the Decision and Order, served on Facebook on August 15, 2012 (the "Order"). The Report describes the manner and form in which Facebook is in compliance with the Order. The Report follows the outline of the Order paragraph by paragraph.

Please do not hesitate to contact us if you have any questions.

Sincerely,



Edward Palmieri
Associate General Counsel, Privacy
Facebook, Inc.



Daniel Li
Product Counsel
Facebook, Inc.

In the Matter of Facebook, Inc., FTC Docket No. C-4365

Public

Page 1 of 14

| | | |
|-------------------------|---|-------------------|
| |) | |
| <i>In the Matter of</i> |) | |
| |) | |
| FACEBOOK, INC., |) | DOCKET NO. C-4365 |
| <i>a corporation.</i> |) | |
| |) | |
| |) | |

Facebook Compliance Report

This report (this “Report”) sets forth the manner and form in which Facebook, Inc. (“Facebook”) is in compliance with the Decision and Order, served on Facebook on August 15, 2012 (the “Order”). This Report is prepared and filed with the Federal Trade Commission (the “Commission”) pursuant to Part IX of the Order. This Report follows the outline of the Order paragraph by paragraph.

I.

Respondent and its representatives, in connection with any product or service, in or affecting commerce, 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:

- A. its collection or disclosure of any covered information;
- B. the extent to which a consumer can control the privacy of any covered information maintained by Respondent and the steps a consumer must take to implement such controls;
- C. the extent to which Respondent makes or has made covered information accessible to third parties;
- D. the steps Respondent takes or has taken to verify the privacy or security protections that any third party provides;
- E. the extent to which Respondent makes or has made covered information accessible to any third party following deletion or termination of a user’s account with Respondent or during such time as a user’s account is deactivated or suspended; and
- F. the extent to which Respondent 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.

Facebook describes the extent to which it maintains the privacy and security of covered information in its Data Use Policy (the “Data Use Policy”), available at https://www.facebook.com/full_data_use_policy. The Data Use Policy is drafted in a layered, web-like format, which makes its description of Facebook’s data collection and disclosure practices easy to navigate. It is drafted in plain and simple language, conspicuously labeled, and formatted in a font that is easily read. It is available in many of the languages used by the

In the Matter of Facebook, Inc., FTC Docket No. C-4365

Public

Page 2 of 14

people who access and share on Facebook.

The Data Use Policy addresses the following topics: 1) Information Facebook receives and how the information is used; 2) Sharing and finding users on Facebook; 3) Other websites and applications; 4) How advertising and sponsored stories work; 5) Cookies, pixels, and other system technologies; and 6) Some other things users need to know. Facebook has designated a member of its Legal team to be responsible for maintaining the Data Use Policy.

Facebook's Data Use Policy was last updated on June 8, 2012. The date of the last revision is clearly provided at the beginning of the Data Use Policy so that a user can determine whether the Data Use Policy has changed since the user's last review of the Data Use Policy.

Facebook's comprehensive privacy program, described in Part IV of this Report (the "Privacy Program"), is reasonably designed to ensure that Facebook does not misrepresent the extent to which it maintains the privacy or security of covered information as set forth in Section I of the Order.

Specifically, as part of the Privacy Program, Facebook built an extensive privacy review process that is supervised and monitored by, among others, Facebook's Chief Privacy Officer, Policy and Facebook's Chief Privacy Officer, Product. This process is designed to integrate a detailed and multi-faceted privacy review into the early development stages of a new product or material product upgrade and to continue that review throughout the product's life cycle. This ongoing privacy review is designed to conform newly released and existing products with the Data Use Policy and other Facebook representations and to revise Facebook's user-facing statements as necessary to reflect the evolution of its products and ecosystem. The privacy review process involves comprehensive review by a cross-functional team of Facebook employees that includes representatives from major segments of Facebook, including Facebook's Privacy, Public Policy, Legal, Marketing, Product, Engineering, Security, and Communications teams (the "Privacy Cross-Functional Team"). The Privacy Cross-Functional Team reviews Facebook products, services, policies, and related disclosures.

In addition, as part of the Privacy Program, Facebook is implementing comprehensive privacy training for all Facebook employees to augment existing group-specific training (e.g., privacy training for new Product Managers), with the goal of educating all Facebook employees about Facebook's privacy policies and representation obligations. Facebook also has dedicated personnel in its Legal department who focus on spotting, vetting, and addressing privacy issues and disclosures.

Facebook has been careful to detail changes in the manner it shares information, even with respect to information that is outside the scope of the Order. For example, on September 30, 2012, Facebook's Privacy Engineer published a blog post titled "Relevant Ads That Protect Your Privacy" concerning targeted advertising, which comprehensively addressed changes in the way Facebook targets ads to users. The blog post is available at <https://www.facebook.com/notes/facebook-and-privacy/relevant-ads-that-protect-your-privacy/457827624267125>. In addition, Facebook recently added privacy education to its new user experience, with the aim of educating Facebook users about how privacy works on Facebook.

In the Matter of Facebook, Inc., FTC Docket No. C-4365

Public

Page 3 of 14

II.

Respondent and its representatives, in connection with any product or service, in or affecting commerce, prior to any sharing of a user’s nonpublic user information by Respondent 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,” “statement of rights and responsibilities” page, 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 such sharing exceeds the restrictions imposed by the privacy setting(s) in effect for the user; and**
- B. obtain the user’s affirmative express consent.**

Nothing in Part II will (1) limit the applicability of Part I of this order; or (2) require Respondent to obtain affirmative express consent for sharing of a user’s nonpublic user information initiated by another user authorized to access such information, provided that such sharing does not materially exceed the restrictions imposed by a user’s privacy setting(s). Respondent may seek modification of this Part pursuant to 15 U.S.C. § 45(b) and 16 C.F.R. 2.51(b) to address relevant developments that affect compliance with this Part, including, but not limited to, technological changes and changes in methods of obtaining affirmative express consent.

Facebook’s Privacy Program is designed in part to identify changes that fall under the scope of Part II of the Order and to implement the disclosure and consent requirements of Part II of the Order, where applicable. The specific policies and procedures mentioned in Part I of this Report and described in more detail in Part IV of this Report—including compliance oversight by Facebook’s two Chief Privacy Officers, review of developing products and services by the Privacy Cross-Functional Team, new and continuing employee training, and dedicated privacy-focused Legal personnel—all contribute to identifying new or changed products or services that may trigger the disclosure and consent requirements of Part II of the Order. The Privacy Cross-Functional Team plays a central role in discussing and providing recommendations to the Chief Privacy Officers with respect to whether the disclosure and consent requirement of Part II of the Order may be triggered by a particular product or change.

In addition, to help communicate the requirements in Part II of the Order, Facebook has distributed a copy of the Order to all Facebook employees and has implemented a global process to similarly distribute the Order to all new employees—steps that go beyond the requirements of Part VII of the Order.

Facebook continues to monitor and evaluate proposed changes (if any) to users’ privacy settings to ensure compliance with Part II of the Order.

III.

In the Matter of Facebook, Inc., FTC Docket No. C-4365

Public

Page 4 of 14

Respondent and its representatives, in connection with any product or service, in or affecting commerce, shall, no later than sixty (60) days after the date of service of this order, implement procedures reasonably designed to ensure that covered information cannot be accessed by any third party from servers under Respondent's control after a reasonable period of time, not to exceed thirty (30) days, from the time that the user has deleted such information or deleted or terminated his or her account, except as required by law or where necessary to protect the Facebook website or its users from fraud or illegal activity. Nothing in this paragraph shall be construed to require Respondent to restrict access to any copy of a user's covered information that has been posted to Respondent's websites or services by a user other than the user who deleted such information or deleted or terminated such account.

Facebook has implemented procedures to comply with Part III of the Order. Specifically, Facebook has implemented a Data Deletion and Retention Framework (the "Data Deletion and Retention Framework"), which outlines the retention period for specific types of data, in all cases in compliance with Part III of the Order. Facebook has also undertaken a historical deletions project, which covers content created prior to implementation of the Data Deletion and Retention Framework. The Data Deletion and Retention Framework ensures that when a user deletes his or her Facebook account, the appropriate user data associated with that account is deleted (subject to any legal obligation to retain data). It also ensures that when a user deletes content, the appropriate content is deleted from Facebook's permanent data stores within a reasonable period of time. The Data Deletion and Retention Framework goes beyond the requirements of Part III of the Order, which focuses only on accessibility by third parties, rather than deletion.

Part III of the Order was a response to reports that some images stored on one of Facebook's old photo storage systems remained accessible after users had deleted the images, where users had retained a unique URL associated with the image. Facebook addressed this issue earlier this year by migrating all of its stored photos to a new storage system ("Haystack"¹) and decommissioning the old photo storage system. Facebook completed the migration to Haystack in July 2012. Haystack controls access to all photos that are served to content delivery networks. It ensures that each photo that is delivered to a content delivery network has a lifespan of 30 days or less. When a photo is deleted by a user, Facebook refuses to provide the photo to any content delivery network that requests it after the moment of deletion. The system is thus designed to ensure that, once the lifespan of the photo expires, it will not be visible via any content delivery network that received the photo previously.

With respect to other covered information, Facebook has comprehensive procedures for deleting information that has been deleted by users and ensuring that it cannot be accessed by third parties from servers under Facebook's control after a reasonable period of time. In addition, Facebook has implemented controls to ensure that any issues that arise with respect to data deletion are identified and addressed.

Facebook has a comprehensive, reliable system for deleting accounts that users have

¹ See Peter Vajgel, *Needle in a Haystack: Efficient Storage of Billions of Photos*, FACEBOOK, April 30, 2009, https://www.facebook.com/note.php?note_id=76191543919.

In the Matter of Facebook, Inc., FTC Docket No. C-4365

Public

Page 5 of 14

terminated. Facebook performs systematic checks on deleted accounts to ensure that its Data Deletion and Retention Framework is operating properly, and it escalates any issues to the appropriate teams.

Facebook's Engineering teams are responsible for building and maintaining the core systems that comprise the Data Deletion and Retention Framework. Any identified issues are raised to Facebook's Security Infrastructure personnel.

IV.

Respondent shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information. Such program, the content and implementation of which must be documented in writing, shall contain controls and procedures appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the covered information, including:

Facebook has taken extensive steps to establish, implement, and maintain the Privacy Program, which is documented in written policies and procedures. Facebook has selected the AICPA and CICA Generally Accepted Privacy Principles ("GAPP") framework as the foundation for its Privacy Program and supporting controls. There are 10 GAPP principles, which are derived from internationally recognized information practices and privacy laws and regulations from around the world. The 10 GAPP principles are:

1. Management. The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.
2. Notice. The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
3. Choice and consent. The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
4. Collection. The entity collects personal information only for the purposes identified in the notice.
5. Use, retention, and disposal. The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.
6. Access. The entity provides individuals with access to their personal information for review and update.

In the Matter of Facebook, Inc., FTC Docket No. C-4365

Public

Page 6 of 14

7. Disclosure to third parties. The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.

8. Security for privacy. The entity protects personal information against unauthorized access (both physical and logical).

9. Quality. The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.

10. Monitoring and enforcement. The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related complaints and disputes.²

In March 2012, Facebook engaged a professional services firm to assess Facebook's Privacy Program against the GAPP framework and provide observations and recommendations for future enhancement of Facebook's Privacy Program.

A. the designation of an employee or employees to coordinate and be responsible for the privacy program.

Facebook has designated specific employees to coordinate and be responsible for the Privacy Program, which is led by the Chief Privacy Officer, Product. Key stakeholders in the Privacy Program include the Chief Privacy Officer, Product; the Chief Privacy Officer, Policy; two Associate General Counsels, Privacy; Regulatory Counsel; and the Chief Security Officer (the "Privacy Governance Team").

While the Chief Privacy Officer, Product provides leadership responsibility for coordinating the Privacy Program, the Privacy Governance Team and many employees are responsible for various aspects of—and are integral to—the Privacy Program. Facebook's Chief Privacy Officer, Product and his team are integrated into the product development process and lead Facebook's commitment to build privacy into its products at an early stage of development. The Privacy Cross-Functional Team meets weekly to review all new products and product changes documented by the Chief Privacy Officer, Product and his team. Members of the Privacy Cross-Functional Team also engage in ongoing review efforts independent of the weekly meetings.

In addition, Facebook's Legal team includes a number of attorneys who serve as primary legal counsel for new products and services. These attorneys are responsible for ensuring that any new or revised products or services are consistent with Facebook's disclosures and comply with applicable legal requirements. These attorneys also support the Privacy Cross-Functional Team and participate in the Privacy Program.

Under the Privacy Program, Facebook considers privacy at all stages of the product cycle and empowers Facebook employees to take ownership over privacy issues, under the leadership

² AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS, INC. AND CANADIAN INSTITUTE OF CHARTERED ACCOUNTANTS, GENERALLY ACCEPTED PRIVACY PRINCIPLES 7 (2009).

In the Matter of Facebook, Inc., FTC Docket No. C-4365

Public

Page 7 of 14

of the Privacy Governance Team.

- B. the identification of reasonably foreseeable, material risks, both internal and external, that could result in Respondent's unauthorized collection, use, or disclosure of covered information and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research.**

A subgroup of the Privacy Governance Team has worked to evaluate Facebook's privacy risks. That process has resulted in a privacy risk assessment and an ongoing process aimed at identifying reasonably foreseeable, material risks, both internal and external. As part of Facebook's privacy risk assessment process, members of Facebook's Legal team interviewed relevant Facebook stakeholders, including representatives of Facebook's Privacy, Engineering, Security, Internal Audit, Legal, Finance, Platform Operations, and User Operations teams. This process identified key internal and external risks that could result in the unauthorized collection, use, or disclosure of covered information.

The discussions considered risks in each relevant area of operation, including governance, product design and engineering (including product development and research), user operations (including third-party developers), advertisers, service providers, employee training and management (including training on the requirements of the Order), and security. The discussions also included an assessment of the sufficiency of the controls in place to control the identified risks. Facebook leveraged previous audits and assessments to identify possible areas of risk exposure, as well as existing controls that help to mitigate the identified risks. Based on this process, Facebook documented its risk assessment and mapped its existing privacy controls to the GAPP framework, as described in more detail below in Part IV.C of this Report.

As part of Facebook's privacy risk assessment process, Facebook will hold an annual "Privacy Summit" of relevant stakeholders, including key representatives from the Privacy Cross-Functional Team. The attendees of the annual Privacy Summit will review and update the privacy risk assessment, which will include evaluating privacy risks in light of changing internal and external risks, changes in operations, and changes in laws and regulations. They will also consider the sufficiency of existing controls in mitigating identified risks and will project forward over the upcoming year to forecast new potential privacy risks. The privacy risk assessment will be updated as a result of any new or revised risks identified at the Privacy Summit. Any control recommendations will be escalated as appropriate. The next Privacy Summit is currently scheduled for January 2012.

In the Matter of Facebook, Inc., FTC Docket No. C-4365

Public

Page 8 of 14

C. 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.

Facebook has performed a granular mapping of its existing privacy controls to the GAPP framework. Facebook assessed each GAPP criteria to determine if the controls in place adequately controlled for the associated risks; it identified certain controls that had room for enhancement; and it implemented remediation plans with respect to those controls.

These processes resulted in the documentation of a mapping of Facebook's controls to the GAPP framework, along with the status of each control. Facebook has implemented remediation steps for the majority of controls where remediation was recommended, and is in the process of implementing remediation steps for a small number of remaining controls. Facebook will continue to refine and implement reasonable controls and procedures to address identified privacy risks on an ongoing basis and will regularly monitor the effectiveness of its controls and procedures.

In order to ensure that the effectiveness of its controls and procedures are regularly monitored, Facebook has designated an "owner" for each one of the controls included in the Privacy Program. Facebook will also utilize the annual Privacy Summit to monitor the effectiveness of controls and procedures in light of changing internal and external risks. In addition, a member of Facebook's Legal team will perform an annual review of the Privacy Program to ensure that the Privacy Program, including the controls and procedures contained therein, remains effective. This Legal team member will update the Privacy Program to reflect any changes or updates communicated by employees of Facebook. This member of the Legal team also serves as the point of contact for all control "owners." The control owners reach out to the Legal point of contact with issues or updates to their respective controls.

Privacy Training

Facebook conducts privacy-related training and is in the process of implementing a comprehensive training program to further extend the audience and topics covered and to further promote recognition and understanding of privacy issues among Facebook employees, including awareness of Facebook's obligations under the Order. All new employees will be required to undergo privacy training within 30 days of their first day of employment at Facebook. All existing Facebook employees will be required to refresh the privacy training on an annual basis. At the time of the annual privacy training, Facebook employees will be required to confirm their understanding of Facebook's privacy practices. Facebook has devoted considerable resources to its employee training program, including engaging an external firm that has expertise in delivering high-impact content.

Facebook has already delivered a copy of the Order to all existing employees and has established a process to similarly distribute the Order to all new employees. Employees are encouraged to review the Order and to direct any questions to a point of

In the Matter of Facebook, Inc., FTC Docket No. C-4365

Public

Page 9 of 14

contact in the Legal team.

Product Design, Development, and Research

Facebook has designed its product-review process to enable the Privacy Cross-Functional Team to consider privacy from the earliest stages in the product development process. The Chief Privacy Officer, Product and his team spearhead this review and lead a number of key functions and responsibilities. First, they educate employees, including Engineers, Product Managers, Content Strategists, and Product Marketing Managers, on Facebook's privacy framework. This includes an overview of Facebook's processes and corresponding legal obligations, and may involve other members of the Privacy Cross-Functional team, such as Privacy Counsel.

Second, the Chief Privacy Officer, Product and his team host weekly reviews of key product-related privacy decisions and material changes to Facebook's privacy framework, which are attended by members of the Privacy Cross-Functional Team. The Chief Privacy Officer, Product and his team also review all new products and material product changes from a privacy perspective and involve the Privacy Cross Functional Team for broader review and feedback. Product launches are added to the launch calendar to ensure review and consideration of privacy issues by the Privacy Cross-Functional Team. Members of the Privacy Cross-Functional Team also communicate back to their respective teams on issues covered in the weekly reviews. The goal of this process is to ensure that privacy is considered throughout the product development process, and to maintain consistency on privacy issues across all Facebook products and services.

D. 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 Respondent and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information.

Where appropriate, Facebook has implemented controls with respect to service providers, including implementing policies to select and retain service providers capable of appropriately protecting the privacy of covered information received from Facebook.

Facebook's Security team has a process for conducting due diligence on service providers who may receive covered information, in order to evaluate whether the service providers' data security standards are in-line with Facebook's commitments to protect covered information. As part of the due diligence process, Facebook may ask prospective service providers to complete a security architecture questionnaire to assess whether the provider meets Facebook's functional security requirements. The process can also involve Facebook sending potential service providers a vendor security questionnaire that provides Facebook with detailed information on the service provider's security posture, including information on protecting the privacy of customer data. Based upon the service provider's responses to the vendor security questionnaire and other data points, Facebook's Security team determines whether further security auditing may be required.

In the Matter of Facebook, Inc., FTC Docket No. C-4365

Public

Page 10 of 14

When the Security team determines further auditing is required, Facebook partners with an outside security consulting firm to conduct a security audit on the potential service provider in order to determine whether the service provider meets Facebook's security requirements. Depending on the particular service provider, this audit may include testing of the service provider's controls, a vulnerability scanning program, a web application penetration test, and/or a code review for security defects. The security consulting firm then reports its findings to Facebook, and Facebook requires service providers to fix critical issues before the service provider is on-boarded. Once the issues are fixed, Facebook Security may ask the security consulting firm to re-test the service provider to make sure the identified issues were resolved according to Facebook's standards.

Depending upon the nature of Facebook data shared with the service provider and other factors, Facebook may require the service provider to undergo a periodic security audit. Facebook also conducts random security audits (logical, network, and/or physical) on selected service providers to assess their compliance with Facebook's security guidelines.

Additionally, in January 2012, Facebook implemented a contract policy (the "Contract Policy"), which governs the review, approval, and execution of contracts for Facebook. It is designed to provide an effective means for establishing contracts while maintaining appropriate internal controls and managing risks associated with entering into and amending contracts. Among other things, the Contract Policy specifies that Facebook contracts must comply with applicable Facebook policies.

The Contract Policy communicates Facebook's preference to enter into contracts on its pre-approved standard contract templates. Facebook's pre-approved contract templates require service providers to implement and maintain appropriate protections for covered information. Facebook reviews contracts that deviate from the pre-approved templates to help ensure that contracts with applicable service providers contain the required privacy protections. Facebook Legal evidences review of any such contracts through formal approval prior to contract execution.

E. the evaluation and adjustment of Respondent's privacy program in light of the results of the testing and monitoring required by subpart C, any material changes to Respondent's operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have a material impact on the effectiveness of its privacy program.

Facebook's Privacy Program is designed with procedures for evaluating and adjusting the Privacy Program in light of the results of testing and monitoring of the program as well as other relevant circumstances. Facebook's annual Privacy Summit is designed to identify, discuss, and assess compliance with privacy policies and procedures, and applicable laws and regulations, as well as identify new or changed risks and recommend responsive controls. The Privacy Program will be adjusted based upon the recommendations derived from the Privacy Summit. The Privacy Summit is attended by relevant stakeholders, which ensures that input is received from appropriate teams throughout Facebook.

In the Matter of Facebook, Inc., FTC Docket No. C-4365

Public

Page 11 of 14

In addition, a member of Facebook's Legal team maintains the Privacy Program and serves as a point of contact for all "owners" of the controls that are currently in place. Such "owners" communicate to the Legal point of contact any recommended adjustments to the Privacy Program based upon their regular monitoring, as well as any internal or external changes that affect the controls in question. The point of contact from Facebook's Legal team adjusts the Privacy Program on an annual basis based upon such input. The Privacy Cross-Functional Team also assesses risks and controls on an on-going basis through weekly meetings and review processes. Any recommendations for adjustments to the Privacy Program are raised to the point of contact in the Legal team.

V.

In connection with its compliance with Part IV of this order, Respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. A person qualified to prepare such Assessments shall have a minimum of three (3) years of experience in the field of privacy and data protection. All persons selected to conduct such Assessments and prepare such reports shall be approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, in his or her sole discretion. Any decision not to approve a person selected to conduct such Assessments shall be accompanied by a writing setting forth in detail the reasons for denying such approval. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

- A. set forth the specific privacy controls that Respondent has implemented and maintained during the reporting period;**
- B. explain how such privacy controls are appropriate to Respondent's size and complexity, the nature and scope of Respondent'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.**

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by Respondent until the order is terminated and provided to the Associate

In the Matter of Facebook, Inc., FTC Docket No. C-4365

Public

Page 12 of 14

Director of Enforcement within ten (10) days of request.

Facebook is in the process of selecting a qualified third-party professional to prepare the Assessments required by Part V of the Order, which Facebook will identify to the Associate Director for Enforcement for approval, in accordance with Part V of the Order.

VI.

Respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of:

- A. for a period of three (3) years from the date of preparation or dissemination, whichever is later, all widely disseminated statements by Respondent or its representatives that describe the extent to which Respondent maintains and protects the privacy, security, and confidentiality of any covered information, including, but not limited to, any statement related to a change in any website or service controlled by Respondent that relates to the privacy of such information, along with all materials relied upon in making such statements, and a copy of each materially different privacy setting made available to users;**

Facebook maintains and will make available to the Commission the enumerated statements, materials and documents in Part VI.A of the Order upon request, so long as such documents are responsive and non-privileged.

- B. for a period of six (6) months from the date received, all consumer complaints directed at Respondent or forwarded to Respondent by a third party, that relate to the conduct prohibited by this order and any responses to such complaints;**

Facebook maintains and will make available to the Commission the enumerated statements, materials, and documents in Part VI.B of the Order upon request, so long as such documents are responsive and non-privileged.

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

Facebook maintains and will make available to the Commission the enumerated statements, materials, and documents in Part VI.C of the Order upon request, so long as such documents are responsive and non-privileged.

- D. for a period of three (3) years from the date of preparation or dissemination, whichever is later, each materially different document relating to Respondent's attempt to obtain the consent of users referred to in 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**

In the Matter of Facebook, Inc., FTC Docket No. C-4365

Public

Page 13 of 14

number of users for whom each such privacy setting was in effect at any time Respondent has attempted to obtain and/or been required to obtain such consent; and

Facebook shall maintain and will make available to the Commission the enumerated statements, materials, and documents in Part VI.D of the Order upon request, so long as such documents are responsive and non-privileged.

- E. 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 Respondent, 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.**

Facebook shall maintain and will make available to the Commission the enumerated statements, materials, and documents in Part VI.E of the Order upon request, so long as such documents are responsive and non-privileged.

VII.

Respondent 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 structure set forth in Part VIII. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VIII, delivery shall be at least ten (10) days prior to the change in structure.

On September 12, 2012, Facebook timely delivered a copy of the Order to all Facebook employees—not just the Facebook employees indicated in Part VII of the Order. Separate delivery of the order was made the same day to each member of Facebook’s Board of Directors. In addition, Facebook has established a process to similarly distribute the Order to all new employees. Employees are encouraged to review the Order and to direct any questions to a point of contact in the Legal team.

VIII.

Respondent shall notify the Commission within fourteen (14) days of any change in Respondent that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. Unless otherwise directed by a representative of the Commission, all notices required by this Part

In the Matter of Facebook, Inc., FTC Docket No. C-4365

Public

Page 14 of 14

shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of Facebook, Inc.*, Commission File No.[]. *Provided, however*, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@Commission.gov.

Facebook shall notify the Commission, in accordance with Part VIII of the Order, should any of the triggering events described in Part VIII occur.

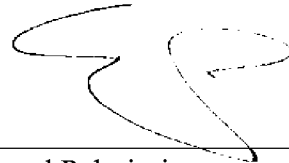
IX.

Respondent, within ninety (90) days after the date of service of this order, 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, Respondent shall submit additional true and accurate written reports.

This Report satisfies the requirement under Part IX of the Order to file a report with the Commission within 90 days after the date of service of the Order.

I affirm under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

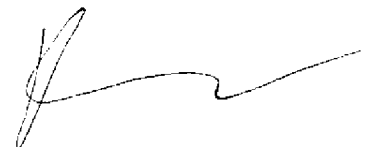
Executed on November 13, 2012



Edward Palmieri
Associate General Counsel, Privacy
Facebook, Inc.

I affirm under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed on November 13, 2012



Daniel Li
Product Counsel
Facebook, Inc.

EXHIBIT 4

GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

MEMORANDUM

April 9, 2018

To: Committee on Energy and Commerce Democratic Members and Staff
Fr: Committee on Energy and Commerce Democratic Staff
Re: Hearing on “Facebook: Transparency and Use of Consumer Data”

On **Wednesday, April 11, 2018, at 10:00 a.m. in room 2123 of the Rayburn House Office Building**, the Committee on Energy and Commerce will hold a hearing titled “Facebook: Transparency and Use of Consumer Data.”

I. BACKGROUND

As online platforms have sought to increase advertising revenue, there has been exponential growth in the amount and detail of the information they collect on consumers and significant changes in how that information is used.¹ In the United States, privacy and data security regulation is sector specific with varying levels of protection for different entities and types of information and some sectors with no requirements at all.²

II. FACEBOOK-CAMBRIDGE ANALYTICA INCIDENT

Reports indicate that beginning in 2013, Aleksandr Kogan of Global Science Research (GSR) began collecting the Facebook data of users participating in a personality test app that Kogan developed.³ The 270,000 users of that particular app consented to the sharing of their

¹ Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, 34 Seattle U. L. Rev. 439 (2011).

² Council on Foreign Relations, *Reforming the U.S. Approach to Data Protection and Privacy* (Jan. 30, 2018) (www.cfr.org/report/reforming-us-approach-data-protection).

³ *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, The Guardian (Mar. 17, 2018).

data.⁴ At the time, Facebook's platform also allowed the app to collect personal data from tens of millions of those users' friends on Facebook who were not notified and did not consent to their information being collected.⁵ Facebook estimates that 87 million of its users' Facebook profiles were swept up by the app.⁶ GSR—Kogan's firm—then sold that data for nearly \$1 million to a political consulting firm, Cambridge Analytica.⁷ Cambridge Analytica in turn used that data to micro-target political ads to U.S. voters in the 2016 election.⁸

Facebook stated that it became aware of the unauthorized sale of this data to a third party in 2015, at which time Facebook banned GSR's app and demanded that Kogan and Cambridge Analytica delete the data.⁹ News reports indicate that Cambridge Analytica may not have deleted the data, although Cambridge Analytica denies those reports.¹⁰

III. PRIOR FTC ACTION AGAINST FACEBOOK

In 2011, the Federal Trade Commission settled charges against Facebook that it deceived consumers by failing to disclose when information its users designated as private was made public.¹¹ In addition, Facebook was charged with failing to properly inform users of how their information would be collected and used by third-party applications.¹² The settlement agreement barred Facebook from making deceptive claims about users' privacy, required that the company get consumers' approval before changing the way it shared their data, and required that it obtain periodic assessments of its privacy practices by independent, third-party auditors for 20 years.¹³

IV. WITNESS

Mark Zuckerberg
CEO
Facebook

⁴ *How Trump Consultants Exploited the Facebook Data of Millions*, New York Times (Mar. 17, 2018).

⁵ Comment on Mark Zuckerberg's Facebook Page (Mar. 21, 2018, 3:36 PM) (www.facebook.com/zuck/posts/10104712037900071).

⁶ *Id.*

⁷ *See* note 1.

⁸ *Id.*

⁹ *See* note 3; Facebook, *Suspending Cambridge Analytica and SCL Group from Facebook* (Mar. 16, 2018) (press release).

¹⁰ *See* note 3.

¹¹ Federal Trade Commission, *Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises* (Nov. 29, 2011) (press release).

¹² *Id.*

¹³ *Id.*

EXHIBIT 5



Independent Assessor's Report on Facebook's Privacy Program

Initial Assessment Report

For the period August 15, 2012 to
February 11, 2013

The contents of this document, including the Report of Independent Accountants, contain PricewaterhouseCoopers LLP proprietary information that shall be protected from disclosure outside of the U.S. Government in accordance with the U.S. Trade Secrets Act and Exemption 4 of the U.S. Freedom of Information Act (FOIA). The document constitutes and reflects work performed or information obtained by PricewaterhouseCoopers LLP, in our capacity as independent assessor for Facebook, Inc. for the purpose of the Facebook, Inc.'s Order. The document contains proprietary information, trade secrets and confidential commercial information of our firm and Facebook, Inc. that is privileged and confidential, and we expressly reserve all rights with respect to disclosures to third parties. Accordingly, we request confidential treatment under FOIA, the U.S. Trade Secrets Act or similar laws and regulations when requests are made for the report or information contained therein or any documents created by the FTC containing information derived from the report. We further request that written notice be given to PwC and Facebook, Inc. before distribution of the information in the report (or copies thereof) to others, including other governmental agencies, to afford our firm and Facebook, Inc. with the right to assert objections and defenses to the release of the information as permitted under FOIA or other similar applicable law or regulation, except when such distribution is already required by law or regulation. This report is intended solely for the information and use of the management of Facebook, Inc. and the U.S. Federal Trade Commission and is not intended to be and should not be used by anyone other than these specified parties.

HIGHLY CONFIDENTIAL



Table of Contents

| | |
|---|----|
| Introduction | 3 |
| Report of Independent Accountants | 4 |
| Facebook’s Privacy Program Overview | 6 |
| PwC’s Privacy Assessment Approach | 14 |
| PwC’s Assessment of Part IV A, B, C, D and E, of the Order | 18 |
| Facebook’s Privacy Program: Assertions, Control Activities and PwC’s Tests Performed and Results | 21 |
| Management’s Assertion | 77 |
| Appendix A – Assessment Interviews Summary | 79 |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 2 of 79

HIGHLY CONFIDENTIAL



Introduction

Facebook, Inc. and the Federal Trade Commission (FTC) entered into Agreement Containing Consent Order File No: 0923184 (“the Order”), which was served on August 15, 2012.

Part IV of the Order requires Facebook to establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information.

Part V of the Order requires Facebook to obtain initial and biennial assessments and reports (“Assessments”) from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Facebook engaged PricewaterhouseCoopers LLP (“PwC”) to perform the initial assessment.

As described on pages 6-13, Facebook established its privacy program by implementing privacy controls to meet or exceed the protections required by Part IV of the Order. As described on pages 14-17, PwC performed inquiry, observation, and inspection/examination procedures to assess the effectiveness of the Facebook privacy controls implemented to meet or exceed the protections required by Part IV of the Order during the first 180 day period ended February 11, 2013, and our conclusions are on pages 4-5.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 3 of 79

HIGHLY CONFIDENTIAL



Report of Independent Accountants

To the Management of Facebook, Inc.:

We have examined Management's Assertion, that as of and for the 180 days ended February 11, 2013 (the "Reporting Period"), in accordance with Parts IV and V of the Agreement Containing Consent Order (the "Order") with an effective date of service of August 15, 2012, between Facebook, Inc. ("Facebook" or "the Company") and the United States of America, acting upon notification and authorization by the Federal Trade Commission ("FTC"), the Company had established and implemented a comprehensive Privacy Program, as described in Management's Assertion ("the Facebook Privacy Program"), based on Company-specific criteria, and the privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the Reporting Period.

The Company's management is responsible for the assertion. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and accordingly, included examining, on a test basis, evidence supporting the effectiveness of the Facebook Privacy Program as described above and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

We are not responsible for Facebook's interpretation of, or compliance with, information security or privacy-related laws, statutes, and regulations applicable to Facebook in the jurisdictions within which Facebook operates. We are also not responsible for Facebook's interpretation of, or compliance with, information security or privacy-related self-regulatory frameworks. Therefore, our examination did not extend to the evaluation of Facebook's interpretation of or compliance with information security or privacy-related laws, statutes, regulations, and privacy-related self-regulatory frameworks with which Facebook has committed to comply.

In our opinion, Facebook's privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the Reporting Period, in all material respects as of and for the 180 days ended February 11, 2013, based upon the Facebook Privacy Program set forth in Management's Assertion.

(b)(3):6(f),(b)(4)



This report is intended solely for the information and use of the management of Facebook and the United States Federal Trade Commission and is not intended to be and should not be used by anyone other than these specified parties.

PricewaterhouseCoopers L.L.P.

San Jose

April 16, 2013

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 5 of 79 **HIGHLY CONFIDENTIAL**



Facebook's Privacy Program Overview

Company Overview

Founded in 2004, Facebook's mission is to give people the power to share and make the world more open and connected. Facebook has been working on privacy since its inception and consistently strives to enhance various elements of its internal privacy programs. For example, Facebook now has a Privacy Cross-Functional ("XFN") internal team (comprised of experts with a range of privacy expertise) that vets and reviews products during the development cycle and before launch. Facebook also created two new corporate officer roles— Chief Privacy Officer, Product and Chief Privacy Officer, Policy—who are charged with ensuring that Facebook's commitments are reflected in all of its activities.

Facebook supports its mission by developing useful and engaging tools that enable people to connect, share, discover, and communicate with each other on mobile devices and computers. Facebook's products include News Feed, Timeline, Platform, Graph Search, Messages, Photos and Video, Groups, Events, and Pages. These products are available through Facebook's website, Facebook.com. They are also accessible through certain Facebook mobile applications or "apps", including Facebook, Camera, Messenger, Pages, and Poke. Versions of Facebook's mobile apps are available for multiple operating systems, such as iOS and Android operating systems. These products and services allow people all over the world to share, and communicate with each other in new and innovate ways, connecting people in ways not possible before these tools were offered.

Facebook Platform ("Platform") is a set of development tools and application programming interfaces ("APIs") that enable developers to build their own social apps, websites, and devices that integrate with Facebook. The Facebook's Developer Operations team is focused on supporting successful applications, driving platform adoption, and maintaining the user experience through developer education and policy enforcement. The Platform Principles that Facebook imposes on all developers are: (1) Create a great user experience (Build social and engaging applications; Give users choice and control; and Help users share expressive and relevant content); and (2) Be trustworthy (Respect privacy; Don't mislead, confuse, defraud, or surprise users; and Don't spam - encourage authentic communications). Additionally, Facebook's Statement of Rights and Responsibilities and Platform Policies outline a variety of developer obligations, including those around privacy, such as providing notice and obtaining consent for certain data uses and restrictions on sharing user information.

Most products and services Facebook offers are free. Facebook is able to do this by providing value for marketers, including brand marketers, small and medium-sized businesses, and developers. Facebook offers a unique combination of reach, relevance, social context, and engagement. Marketers can also use Facebook's analytics platform, Facebook Ad Analytics, to understand and optimize the performance of their campaigns.

In addition to Facebook created products and services, Facebook acquired Instagram on August 31, 2012. Instagram is a photo sharing service that enables users to take photos, apply digital filters to the photos, share them with others, and comment on photos posted by themselves or by others. At the time of acquisition, Instagram had approximately 13 employees. During the reporting period subsequent to the acquisition, Instagram was

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 6 of 79

HIGHLY CONFIDENTIAL



available on the web at Instagram.com and as an app on the iOS and Android operating systems.

Facebook Privacy Program Scope

Facebook designed the Privacy Program to accomplish two primary objectives: (a) to address privacy risks related to the development, management, and use of new and existing products; and (b) to protect the privacy and confidentiality of the information Facebook receives from or about consumers. Facebook leveraged the Generally Accepted Privacy Principles (“GAPP”) framework, set forth by the American Institute of Certified Public Accountants (“AICPA”) and Canadian Institute of Chartered Accountants (“CICA”), to define company-specific criteria for the foundation of the Facebook Privacy Program. The GAPP framework is globally recognized as a leading and comprehensive standard for privacy programs.

The ten GAPP principles, which are derived from internationally recognized information practices, are as follows:

1. **Management.** The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.
2. **Notice.** The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
3. **Choice and consent.** The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
4. **Collection.** The entity collects personal information only for the purposes identified in the notice.
5. **Use, retention, and disposal.** The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.
6. **Access.** The entity provides individuals with access to their personal information for review and update.
7. **Disclosure to third parties.** The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
8. **Security for privacy.** The entity protects personal information against unauthorized access (both physical and logical).
9. **Quality.** The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
10. **Monitoring and enforcement.** The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related complaints and disputes.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 7 of 79

HIGHLY CONFIDENTIAL



The following is a brief description of the Facebook Privacy Program.

Facebook has designated a team of employees who are directly responsible for the Facebook Privacy Program (the “Privacy Governance Team”). Facebook’s Chief Privacy Officer, Product leads the Privacy Governance Team. Other team members include the Chief Privacy Officer, Policy; Chief Security Officer, Associate General Counsel, Privacy; Associate General Counsel, Privacy and Product; Associate General Counsel, Advertising and Product; and Associate General Counsel, Regulatory. While the Chief Privacy Officer, Product provides leadership responsibility for coordinating the Privacy Program, the entire Privacy Governance Team and many employees (including engineers, product managers, etc.) are responsible for various aspects of the Privacy Program and play a crucial role driving and implementing decisions made by the Privacy Governance Team. Of particular note are the Privacy Program Managers who work directly under Chief Privacy Officer, Product. This team is embedded in the product organization and is responsible for: (1) engaging closely with legal, policy, and other members of the Privacy XFN Team to drive privacy decisions; (2) coordinating and presenting privacy issues to the Privacy XFN Team; and (3) maintaining records of privacy decisions and reviews.

A central aspect of Facebook’s Privacy Program is a continuous assessment of privacy risks. As part of this risk assessment process, members of the Privacy Governance Team work with relevant Facebook stakeholders, including representatives of Facebook’s Privacy, Engineering, Security, Internal Audit, Marketing, Legal, Public Policy, Communications, Finance, Platform Operations, and User Operations teams, to identify reasonably foreseeable, material risks, both internal and external, that could result in the unauthorized collection, use or disclosure of covered information. This process is enriched by input from the Chief Privacy Officer, Policy and her team, which engage with industry stakeholders and regulators and integrate external feedback into Facebook’s program.

The team considers risks in each relevant area of operation, including governance, product design, and engineering (including product development and research), user operations (including third-party developers), advertising, service providers, employee awareness and training, employee management, and security for privacy. The team also considers the sufficiency of the safeguards in place to control the identified risks. Through this process, Facebook has documented reasonably foreseeable material risks to user privacy and has put in place reasonable privacy processes and controls to address those risks.

As part of Facebook’s on-going privacy risk assessment process, Facebook holds an annual “Privacy Summit” of relevant stakeholders, including key representatives from the Privacy XFN Team. The Privacy XFN Team includes representatives from each major segment of Facebook, including Facebook’s Privacy, Public Policy, Legal, Marketing, Product, Engineering, Security, and Communications teams. Attendees of the annual Privacy Summit review and update the privacy risk assessment, focusing on significant material risks identified by the Privacy Governance Team. Attendees evaluate those privacy risks in light of changing internal and external threats, changes in operations, and changes in laws and regulations. Attendees also examine the sufficiency of existing privacy controls in mitigating those risks, as well as new potential risks. Finally, attendees engage in discussion around ways to improve the work performed by the Privacy XFN Team. The last Privacy Summit occurred on January 15, 2013.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 8 of 79

HIGHLY CONFIDENTIAL



As indicated above, Facebook's Privacy Governance Team, led by the Chief Privacy Officer, Product is responsible for the design, implementation, and maintenance of the Privacy Program, which is documented in written policies and procedures. Highlights of the program are detailed below.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 9 of 79 **HIGHLY CONFIDENTIAL**



Privacy and Security Awareness Activities

Facebook communicates Privacy and Security awareness matters to new and existing employees and tailors such communications according to role and responsibility. For example, as part of its regular training for new project managers, Facebook trains project managers about the privacy program and key privacy considerations during the product development cycle. This training involves representatives from the Privacy XFN Team presenting to the project managers (the Privacy XFN process covers those directly involved in the development and management of new products, enhancements to existing products and services for consumers, as described below under “Product Design, Development and Research Activities”). As a further example, engineers at Facebook spend their first six weeks in bootcamp, an immersive, cross-functional orientation program. During bootcamp, engineers are instructed on the importance of privacy and security at Facebook, along with their obligations to protect user information as it relates to their roles and responsibilities. Similar group-specific trainings are held for other constituents in the Company (e.g., user operations).

Facebook also holds “Hacktober” annually in October. Hacktober is a month-long event intended to increase employee privacy and security awareness. A series of simulated security threats (e.g., phishing scams) are presented to employees to determine how the employees would respond. If employees report the security threat, they receive a reward, such as Facebook-branded merchandise. If the security threat goes unreported, or if vulnerability is exploited, the employees undergo further education and awareness.

To further promote recognition and understanding of privacy issues and obligations among all Facebook employees, Facebook recently deployed, in addition to initiatives described above, a computer-based privacy training program to all employees. This training provides an overview of applicable privacy laws and Facebook’s privacy commitments. All new employees are now required to complete the privacy training within 30 days of employment, while all existing employees are required to complete the privacy training annually. Facebook employees are quizzed on their understanding of Facebook’s privacy practices during the training.

Product Design, Development, and Research Activities

The Privacy XFN Team considers privacy from the earliest stages in the product development process (i.e., “privacy by design”). The Chief Privacy Officer, Product and his team spearhead this review and lead a number of key functions and responsibilities. First, as described above, employees, including engineers, product managers, content strategists, and product marketing managers, are educated on Facebook’s privacy framework. This education includes an overview of Facebook’s processes and corresponding legal obligations, and may involve other members of the Privacy XFN team, such as Privacy and Product Counsel.

Second, the Chief Privacy Officer, Product and his team host weekly reviews of key product-related decisions and material changes to Facebook’s privacy framework, which are attended by members of the Privacy XFN Team. The Chief Privacy Officer, Product and his team also review all new product proposals and any material changes to existing products from a privacy perspective and involve the Privacy XFN Team for broader review and feedback. The impact of privacy principles such as notice, choice, consent, access, security,

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 10 of 79

HIGHLY CONFIDENTIAL



retention, deletion, and disclosure are considered as part of this review. Product launches are added to the Privacy Launch Calendar to ensure on-going review and consideration of privacy issues by the Privacy XFN Team throughout the development process. Members of the Privacy XFN Team also communicate back to their respective teams on issues covered in the weekly reviews. This review process helps ensure that privacy is considered throughout the product development process, and maintains consistency on privacy issues across all Facebook products and services.

The following products, available on the platforms and devices indicated, are included in the scope of Facebook's Privacy Program and the Order:

- Facebook: Facebook.com (internet/web), m.facebook.com, iOS, Android, Facebook for Every Phone, Facebook for Blackberry, Facebook for Windows;
- Messenger: iOS, Android;
- Camera: iOS;
- Pages Manager: iOS, Android;
- Poke: iOS; and
- Instagram: Instagram.com (internet/web), iOS, Android.

Facebook Platform

Platform applications and developers are required to comply with, and are subject to, Facebook's Statement of Rights and Responsibilities, Platform Principles, and Platform Policies. These terms and policies outline a variety of privacy obligations and restrictions, such as limits on an application's use of data received through Facebook, requirements that an application obtain consent for certain data uses, and restrictions on sharing user data. Facebook's Platform privacy setting and Granular Data Permissions ("GDP") process allows users to authorize the transfer of Facebook user information to third-party applications. Monitoring controls are in place to detect material misuse of the Platform (e.g., user complaints, third-party applications that do not have active privacy policy links).

Security for Privacy

Facebook has implemented technical, physical, and administrative security controls designed to protect user data from unauthorized access, as well as to prevent, detect, and respond to security threats and vulnerabilities. Facebook's security program is led by the Chief Security Officer ("CSO") and supported by a dedicated Security Team. As mentioned above, the CSO is a key and active member of the Privacy Governance team. Facebook's security and privacy employees work closely on an on-going basis to protect user data and Facebook's systems.

Monitoring Activities

In order to ensure that the effectiveness of its controls and procedures are regularly monitored, Facebook has designated an "owner" for each of the controls included in the Privacy Program. Facebook utilizes the annual Privacy Summit to monitor the effectiveness of controls and procedures in light of changing internal and external risks. In addition, members of Facebook's Legal team periodically review the Privacy Program to ensure it, including the controls and procedures contained therein, remains effective. These Legal team members also will serve as point of contacts for control owners and will update the Privacy Program to reflect any changes or updates surfaced.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 11 of 79

HIGHLY CONFIDENTIAL



Service Providers

Facebook has implemented controls with respect to third-party service providers, including implementing policies to select and retain service providers capable of appropriately protecting the privacy of covered information received from Facebook.

Facebook's Security team has a process for conducting due diligence on service providers who may receive covered information in order to evaluate whether their data security standards are aligned with Facebook's commitments to protect covered information. As part of the due diligence process, Facebook asks prospective service providers to complete a security architecture questionnaire or vendor security questionnaire to assess whether the provider meets Facebook's functional security requirements to protect the privacy of user data. Based upon the service provider's responses to the vendor security questionnaire and other data points, Facebook's Security team determines whether further security auditing is required. Facebook partners with an outside security consulting firm to conduct security audits, which may include testing of the service provider's controls, a vulnerability scanning program, a web application penetration test, and/or a code review for security defects. The security consulting firm reports its findings to Facebook, and Facebook requires that the prospective service provider fix critical issues before being on-boarded. Depending on the sensitivity of Facebook data shared with the service provider and other factors, Facebook may require that the service provider undergo a periodic or random security and/or privacy audit.

Facebook also has a contract policy (the "Contract Policy"), which governs the review, approval, and execution of contracts for Facebook. Facebook's pre-approved contract templates require service providers to implement and maintain appropriate protections for covered information. Facebook reviews contracts that deviate from the pre-approved templates to help ensure that contracts with applicable service providers contain the required privacy protections. Facebook Legal documents review of any such contracts through formal approval prior to contract execution.

Monitoring

Facebook's Privacy Program is designed with procedures for evaluating and adjusting the Privacy Program in light of the results of testing and monitoring of the program as well as other relevant circumstances. As mentioned above, Facebook's annual Privacy Summit is designed to identify, discuss, and assess compliance with privacy policies and procedures, and applicable laws and regulations, as well as identify new or changed risks and recommend responsive controls. The Privacy XFN Team assesses risks and controls on an on-going basis through weekly meetings and review processes. Members of Facebook's Legal team support the Privacy Program and serve as points of contact for all relevant control owners to communicate recommended adjustments to the Privacy Program based on regular monitoring of the controls for which they are responsible, as well as any internal or external changes that affect those controls. Additionally, the Privacy Governance Team regularly discusses the Privacy Program in the context of various product and operational discussions. During these discussions, the effectiveness and efficiency of the Privacy Program are considered and reviewed and, when appropriate, adjustments are made to maintain a strong program.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 12 of 79

HIGHLY CONFIDENTIAL



Facebook also continuously evaluates acquisitions for inclusion in the Privacy Program, based on the nature of the acquisition (e.g., talent or people, intellectual property, product or infrastructure). Specifically, Facebook takes steps, as appropriate, to integrate acquisitions into the Privacy Program and reviews products and features developed by acquisitions with the same level of rigor applied to Facebook's products and services. The acquisitions in the current Reporting Period were primarily talent acquisitions, except for Instagram. Instagram's people, product, and supporting infrastructure were acquired on August 31, 2012.

Facebook assessed the privacy risks associated with Instagram's people, process, and technology upon acquisition. In comparison to Facebook, Instagram has significantly fewer users, employees, and products. As described in the Company Overview above, Instagram's products focus on photo taking, filtering, and sharing. From a privacy perspective, Instagram users have one binary choice - to make all photos private or all photos public by setting the "Photos are Private" on/off slider. Once private, the user approves any "follower" requests. After obtaining approval, the follower can access posted photos and related comments. The Privacy XFN Team also was involved in reviewing Instagram's January 19, 2013 privacy policy update.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 13 of 79

HIGHLY CONFIDENTIAL



PwC's Privacy Assessment Approach

PwC's Assessment Standards

Part V of the Order requires that the Assessments be performed by a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. This report was issued by PwC under professional standards which meet these requirements.

As a public accounting firm, PwC must comply with the public accounting profession's technical and ethical standards, which are enforced through various mechanisms created by the American Institute of Certified Public Accountants ("AICPA"). Membership in the AICPA requires adherence to the Institute's Code of Professional Conduct. The AICPA's Code of Professional Conduct and its enforcement are designed to ensure that CPAs who are members of the AICPA accept and achieve a high level of responsibility to the public, clients, and colleagues. The AICPA Professional Standards provide the discipline and rigor required to ensure engagements performed by CPAs consistently follow specific General Standards, Standards of Fieldwork, and Standards of Reporting ("Standards").

In order to accept and perform this FTC assessment ("engagement"), the Standards state that PwC, as a practitioner, must meet specific requirements, such as the following.

General Standards:

- Have reason to believe that the subject matter is capable of evaluation against criteria that are suitable and available to users. Suitable criteria must be free from bias (objective), permit reasonably consistent measurements, qualitative or quantitative, of subject matter (measurable), be sufficiently complete so that those relevant factors that would alter a conclusion about subject matter are not omitted (complete), and be relevant to the subject matter;
- Have adequate technical training and proficiency to perform the engagement;
- Have adequate knowledge of the subject matter; and
- Exercise due professional care in planning and performance of the engagement and the preparation of the report.

Standards of Fieldwork:

- Adequately plan the work and properly supervise any assistants; and
- Obtain sufficient evidence to provide a reasonable basis for the conclusion that is expressed in the report.

Standards of Reporting:

- Identify the assertion being reported on in the report; and
- State the practitioner's conclusion about the assertion in relation to the criteria.

In performing this assessment, PwC complied with all of these Standards.



Independence

The Standards also require us to maintain independence in the performance of professional services. Independence requirements fall into five categories: personal financial interests; business relationships; employment relationships; prohibited services; prohibition from serving in the Company's management capacity; and independence in mental attitude. In summary, relevant individuals must not have personal financial interests in the Company; the Company and the Assessor may not have certain business relationships; there are restrictions on relationships that may exist between employees performing the assessment and employees at the Company or formerly at the Company or at the Assessor firm; there are numerous services that cannot be provided by the Assessor to the Company; and the Assessor may not act in a management capacity or make any decisions for the Company.

Further, the Standards require us to maintain independence in mental attitude in all matters relating to the engagement. Independence in mental attitude means there is an objective consideration of facts, unbiased judgments, and honest neutrality on the part of the practitioner in forming and expressing conclusions. We are required to maintain intellectual honesty and impartiality necessary to reach an objective and unbiased conclusion.

PwC is independent with respect to the Standards required for this engagement.

PwC Assessor Qualifications

PwC assembled an experienced, cross-disciplinary team of PwC team members with privacy, assessment, and technology industry expertise to perform the Assessor role for the Order. A Partner in PwC's Data Protection and Privacy practice with more than 32 years of experience providing professional services led the engagement. The assessment was performed by an experienced team of over thirteen professionals with a combination of privacy, data protection, information security, industry, and assessment experience. The team included Certified Information Privacy Professionals ("CIPP"), Certified Information Systems Auditors ("CISA"), and Certified Public Accountants ("CPA"). To ensure quality, a Quality Assurance Partner was involved as well as Risk Management personnel from PwC's National Professional Services team.

PwC's procedures lasted over fifteen weeks. The fieldwork was primarily performed at Facebook's headquarters in Menlo Park, CA, with the exception of data center physical and environment control testing. Instagram is also located at Facebook's headquarters.

PwC Assessment Process Overview

The procedures performed by PwC were designed to:

- Assess the applicability of management's assertion to address the Company's obligations within Part IV of the Order;
- Assess the design effectiveness of the control activities implemented by the Company to address the relevant sections of the management assertion; and
- Assess the operating effectiveness of the implemented control activities for the 180-day period ended February 11, 2013.



PwC designed and performed test procedures to evaluate the design effectiveness and operating effectiveness of the control activities implemented by Facebook for the 180 days ended February 11, 2013. For the Instagram-only controls, PwC tested controls from the date of acquisition of Instagram, August 31, 2012 through to February 11, 2013. Where Instagram processes and controls were maintained separately during the period, PwC tested the Instagram-only controls separately. Where Instagram processes and controls were integrated into the Facebook privacy program, PwC included Instagram as part of our testing of Facebook's processes and controls.

The nature of PwC's testing was dependent on each control, and PwC developed a test plan based on our understanding of the risk, complexity, extent of judgment and other factors. We used a combination of inquiry, observation and/or inspection for testing of the controls. Refer below for a description of the test procedures utilized by PwC:

Inquiry: To understand the design of the controls implemented and how they operate to meet or exceed the protections required by Part IV of the order, PwC had discussions with Facebook personnel. The inquiry procedures included asking the Facebook personnel about relevant controls, policies and procedures, as well as roles and responsibilities. To validate the information obtained in the discussions, PwC performed corroborative inquiry procedures with multiple individuals and, using the testing techniques below, obtained additional evidence to validate the responses.

Observation: PwC utilized the observation testing method to validate the design and operating effectiveness of controls. In areas where Facebook has implemented controls that meet or exceed the protections required by Part IV of the order, the PwC team met with relevant Facebook personnel and observed how the control is designed and how it functions. For example, PwC attended Privacy XFN meetings to observe first-hand the operation of this control. PwC watched the attendees interact, discuss products and policy changes, and assess the potential impact on the users and the Privacy Program.

Examination or inspection of evidence: PwC used the examination and/or inspection test approach to validate the operating effectiveness of controls and to evaluate the sufficiency of controls implemented to address Part IV of the Order. PwC inspected, physically or online, artefacts and documents (including documentation of the company's policies and procedures, risk assessment, training, and awareness programs) to evidence the design and operating effectiveness of the controls and safeguards implemented. The nature of the evidence examined varied from control to control and, where appropriate, other procedures like observation and inquiry were utilized to confirm the results of the examination procedures.

To assess design effectiveness, PwC performed walkthroughs of the processes and controls to determine whether the controls were built to achieve the intended assertions as well as to determine whether the controls had been placed into operation. To perform a walkthrough, PwC met with relevant Facebook control owners. Additionally, during the design assessment, PwC assessed whether the persons performing the controls possessed the necessary authority and competence to perform the controls effectively. Our design effectiveness test procedures included performing a combination of inquiry, observation, and/or inspection/ examination.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 16 of 79

HIGHLY CONFIDENTIAL



To assess operating effectiveness, PwC performed procedures to determine whether controls were executed by Facebook (or Facebook's systems if automated) on a regular frequency and whether documentation and/or support was maintained to evidence the controls' execution. Our operating effectiveness test procedures included, where appropriate, selecting samples from throughout the period and performing a combination of inquiry, observation, and/or inspection/ examination procedures to evaluate the effectiveness of the Facebook control activities documented on pages 21-76 of this document.

Over the course of the reporting period, PwC performed procedures that included interviewing individuals from Privacy, Legal, Identity, Security, User Operations, Developer Operations, Engineering, Infrastructure, Mobile Partner Management, and Human Resources. Test plans for each control activity tested are also included on pages 21-76 of this document. See Appendix A for a summary of interviewees.



PwC's Assessment of Part IV A, B, C, D and E, of the Order

The tables in section "Facebook's Privacy Program: Assertions, Control Activities and PwC's Tests Performed and Results" of this report describe the scope of Facebook's Privacy Program referenced in the Management Assertion on pages 77-78. Facebook established its privacy program by implementing privacy controls to meet or exceed the protections required by Part IV of the Order. The table also includes PwC's inquiry, observation, and inspection/examination test procedures to assess the effectiveness of Facebook's program and test results. PwC's final conclusions are detailed on pages 4-5 of this document.

A. Set forth the specific privacy controls that respondent has implemented and maintained during the reporting period.

As depicted within the table on pages 21-76, Facebook has listed the privacy controls that were implemented and maintained during the reporting period.

B. Explain how such privacy controls are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered information.

Based on the size and complexity of the organization, the nature and scope of Facebook's activities, and the sensitivity of the covered information (as defined in by the order), Facebook management developed the company-specific criteria (assertions) detailed on pages 77-78 as the basis for its Privacy Program. The management assertions and the related control activities are intended to be implemented to address the risks identified by Facebook's privacy risk assessment.

C. Explain how the privacy controls that have been implemented meet or exceed the protections required by Part IV of the Order.

As summarized in the Facebook's Privacy Program on pages 6-13, Facebook has implemented the following protections:

A. Designation of an employee or employees to coordinate and be responsible for the privacy program.

As described above, Facebook has designated a team of employees to coordinate and be responsible for the Privacy Program as required by Part IV of the Order. As described on pages 21-23 (Management's Assertion A), PwC performed test procedures to assess the effectiveness of the Facebook privacy controls implemented to meet or exceed the protections required by Part IV of the Order.

B. The identification of reasonably foreseeable, material risks, both internal and external, that could result in Respondent's unauthorized collection, use, or disclosure of covered information and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk assessment should include consideration of risks in each area of relevant operation,



including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research.

As described above, Facebook has identified reasonably foreseeable, material risks, both internal and external, that could result in Facebook's unauthorized collection, use, or disclosure of covered information, and assessed the sufficiency of any safeguards in place to control these risks as required by Part IV of the Order. As described on page 24 (Management's Assertion B), PwC performed test procedures to assess the effectiveness of the Facebook privacy controls implemented to meet or exceed the protections required by Part IV of the Order.

C. 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.

As described above, Facebook has designed and implemented 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 as required by Part IV of the Order. As described on pages 25-65 (Management's Assertions C, D, E, F, and G), PwC performed test procedures to assess the effectiveness of the Facebook privacy controls implemented to meet or exceed the protections required by Part IV of the Order.

D. 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 Respondent and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information.

As described above, Facebook has developed and implemented reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from Facebook as required by Part IV of the Order. Facebook also includes terms in contracts with service providers requiring that such service providers implement and maintain appropriate privacy protections. As described on pages 66-70 (Management's Assertion H), PwC performed test procedures to assess the effectiveness of the Facebook privacy controls implemented to meet or exceed the protections required by Part IV of the Order.

E. The evaluation and adjustment of Respondent's privacy program in light of the results of the testing and monitoring required by subpart C, any material changes to Respondent's operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have a material impact on the effectiveness of its privacy program.

As described above, Facebook has evaluated and adjusted its Privacy Program in light of the results of the testing and monitoring required by subpart C within Part IV of the Order, any material changes to Facebook's operations or business arrangements, or any other circumstances that Facebook knows or has reason to



know may have a material impact on the effectiveness of its privacy program as required by Part IV of the Order. As described on pages 71-76 (Management's Assertion I), PwC performed test procedures to assess the effectiveness of the Facebook privacy controls implemented to meet or exceed the protections required by Paragraph IV of the Order.

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.

As described in the PwC Assessment Process Overview section above, PwC performed its assessment of Facebook's Privacy Program in accordance with AICPA Attestation Standards. Refer to pages 4-5 of this document for PwC's conclusions.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 20 of 79

HIGHLY CONFIDENTIAL



Facebook’s Privacy Program: Assertions, Control Activities and PwC’s Tests Performed and Results

Provided below are the Facebook Privacy Program controls and PwC’s tests performed. Also provided are the results of the testing performed by PwC. Finally, additional information has been provided by PwC for the instances in which PwC identified an exception during testing. This information is provided in an effort to enhance the FTC’s understanding of the exception. Unless otherwise indicated in the table below, exceptions identified relate to the Reporting Period (August 15, 2012 to February 11, 2013) for Facebook or from the date of acquisition to the end of the Reporting Period (August 31, 2012 to February 11, 2013) for Instagram.

| Ref. | Facebook’s Control Activity | PwC’s Tests Performed | PwC’s Test Results | Additional Information |
|--|---|-----------------------|--------------------|------------------------|
| Assertion A – Responsibility for the Facebook Privacy Program | | | | |
| Facebook has designated an employee or employees to coordinate and be responsible for the privacy program. | | | | |
| A-1 | Facebook has designated a team of employees who are directly responsible for the Privacy Program (the “Privacy Governance Team”). Facebook’s Chief Privacy Officer, Product leads the Privacy Governance Team. | (b)(3):6(f),(b)(4) | | |
| A-2 | Facebook has designated a team of employees who are directly responsible for the Information Security Program (the “Security Team”). Facebook’s Chief Security Officer leads the Security Team. | | | |
| A-3 | Facebook has defined roles and responsibilities for teams supporting the Privacy and Information Security Programs, including: <ul style="list-style-type: none"> Privacy Governance Team - Responsible for coordinating Facebook’s Privacy Program, which is led by the Chief Privacy Officer, Product. The Privacy | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 21 of 79 HIGHLY CONFIDENTIAL



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|--|--|---------------------------|--------------------|------------------------|
| Assertion A – Responsibility for the Facebook Privacy Program | | | | |
| Facebook has designated an employee or employees to coordinate and be responsible for the privacy program. | | | | |
| | <p>Governance Team is integrated into the product development process and leads Facebook's commitment to build privacy into its products at an early stage of development.</p> <ul style="list-style-type: none"> Privacy Cross Functional Team (XFN) - Includes representatives from major segments of Facebook, including: Privacy Governance team, Policy, Legal, Marketing, Product, Engineering, Security, and Communications. Responsible for the product development process and leads Facebook's commitment to build privacy into its products at an early stage of development. Information Security Team - Responsible for coordinating Facebook's Security Program, which is led by the Chief Security Officer. The Information Security Team is integrated as part of the Privacy XFN Team, and is responsible for ensuring that security for privacy programs, policies and procedures are implemented within the organization. | <p>(b)(3):6(f),(b)(4)</p> | | |
| A-4 | Facebook has defined and documented qualifications for key positions that are directly responsible for the privacy and security of user information. | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 22 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|--|---|-----------------------|--------------------|------------------------|
| Assertion A – Responsibility for the Facebook Privacy Program | | | | |
| Facebook has designated an employee or employees to coordinate and be responsible for the privacy program. | | | | |
| A-5 | Facebook's hiring procedures establish the due diligence procedures (i.e., background checks) needed to ensure personnel responsible for protecting privacy and security are qualified. | (b)(3):6(f),(b)(4) | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 23 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|---|---------------------------|--------------------|------------------------|
| Assertion B – Privacy Risk Assessment | | | | |
| <p>Facebook has identified reasonably foreseeable, material risks, both internal and external, 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. This privacy risk assessment includes consideration of risks in areas of relevant operations, including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research.</p> | | | | |
| B-1 | <p>Facebook holds an Annual Privacy Summit of relevant stakeholders, including key representatives from the Privacy Cross-Functional (XFN) Team. The attendees of the Annual Privacy Summit review and update the privacy risk assessment, focusing on significant material risks identified by the Privacy Governance Team. The attendees also evaluate those privacy risks in light of changing internal and external threats, changes in operations, and changes in laws and regulations. The sufficiency of existing controls is considered in mitigating identified risks.</p> | <p>(b)(3):6(f),(b)(4)</p> | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 24 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|--|-----------------------|--------------------|------------------------|
| Assertion C. Privacy and Security (for Privacy) Awareness | | | | |
| Facebook has a privacy and security for privacy awareness program in place which is defined and documented in privacy and security for privacy policies. The extent of communications to employees is based on their role and responsibility and may include internal communications through various channels, training, and the Privacy Cross-Functional ("XFN") team process. | | | | |
| C-1 | <p>Facebook's privacy policy is called the "Data Use Policy." Facebook's terms of service are outlined in the "Statement of Rights and Responsibilities," which governs Facebook's relationship with users and others who interact with Facebook.</p> <p>Instagram maintains a separate privacy policy and terms of service.</p> <p>The topics covered within these policies include the following:</p> <ul style="list-style-type: none"> • Notice • Choice and consent • Collection • Use, retention, and deletion • Access • Disclosure to third parties • Security for privacy • Quality • Monitoring and enforcement | (b)(3):6(f),(b)(4) | | |
| C-2 | (b)(3):6(f),(b)(4) | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 25 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|---|-----------------------|--------------------|------------------------|
| Assertion C. Privacy and Security (for Privacy) Awareness | | | | |
| Facebook has a privacy and security for privacy awareness program in place which is defined and documented in privacy and security for privacy policies. The extent of communications to employees is based on their role and responsibility and may include internal communications through various channels, training, and the Privacy Cross-Functional ("XFN") team process. | | | | |
| | (b)(3):6(f),(b)(4) | | | |
| C-3 | The information security policy and other supporting internal procedures are available to all employees via an internal site. | (b)(3):6(f),(b)(4) | | |
| C-4 | (b)(3):6(f),(b)(4) | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 26 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|---|-----------------------|--------------------|------------------------|
| Assertion C. Privacy and Security (for Privacy) Awareness | | | | |
| Facebook has a privacy and security for privacy awareness program in place which is defined and documented in privacy and security for privacy policies. The extent of communications to employees is based on their role and responsibility and may include internal communications through various channels, training, and the Privacy Cross-Functional ("XFN") team process. | | | | |
| | (b)(3):6(f),(b)(4) | | | |
| C-5 | Facebook and Instagram communicate their privacy policies and terms of service via the Facebook and Instagram external facing websites and across all available platforms and products. Material changes to Facebook's privacy policies and terms of service are communicated via company-wide notification channels, which includes the: <ul style="list-style-type: none"> • Internal site; • Company-wide privacy training programs; and • Facebook's Site Governance page, which is the site where proposed changes to the Data Use Policy and Statement of Rights and Responsibilities are made available to the Facebook community for seven (7) days. The Site Governance page is intended to facilitate open-forum discussion of proposed changes to the Data Use Policy and Statement of Rights and Responsibilities, before the changes are put into effect. | (b)(3):6(f),(b)(4) | | |
| C-6 | (b)(3):6(f),(b)(4) | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 27 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|-----------------------------|-----------------------|--------------------|------------------------|
| Assertion C. Privacy and Security (for Privacy) Awareness | | | | |
| Facebook has a privacy and security for privacy awareness program in place which is defined and documented in privacy and security for privacy policies. The extent of communications to employees is based on their role and responsibility and may include internal communications through various channels, training, and the Privacy Cross-Functional ("XFN") team process. | | | | |
| | | | | (b)(3):6(f),(b)(4) |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 28 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|-----------------------------|-----------------------|--------------------|------------------------|
| Assertion C. Privacy and Security (for Privacy) Awareness | | | | |
| Facebook has a privacy and security for privacy awareness program in place which is defined and documented in privacy and security for privacy policies. The extent of communications to employees is based on their role and responsibility and may include internal communications through various channels, training, and the Privacy Cross-Functional ("XFN") team process. | | | | |
| | | | | (b)(3):6(f), (b)(4) |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 29 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|-----------------------------|-----------------------|--------------------|------------------------|
| Assertion C. Privacy and Security (for Privacy) Awareness | | | | |
| Facebook has a privacy and security for privacy awareness program in place which is defined and documented in privacy and security for privacy policies. The extent of communications to employees is based on their role and responsibility and may include internal communications through various channels, training, and the Privacy Cross-Functional ("XFN") team process. | | | | |
| | | | | (b)(3):6(f),(b)(4) |
| C-7 | (b)(3):6(f),(b)(4) | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 30 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|--|-----------------------|--------------------|------------------------|
| Assertion C. Privacy and Security (for Privacy) Awareness | | | | |
| Facebook has a privacy and security for privacy awareness program in place which is defined and documented in privacy and security for privacy policies. The extent of communications to employees is based on their role and responsibility and may include internal communications through various channels, training, and the Privacy Cross-Functional ("XFN") team process. | | | | |
| | | | | (b)(3):6(f),(b)(4) |
| C-8 | The Security Team conducts month long company-wide security awareness activities during National Cyber Security Awareness Month (October). Facebook refers to these activities as "Hacktober." Hacktober activities are intended to increase the awareness and visibility of security responsibilities and issues amongst Facebook employees. | (b)(3):6(f),(b)(4) | | |
| C-9 | Facebook has a Privacy Cross-Functional (XFN) team that is responsible for reviewing product launches, major changes, and privacy-related bug fixes to products and features to ensure that privacy policies and procedures are consistently applied. The Privacy XFN team is represented by members from the following major segments of Facebook: Privacy & Public Policy; Legal; Marketing; | (b)(3):6(f),(b)(4) | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 31 of 79 HIGHLY CONFIDENTIAL



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|--|-----------------------|--------------------|------------------------|
| Assertion C. Privacy and Security (for Privacy) Awareness | | | | |
| Facebook has a privacy and security for privacy awareness program in place which is defined and documented in privacy and security for privacy policies. The extent of communications to employees is based on their role and responsibility and may include internal communications through various channels, training, and the Privacy Cross-Functional ("XFN") team process. | | | | |
| | <p>Product; Engineering; Security; and Communications.</p> <p>Product launches, major changes and privacy-related bug fixes are added to the launch calendar for review and consideration of privacy by the XFN team. The XFN team meets on a weekly basis to review each new or modified product and/or feature launch to ensure that privacy policies and procedures are consistently applied.</p> <p>The XFN process ensures that new products and changes to existing products that result in material and/or retroactive changes to the use of information are evaluated to determine whether additional notice or consent from Facebook users is required. Where required, key decisions around the need for additional consent from users are discussed and recommendations are made and implemented by the XFN team.</p> | (b)(3):6(f), (b)(4) | | |
| C-10 | <p><u>Instagram only:</u> New Instagram products/features and changes to existing products/features were not incorporated into Facebook's XFN process (Control C-9) until November 2012. Prior to this time, Instagram had a separate process, which included:</p> <ul style="list-style-type: none"> • Developing a detailed product plan including project goals and a problem statement; and • Performing detailed testing of the | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 32 of 79 HIGHLY CONFIDENTIAL



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|---|-----------------------|--------------------|------------------------|
| Assertion C. Privacy and Security (for Privacy) Awareness | | | | |
| Facebook has a privacy and security for privacy awareness program in place which is defined and documented in privacy and security for privacy policies. The extent of communications to employees is based on their role and responsibility and may include internal communications through various channels, training, and the Privacy Cross-Functional ("XFN") team process. | | | | |
| | functionality of the new product, as well as the product's impact on privacy prior to launch. | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 33 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|--|---|-----------------------|--------------------|------------------------|
| Assertion D. Notice, Choice, Consent, Collection and Access | | | | |
| Facebook provides notice about its privacy policies and procedures and terms of service to users which identifies the purposes for which personal information is collected and used, describes the choices available to users, obtains implicit or explicit consent, collects personal information only for the purposes identified in the notices and provides users with access to their personal information for review and update. | | | | |
| D-1 | The privacy policies for Facebook and Instagram are: <ul style="list-style-type: none"> • In plain and simple language. • Appropriately labeled, easy to see, and not in unusually small print. • Available in many languages used on the site. • Describes the companies' operations and the types of information covered. • Readily accessible and available when personal information is first collected from the individual. • Provided in a timely manner (that is, at or before the time personal information is collected, or as soon as practical thereafter) to enable individuals to decide whether or not to submit personal information. • Clearly dated to allow individuals to determine whether the privacy practices have changed since the last time they read it or since the last time they submitted personal information. | (b)(3):6(f),(b)(4) | | |
| D-2 | Notice of proposed changes is provided to the privacy policy to all current users. | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 34 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|-----------------------------|-----------------------|--------------------|------------------------|
| <p>Assertion D. Notice, Choice, Consent, Collection and Access</p> <p>Facebook provides notice about its privacy policies and procedures and terms of service to users which identifies the purposes for which personal information is collected and used, describes the choices available to users, obtains implicit or explicit consent, collects personal information only for the purposes identified in the notices and provides users with access to their personal information for review and update.</p> | | | | |
| | | (b)(3):6(f),(b)(4) | | |
| D-3 | (b)(3):6(f),(b)(4) | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 35 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|--|-----------------------|--------------------|------------------------|
| <p>Assertion D. Notice, Choice, Consent, Collection and Access</p> <p>Facebook provides notice about its privacy policies and procedures and terms of service to users which identifies the purposes for which personal information is collected and used, describes the choices available to users, obtains implicit or explicit consent, collects personal information only for the purposes identified in the notices and provides users with access to their personal information for review and update.</p> | | | | |
| | | | | (b)(3):6(f),(b)(4) |
| D-4 | Facebook and Instagram obtain the user's explicit consent at the time of account creation. | (b)(3):6(f),(b)(4) | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 36 of 79 HIGHLY CONFIDENTIAL



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|--|---------------------------|--------------------|------------------------|
| <p>Assertion D. Notice, Choice, Consent, Collection and Access</p> <p>Facebook provides notice about its privacy policies and procedures and terms of service to users which identifies the purposes for which personal information is collected and used, describes the choices available to users, obtains implicit or explicit consent, collects personal information only for the purposes identified in the notices and provides users with access to their personal information for review and update.</p> | | | | |
| | <p>A user enters certain 'basic' personal information (e.g., first name, last name, email address, date of birth and gender information) and clicks on the "Sign Up" button. By clicking this button, the user chooses to share the information with Facebook, make this information public and be searchable online. If an individual chooses not to share any of this information, he or she cannot create a user account.</p> | <p>(b)(3):6(f),(b)(4)</p> | | |
| D-5 | Facebook provides users with explicit and implicit notice of the in-line privacy settings | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 37 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|--|---|-----------------------|--------------------|------------------------|
| Assertion D. Notice, Choice, Consent, Collection and Access | | | | |
| Facebook provides notice about its privacy policies and procedures and terms of service to users which identifies the purposes for which personal information is collected and used, describes the choices available to users, obtains implicit or explicit consent, collects personal information only for the purposes identified in the notices and provides users with access to their personal information for review and update. | | | | |
| | available within Facebook at the time of posting content (e.g., comment, photo, check-in, etc.). | (b)(3):6(f),(b)(4) | | |
| D-6 | <p><u>Instagram only:</u> By clicking on the "Register" button after entering required information (email address), the user chooses to share the information with Instagram and to make certain information public (e.g., pictures) and searchable online. The information requested during sign-up is required. If an individual chooses not to share any of this information, he or she cannot create a user account.</p> <p>The user is able can change privacy settings associated with posting photos, "follow" and "block" other Instagram user accounts from viewing posted photos and "like" photos from other Instagram users.</p> | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 38 of 79 HIGHLY CONFIDENTIAL



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|---|---------------------------|--------------------|------------------------|
| <p>Assertion D. Notice, Choice, Consent, Collection and Access</p> <p>Facebook provides notice about its privacy policies and procedures and terms of service to users which identifies the purposes for which personal information is collected and used, describes the choices available to users, obtains implicit or explicit consent, collects personal information only for the purposes identified in the notices and provides users with access to their personal information for review and update.</p> | | | | |
| | | <p>(b)(3):6(f),(b)(4)</p> | | |
| D-7 | <p>The Privacy XFN process ensures that new products and changes to existing products that result in material and/or retroactive changes to the use of information are evaluated to determine whether additional notice or consent is required. Where required, key decisions around the need for additional consent from users are discussed and recommendations are made by the XFN team.</p> | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 39 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|--|---------------------------|--------------------|------------------------|
| <p>Assertion D. Notice, Choice, Consent, Collection and Access</p> <p>Facebook provides notice about its privacy policies and procedures and terms of service to users which identifies the purposes for which personal information is collected and used, describes the choices available to users, obtains implicit or explicit consent, collects personal information only for the purposes identified in the notices and provides users with access to their personal information for review and update.</p> | | | | |
| | | <p>(b)(3):6(f),(b)(4)</p> | | |
| D-8 | <p><u>Instagram only:</u> New Instagram products/features and changes to existing products/features were not incorporated into Facebook's XFN process until November 2012. Prior to this time, Instagram had a separate process, which included:</p> <ul style="list-style-type: none"> • Putting together a detailed product plan including project goals and a problem statement; and • Performing detailed testing of the functionality of the new product, as well as the product's impact on privacy. | | | |
| D-9 | <p>The Facebook and Instagram privacy policies disclose the use of cookies, pixels, and local storage and the types of uses for which those technologies are utilized. The user is advised that they may have device or browser options to block or remove cookies or other data stored on their computer or device and that doing so may limit their ability to use Facebook's products and services.</p> | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 40 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|---|---------------------------|--------------------|------------------------|
| <p>Assertion D. Notice, Choice, Consent, Collection and Access</p> <p>Facebook provides notice about its privacy policies and procedures and terms of service to users which identifies the purposes for which personal information is collected and used, describes the choices available to users, obtains implicit or explicit consent, collects personal information only for the purposes identified in the notices and provides users with access to their personal information for review and update.</p> | | | | |
| | <p>The privacy policy is made available to users at the time of account creation. By clicking on the "Sign Up" or "Register" button during account creation, the user provides consent for Facebook and Instagram to utilize these technologies.</p> | <p>(b)(3):6(f),(b)(4)</p> | | |
| D-10 | <p>Facebook's Data Use Policy and Instagram's privacy policy addresses the following:</p> <ul style="list-style-type: none"> • Collection of user information. For example, the "Information we receive about you" section describes the different types of information collected from users. • Discloses to users the different types of information collected about them and the sources of the information collected. • The types of personal information collected from users and the general methods of collection. • How a user can access or download their information. • The company may develop and acquire information about the individual using third-party sources, browsing, credit and purchasing history. | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 41 of 79 HIGHLY CONFIDENTIAL



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|---|---------------------------|--------------------|------------------------|
| <p>Assertion D. Notice, Choice, Consent, Collection and Access</p> <p>Facebook provides notice about its privacy policies and procedures and terms of service to users which identifies the purposes for which personal information is collected and used, describes the choices available to users, obtains implicit or explicit consent, collects personal information only for the purposes identified in the notices and provides users with access to their personal information for review and update.</p> | | | | |
| D-11 | <p>Facebook users and non-users can access their personal information via the following methods:</p> <p>(1) By logging into their active Facebook account to review, update, delete or correct information previously provided.</p> <p>(2) By downloading a copy of the information they have provided Facebook by visiting "Account Settings" and clicking on "Download a copy of your Facebook data" on facebook.com. This takes you to the "Download Your Information" (DYI) tool. Once the archive has been systematically generated, an email is sent to the email address on record for the user with a link to the file(s). The user is required to re-authenticate by entering his or her Facebook account password.</p> <p>(3) By downloading publicly available information through Facebook's Graph API by typing https://www.facebook.com/[User ID or Username]?metadata=1 into their browser.</p> <p>(4) By requesting access to their data by clicking the "Personal data requests" link under "Help" on Facebook.com. Facebook responds within a reasonable period of time, typically 40 days. UO tracks and documents responses to user data access requests using the TPS system. Facebook holds limited information for non-users (usually limited to e-mail address), which is stored on behalf of the user who shared that information.</p> | <p>(b)(3):6(f),(b)(4)</p> | | |



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|---|---------------------------|--------------------|------------------------|
| <p>Assertion D. Notice, Choice, Consent, Collection and Access</p> <p>Facebook provides notice about its privacy policies and procedures and terms of service to users which identifies the purposes for which personal information is collected and used, describes the choices available to users, obtains implicit or explicit consent, collects personal information only for the purposes identified in the notices and provides users with access to their personal information for review and update.</p> | | | | |
| D-12 | <p><u>Instagram only</u></p> <p>Instagram users can access their personal information via the following methods:</p> <p>(1) By logging into their Instagram account to review, update, delete or correct information previously provided.</p> <p>(2) By requesting any personal information associated with their account (e.g., pictures, email, and phone number) through the Help Center.</p> | <p>(b)(3):6(f),(b)(4)</p> | | |
| D-13 | <p>Facebook does not deny active users access to their personal information displayed on Facebook.com, unless the user violates Facebook's policies, and/or the users' account has been compromised or excessive login attempts have been made.</p> <p>In the event a user account is disabled for violating Facebook's policies, Facebook will communicate to the user, upon his or her attempt to log in, why access has been denied. Users may appeal the disablement via email to Facebook. These appeals are tracked via TPS tickets.</p> <p>In the event a user encounters a login issue and cannot access their account because the account has been compromised, Facebook offers ways for the user to regain access to his or her account through the Facebook Help Center.</p> | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 43 of 79 HIGHLY CONFIDENTIAL



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|--|-----------------------|--------------------|------------------------|
| Assertion E - Use, Retention, Deletion and Quality | | | | |
| Facebook limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. Facebook retains personal information for as long as necessary to provide services or fulfil the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information. Facebook maintains accurate, complete, and relevant personal information for the purposes identified in the notice. | | | | |
| E-1 | The privacy policy and terms of service addresses the use, retention, and deletion of user information, as well as the deletion and retention of individual content. | (b)(3):6(f),(b)(4) | | |
| E-2 | The Privacy XFN process ensures that uses of data are evaluated to determine whether additional notice or consent is required. Where required, key decisions around the need for additional consent from users are discussed and recommendations are made by the XFN team. | | | |
| E-3 | (b)(3):6(f),(b)(4) | | | |
| E-4 | | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 44 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|-----------------------------|-----------------------|--------------------|------------------------|
| Assertion E - Use, Retention, Deletion and Quality | | | | |
| Facebook limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. Facebook retains personal information for as long as necessary to provide services or fulfil the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information. Facebook maintains accurate, complete, and relevant personal information for the purposes identified in the notice. | | | | |
| E-5 | (b)(3):6(f),(b)(4) | | | |
| E-6 | | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 45 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|--|-----------------------|--------------------|------------------------|
| Assertion E - Use, Retention, Deletion and Quality | | | | |
| Facebook limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. Facebook retains personal information for as long as necessary to provide services or fulfil the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information. Facebook maintains accurate, complete, and relevant personal information for the purposes identified in the notice. | | | | |
| E-7 | (b)(3):6(f),(b)(4) | (b)(3):6(f),(b)(4) | | |
| E-8 | <u>Instagram only:</u> When a user requests their Instagram account to be deleted, the user's account, photos and comments are no longer viewable by other Instagram users. | | | |
| E-9 | (b)(3):6(f),(b)(4) | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 46 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|---|-----------------------|--------------------|------------------------|
| Assertion E - Use, Retention, Deletion and Quality | | | | |
| Facebook limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. Facebook retains personal information for as long as necessary to provide services or fulfil the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information. Facebook maintains accurate, complete, and relevant personal information for the purposes identified in the notice. | | | | |
| E-10 | Facebook's Statement of Rights and Responsibilities contains a section stating that users consent to not provide any false personal information on Facebook and have the responsibility to keep such information accurate and up-to-date. | (b)(3):6(f),(b)(4) | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 47 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|--|--|-----------------------|--------------------|------------------------|
| Assertion F - Security for Privacy | | | | |
| Facebook protects personal information of users against unauthorized access. | | | | |
| F-1 | A program is established to maintain and increase the security awareness of employees. | (b)(3):6(f),(b)(4) | | |
| F-2 | (b)(3):6(f),(b)(4) | | | |
| F-3 | | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 48 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|--|-----------------------------|-----------------------|--------------------|------------------------|
| Assertion F - Security for Privacy | | | | |
| Facebook protects personal information of users against unauthorized access. | | | | |
| F-4 | (b)(3):6(f),(b)(4) | | | |
| F-5 | | | | |
| F-6 | | | | |
| F-7 | | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 49 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|--|--|-----------------------|--------------------|------------------------|
| Assertion F - Security for Privacy | | | | |
| Facebook protects personal information of users against unauthorized access. | | | | |
| F-8 | Facebook's systems are configured to enforce strong passwords for user accounts that access internal systems. The password policy requires a minimum password length and the password must meet certain complexity requirements. | (b)(3):6(f),(b)(4) | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 50 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|--|-----------------------------|-----------------------|--------------------|------------------------|
| Assertion F - Security for Privacy | | | | |
| Facebook protects personal information of users against unauthorized access. | | | | |
| | | | | (b)(3):6(f),(b)(4) |
| F-9 | (b)(3):6(f),(b)(4) | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 51 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|--|-----------------------------|-----------------------|--------------------|------------------------|
| Assertion F - Security for Privacy | | | | |
| Facebook protects personal information of users against unauthorized access. | | | | |
| | | (b)(3):6(f),(b)(4) | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 52 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|--|-----------------------------|-----------------------|--------------------|------------------------|
| Assertion F - Security for Privacy | | | | |
| Facebook protects personal information of users against unauthorized access. | | | | |
| | | | | (b)(3):6(f),(b)(4) |
| F-10 | (b)(3):6(f),(b)(4) | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 53 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|--|-----------------------------|-----------------------|--------------------|------------------------|
| Assertion F - Security for Privacy | | | | |
| Facebook protects personal information of users against unauthorized access. | | | | |
| | | | | (b)(3):6(f),(b)(4) |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 54 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|--|-----------------------------|-----------------------|--------------------|------------------------|
| Assertion F - Security for Privacy | | | | |
| Facebook protects personal information of users against unauthorized access. | | | | |
| | | | | (b)(3):6(f),(b)(4) |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 55 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|--|-----------------------------|-----------------------|--------------------|------------------------|
| Assertion F - Security for Privacy | | | | |
| Facebook protects personal information of users against unauthorized access. | | | | |
| | | | | (b)(3):6(f),(b)(4) |
| F-11 | (b)(3):6(f),(b)(4) | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 56 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|--|-----------------------------|-----------------------|--------------------|------------------------|
| Assertion F - Security for Privacy | | | | |
| Facebook protects personal information of users against unauthorized access. | | | | |
| | | | | (b)(3):6(f),(b)(4) |
| F-12 | (b)(3):6(f),(b)(4) | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 57 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|--|-----------------------|--------------------|------------------------|
| Assertion F - Security for Privacy | | | | |
| Facebook | protects personal information of users against unauthorized access | | | |
| F-13 | (b)(3):6(f),(b)(4) | | | |
| F-14 | | | | |
| F-15 | | | | |
| | | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 58 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|--|-----------------------------|-----------------------|--------------------|------------------------|
| Assertion F - Security for Privacy | | | | |
| Facebook protects personal information of users against unauthorized access. | | | | |
| F-16 | (b)(3):6(f),(b)(4) | | | |
| F-17 | | | | |
| F-18 | | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 59 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|--|-----------------------------|-----------------------|--------------------|------------------------|
| Assertion F - Security for Privacy | | | | |
| Facebook protects personal information of users against unauthorized access. | | | | |
| F-19 | (b)(3):6(f),(b)(4) | | | |
| F-20 | | | | (b)(3):6(f),(b)(4) |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 60 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|--|---|-----------------------|--------------------|------------------------|
| Assertion F - Security for Privacy | | | | |
| Facebook protects personal information of users against unauthorized access. | | | | |
| | | | | (b)(3):6(f),(b)(4) |
| F-21 | Facebook's data centers are equipped with environmental controls, including fire suppression systems and fire extinguishers; air conditioning systems; water detection systems; and alternative power supply. | (b)(3):6(f),(b)(4) | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 61 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|--|---|-----------------------|--------------------|------------------------|
| Assertion F - Security for Privacy | | | | |
| Facebook protects personal information of users against unauthorized access. | | | | |
| F-22 | Monitoring of data centers is performed through regularly scheduled reviews of physical and environmental controls as well as periodic reviews of physical security access lists. | (b)(3):6(f),(b)(4) | | |
| F-23 | (b)(3):6(f),(b)(4) | | | |
| F-24 | | | | |
| F-25 | Direct access to user data on Facebook production servers is restricted to authorized personnel. | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 62 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|---|---------------------------|--------------------|------------------------|
| Assertion G - Third-party developers | | | | |
| Facebook discloses personal information to third-party developers only for the purposes identified in the notice and with the implicit or explicit consent of the individual. | | | | |
| G-1 | <p>Facebook has the following formal policies in place to ensure that personal information is disclosed only to developers who have agreements with Facebook to protect personal information in a manner consistent with Facebook's privacy program:</p> <ul style="list-style-type: none"> • Data Use Policy, which informs users about how information is disclosed to applications created by developers when a user connects to those applications. • Facebook's platform policies, which provide specific instructions and details to developers on the handling of user information. • Statement of Rights and Responsibilities, which details specific requirements for handling personal information and the responsibility of the developer to disclose a privacy policy to end users. <p>Non-branded Facebook application developers - Third party developers who leverage on Facebook's Application Programming Interface (API) and tokenization to interact with Facebook users.</p> <p>Facebook Experience (branded) application developers – Third party developer partners who develop Facebook-branded applications as a</p> | <p>(b)(3):6(f),(b)(4)</p> | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 63 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|---|-----------------------|--------------------|------------------------|
| Assertion G - Third-party developers | | | | |
| Facebook discloses personal information to third-party developers only for the purposes identified in the notice and with the implicit or explicit consent of the individual. | | | | |
| | conduit for interfacing with Facebook services and user data (e.g., Microsoft - "Facebook for Windows"; RIM - "Facebook for Blackberry"). Refer to Assertion H – Service providers for an outline of the control activities that relate to this type of developer. | | | |
| G-2 | <p>Developers must read and sign-off on Facebook's Data Use Policy and Platform Policies during the developer registration process.</p> <p>The developer is responsible for disclosing their own privacy policy to users of their application(s).</p> | (b)(3):6(f),(b)(4) | | |
| G-3 | <p><u>Instagram only:</u> Instagram's "API Terms of Use" and developer site provide specific instructions and details to developers on the handling of user information.</p> <p>Developers must agree to Instagram's terms of service during the developer sign up process, which also details specific requirements for handling personal information and the responsibility of the developer to disclose a privacy policy to its users.</p> <p>Instagram data obtained through the API is consistent with a user's privacy settings and status.</p> | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 64 of 79 HIGHLY CONFIDENTIAL



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|-----------------------------|-----------------------|--------------------|------------------------|
| Assertion G - Third-party developers | | | | |
| Facebook discloses personal information to third-party developers only for the purposes identified in the notice and with the implicit or explicit consent of the individual. | | | | |
| G-4 | (b)(3):6(f),(b)(4) | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 65 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|--|---|-----------------------|--------------------|------------------------|
| Assertion H - Service Providers | | | | |
| Facebook has developed and used reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from the Company and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information. | | | | |
| H-1 | The privacy policies of Facebook and Instagram contain a section that informs users that the information Facebook and Instagram receive may be shared with service organizations when a user signs up for Facebook and Instagram accounts. | (b)(3):6(f),(b)(4) | | |
| H-2 | (b)(3):6(f),(b)(4) | | | |
| H-3 | Facebook Experience application developers (e.g., Microsoft and RIM) must read and sign-off on the Extended API Addendum (the "Addendum"), or other similar agreement, which sets forth the terms and conditions for a developer's adherence to Facebook's Platform | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 66 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|--|---|-----------------------|--------------------|------------------------|
| Assertion H - Service Providers | | | | |
| Facebook has developed and used reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from the Company and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information. | | | | |
| | Policies, Statement of Rights and Responsibilities and data policies and procedures, which includes consideration of the following privacy-related requirements: <ul style="list-style-type: none"> • Purpose of Use • Restrictions on Use • Deletion of Data • No Transfer • Updates of Data • Storage | | | |
| H-4 | (b)(3):6(f),(b)(4) | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 67 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|--|-----------------------------|-----------------------|--------------------|------------------------|
| Assertion H - Service Providers | | | | |
| Facebook has developed and used reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from the Company and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information. | | | | |
| | | (b)(3):6(f),(b)(4) | | |
| H-5 | (b)(3):6(f),(b)(4) | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 68 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|--|-----------------------------|-----------------------|--------------------|------------------------|
| Assertion H - Service Providers | | | | |
| Facebook has developed and used reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from the Company and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information. | | | | |
| | | | | (b)(3):6(f),(b)(4) |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 69 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|--|---|-----------------------|--------------------|------------------------|
| Assertion H - Service Providers | | | | |
| Facebook has developed and used reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from the Company and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information. | | | | |
| H-6 | Service provider contracts may be terminated if Facebook identifies misuse of user information (based on violations of the Statement of Rights and Responsibilities and/or the vendor security policy). | (b)(3):6(f),(b)(4) | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 70 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|---|-----------------------|--------------------|------------------------|
| <p>Assertion I - On-going Monitoring of the Privacy Program</p> <p>Facebook evaluates and adjusts the Company's privacy program in light of the results of monitoring activities, any material changes to the Company's operations or business arrangements, or any other circumstances that the Company knows or has reason to know may have a material impact on the effectiveness of its privacy program.</p> | | | | |
| I-1 | (b)(3):6(f),(b)(4) | (b)(3):6(f),(b)(4) | | |
| I-2 | <p>The XFN process ensures that new products and changes to existing products that result in material and/or retroactive changes to the use of information are evaluated to determine whether additional notice or consent from Facebook users is required. Where required, key decisions around the need for additional consent from users are discussed and recommendations are made and implemented by the XFN team.</p> | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 71 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|-----------------------------|-----------------------|--------------------|------------------------|
| Assertion I - On-going Monitoring of the Privacy Program | | | | |
| Facebook evaluates and adjusts the Company's privacy program in light of the results of monitoring activities, any material changes to the Company's operations or business arrangements, or any other circumstances that the Company knows or has reason to know may have a material impact on the effectiveness of its privacy program. | | | | |
| I-3 | (b)(3):6(f),(b)(4) | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 72 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|-----------------------------|-----------------------|--------------------|------------------------|
| Assertion I - On-going Monitoring of the Privacy Program | | | | |
| Facebook evaluates and adjusts the Company's privacy program in light of the results of monitoring activities, any material changes to the Company's operations or business arrangements, or any other circumstances that the Company knows or has reason to know may have a material impact on the effectiveness of its privacy program. | | | | |
| I-4 | (b)(3):6(f),(b)(4) | | | |
| I-5 | | | | |
| I-6 | | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 73 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|-----------------------------|-----------------------|--------------------|------------------------|
| Assertion I - On-going Monitoring of the Privacy Program | | | | |
| Facebook evaluates and adjusts the Company's privacy program in light of the results of monitoring activities, any material changes to the Company's operations or business arrangements, or any other circumstances that the Company knows or has reason to know may have a material impact on the effectiveness of its privacy program. | | | | |
| (b)(3):6(f),(b)(4) | | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 74 of 79

HIGHLY CONFIDENTIAL



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|---|---|-----------------------|--------------------|------------------------|
| Assertion I - On-going Monitoring of the Privacy Program | | | | |
| Facebook evaluates and adjusts the Company's privacy program in light of the results of monitoring activities, any material changes to the Company's operations or business arrangements, or any other circumstances that the Company knows or has reason to know may have a material impact on the effectiveness of its privacy program. | | | | |
| | | (b)(3):6(f),(b)(4) | | |
| I-7 | (b)(3):6(f),(b)(4) | | | |
| I-8 | Facebook's Help Center provides information on how to contact the company with inquiries, complaints and disputes. Users can use e-mail or the "Report" button on the site or in Facebook's products to communicate with Facebook's User Operations (UO) team. The Help Center can be accessed from the "Help" link on any Facebook page. | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 75 of 79 **HIGHLY CONFIDENTIAL**



| Ref. | Facebook's Control Activity | PwC's Tests Performed | PwC's Test Results | Additional Information |
|--|-----------------------------|-----------------------|--------------------|------------------------|
| Assertion I - On-going Monitoring of the Privacy Program Facebook evaluates and adjusts the Company's privacy program in light of the results of monitoring activities, any material changes to the Company's operations or business arrangements, or any other circumstances that the Company knows or has reason to know may have a material impact on the effectiveness of its privacy program. | | | | |
| I-9 | (b)(3):6(f),(b)(4) | | | |
| I-10 | | | | |
| | | | | |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
 Page 76 of 79 **HIGHLY CONFIDENTIAL**



Management's Assertion

The management of Facebook represents that as of and for the 180 days ended February 11, 2013 ("the Reporting Period"), in accordance with Parts IV and V of the Agreement Containing Consent Order ("The Order"), with a service date of August 15, 2012, between Facebook, Inc. ("the Company") and the United States of America, acting upon notification and authorization by the Federal Trade Commission ("FTC"), the Company had established and implemented a comprehensive Privacy Program, ("the Facebook Privacy Program"), based on Company specific criteria (described in paragraph two of this assertion); and the privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the Reporting Period.

The company specific criteria ("assertions") used as the basis for Facebook's Privacy Program are described below. The below assertions have corresponding controls on pages 21-76.

Assertion A - Responsibility for the Facebook Privacy Program, which is "Facebook has designated an employee or employees to coordinate and be responsible for the privacy program."

Assertion B - Privacy Risk Assessment, which is "Facebook has identified reasonably foreseeable, material risks, both internal and external, 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. This privacy risk assessment includes consideration of risks in areas of relevant operations, including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research."

Assertion C - Privacy and Security Awareness, which is "Facebook has a privacy and security for privacy awareness program in place which is defined and documented in privacy and security for privacy policies. The extent of communications to employees is based on their role and responsibility and may include internal communications through various channels, training, and the Privacy Cross-Functional ("XFN") team process."

Assertion D - Notice, Choice, Consent, Collection and Access, which is "Facebook provides notice about its privacy policies and procedures and terms of service to users which identifies the purposes for which personal information is collected and used, describes the choices available to users, obtains implicit or explicit consent, collects personal information only for the purposes identified in the notices and provides users with access to their personal information for review and update."

Assertion E - Use, Retention, Deletion and Quality, which is "Facebook limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. Facebook retains personal information for as long as necessary to provide services or fulfil the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information. Facebook maintains accurate, complete, and relevant personal information for the purposes identified in the notice."

1601 Willow Road, Menlo Park, California 94025
650.543.4800 – tel 650.543.4801 – fax

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 77 of 79 **HIGHLY CONFIDENTIAL**



Assertion F - Security for Privacy, which is “Facebook protects personal information of users against unauthorized access.”

Assertion G - Third-party developers, which is “Facebook discloses personal information to third-party developers only for the purposes identified in the notice and with the implicit or explicit consent of the individual.”

Assertion H - Service Providers, which is “Facebook has developed and used reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from the Company and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information.”

Assertion I - On-going Monitoring of the Privacy Program, which is “Facebook evaluates and adjusts the Company’s privacy program in light of the results of monitoring activities, any material changes to the Company’s operations or business arrangements, or any other circumstances that the Company knows or has reason to know may have a material impact on the effectiveness of its privacy program.”

Facebook, Inc.

By: _____

Edward Palmieri
Associate General Counsel, Privacy
Facebook, Inc.

By: _____

Daniel Li
Product Counsel
Facebook, Inc.

1601 Willow Road, Menlo Park, California 94025
650.543.4800 – tel 650.543.4801 – fax

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 78 of 79 **HIGHLY CONFIDENTIAL**



Appendix A – Assessment Interviews Summary

The primary Facebook individuals interviewed by PwC, as a part of the above Assessment procedures, include, but are not limited to, those individuals listed in the table below.

| Title | Team |
|---|--------------------------------|
| Chief Privacy Officer, Product | Privacy |
| Chief Privacy Officer, Policy | Public Policy |
| VP & Deputy General Counsel | Legal |
| Associate General Counsel, Privacy | Legal |
| Privacy & Product Counsel | Legal |
| Lead Contracts Manager | Legal |
| Compliance Associate | Legal |
| Privacy Program Manager | Identity |
| Specialist, User Operations | User Operations |
| Engineering Manager | Engineering |
| Software Engineer | Engineering |
| Developer Policy Enforcement Manager | Developer Operations |
| Platform Operations Analyst | Developer Operations |
| Chief Security Officer | Security |
| Manager, Information Security | Security |
| Policy and Operations Analyst | Security |
| Security Manager, Incident Response | Security |
| Mobile Program Manager | Mobile Partner Management |
| Recruiting Process Manager | Human Resources |
| US Data Center Operations Director | Infrastructure |
| Group Technical Program Manager | Infrastructure |
| Engineering Manager (formerly Instagram Chief Technology Officer) | Instagram - Engineering |
| User Operations Manager | Instagram - User Operations |
| Product Manager | Instagram - Product Management |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 79 of 79 **HIGHLY CONFIDENTIAL**

EXHIBIT 6

The Facebook logo is displayed in white lowercase letters on a dark, textured rectangular background.

April 22, 2013

VIA EMAIL AND FEDERAL EXPRESS

James A. Kohm Esq.
Associate Director for the Division of Enforcement
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, DC 20850

Re: *In re Facebook, Inc.*, FTC Docket No. C-4365

Dear Mr. Kohm:

In accordance with Part V of the Decision and Order entered in *In re Facebook*, Docket No. C-4365 (July 27, 2012) ("FTC Order"), enclosed please find a copy of the assessment and report ("Assessment"), prepared by a qualified, objective, independent third-party professional ("Independent Assessor"), examining the sufficiency of the privacy controls that Facebook maintained during the period from August 15, 2012 to February 11, 2013. We are pleased that the Assessment concludes that our Privacy Program was operating effectively throughout the reporting period. This conclusion is based on an exhaustive examination of our program, conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants ("AICPA").

The Facebook Privacy Program

Privacy is central to everything we do at Facebook. Since our founding less than a decade ago, we have worked to develop practices and procedures that ensure that people's personal information is safe, secure, and used in accordance with their sharing settings and choices. Our privacy efforts received a substantial boost in 2011 and 2012, when the Data Protection Commissioner ("DPC") in Ireland, where Facebook's international headquarters is located, undertook the first major governmental review of an internet company's compliance with European data protection law. That review resulted in two comprehensive audit reports that documented Facebook's controls, addressed and rejected a number of misperceptions about how Facebook approaches privacy, and identified areas where we can continue to improve. Facebook Ireland, Ltd., continues to work closely with the DPC to ensure ongoing compliance with EU privacy and data protection law.

The Privacy Program reflected in the attached Assessment built upon our work with the Irish DPC. In developing our program, we went beyond the general requirements set out in Section IV of the FTC Order and leveraged the Generally Accepted Privacy Principles

1601 Willow Road, Menlo Park, California 94025
650.543.4800 - tel 650.543.4801 - fax



("GAPP"), a comprehensive framework created by the AICPA and Canadian Institute of Chartered Accountants. The GAPP framework is the most comprehensive standard for privacy programs, derived from ten internationally-recognized information principles, including notice, choice and consent, access obligations, and limitations on the use, retention, disposal, and disclosure of personal information. We used the GAPP principles and criteria as a guide in developing our own company-specific privacy assertions and controls. Key features of our program include: (a) the designation of responsible employees, including an experienced Privacy Governance Team, (b) comprehensive awareness and training for all employees, appropriate to their job functions, (c) consideration of privacy issues throughout the development process (i.e., "privacy by design"), (d) robust security for privacy controls, (e) safeguards for Platform developers, (f) screening and contractual obligations for service providers, and (g) assessment and integration of acquisitions.

We also have invested in building innovative tools that provide people with control over the sharing of their information. Our Per-Object Privacy controls and Granular Data Permissions model, for example, enable users to choose, at the time of sharing, the specific audience for each piece of content they share and to have direct visibility into the information available to applications they use. Likewise, our Data Use Policy presents layered content, practical headings and screenshots to help users understand how the information they provide is used and shared. We have strengthened existing controls, like Activity Log, which allows people to sort, review, delete or hide the things they post on Facebook. In addition, we continue to launch new controls, such as our privacy shortcuts, which are located at the top of most pages on Facebook and allow users to quickly access key settings and easily visit their main settings page. We believe these tools demonstrate our commitment to achieving the balance users want between sharing information quickly and easily while maintaining appropriate privacy and control.

Independent Assessment

The attached report is a comprehensive assessment of our Privacy Program. It documents our assertions and controls and, for each, describes the testing procedures used to gauge whether the control was operating effectively. The Assessment also identifies areas where control design and/or operating effectiveness can continue to improve. This report follows fifteen weeks of intense on-site work by the Independent Assessor at Facebook's headquarters in Menlo Park. As part of that process, the Independent Assessor engaged in over 65 in-person meetings with key individuals involved in our program (e.g., the Chief Security Officer, the Chief Privacy Officer, Product, the Chief Privacy Officer, Policy) and examined a wide range of materials—including, among other things, written policies and procedures and representative data sets. The Independent Assessor was comprised of thirteen team members with cross-disciplinary experience in privacy, assessment, and technology and led by a partner with decades of experience in the area of data protection and privacy. Among the team were Certified Information Privacy Professionals, Certified Information Systems Auditors, and Certified Public Accountants. In addition, individuals with specialized experience in the Independent Assessor's

1601 Willow Road, Menlo Park, California 94025
650.543.4800 - tel 650.543.4801 - fax



quality assurance and risk management practices were consulted and brought into the assessment as needed.

At Facebook, we put privacy at the core of our mission. The attached Assessment reaffirms our commitment to implementing meaningful and effective privacy and security controls. While the Assessment reflects our years of privacy and security innovation and expertise, we view this commitment as ongoing. We will continue to work to meet the changing and evolving needs of our users and to put user privacy and security at the center of everything we do. The Privacy Program – and the Assessment – provide a clear, positive framework for Facebook to move forward in this pursuit.

* * *

Request for Confidentiality

Pursuant to 16 C.F.R. § 4.10(a)(2), we have enclosed two versions of the Assessment – a confidential version that contains highly confidential Facebook and Independent Assessor commercial and trade secret information, and a non-confidential version that redacts such information.

The redacted text contains detailed trade secret information regarding the design and testing of the Facebook Privacy Program. We believe that release of the redacted information would place user information at risk, as it would reveal detailed information regarding the specific strengths and possible limitations of the Facebook Privacy Program to hackers and other third parties that may attempt to infiltrate our system in the future. Furthermore, public disclosure of this information would place both Facebook and the Independent Assessor at a competitive disadvantage vis-à-vis competitors, who could use the information to mimic Facebook's industry-leading development processes or the Independent Assessor's proprietary testing protocols.

For these reasons, we respectfully request that the Commission treat the redacted information as confidential and not subject to the Freedom of Information Act, pursuant to 5 U.S.C. § 552(b)(4).

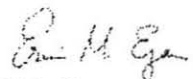
* * *

We hope that you find the information above and the enclosed Assessment informative. Please do not hesitate to contact us should you have any questions.

Sincerely,



Michael Richter
Chief Privacy Officer, Product



Erin Egan
Chief Privacy Officer, Policy

1601 Willow Road, Menlo Park, California 94025
650.543.4800 - tel 650.543.4801 - fax



Independent Assessor's Report on Facebook's Privacy Program

Initial Assessment Report

For the period August 15, 2012 to
February 11, 2013

The contents of this document, including the Report of Independent Accountants, contain PricewaterhouseCoopers LLP proprietary information that shall be protected from disclosure outside of the U.S. Government in accordance with the U.S. Trade Secrets Act and Exemption 4 of the U.S. Freedom of Information Act (FOIA). The document constitutes and reflects work performed or information obtained by PricewaterhouseCoopers LLP, in our capacity as independent assessor for Facebook, Inc. for the purpose of the Facebook, Inc.'s Order. The document contains proprietary information, trade secrets and confidential commercial information of our firm and Facebook, Inc. that is privileged and confidential, and we expressly reserve all rights with respect to disclosures to third parties. Accordingly, we request confidential treatment under FOIA, the U.S. Trade Secrets Act or similar laws and regulations when requests are made for the report or information contained therein or any documents created by the FTC containing information derived from the report. We further request that written notice be given to PwC and Facebook, Inc. before distribution of the information in the report (or copies thereof) to others, including other governmental agencies, to afford our firm and Facebook, Inc. with the right to assert objections and defenses to the release of the information as permitted under FOIA or other similar applicable law or regulation, except when such distribution is already required by law or regulation. This report is intended solely for the information and use of the management of Facebook, Inc. and the U.S. Federal Trade Commission and is not intended to be and should not be used by anyone other than these specified parties.

HIGHLY CONFIDENTIAL



Table of Contents

| | |
|---|----|
| Introduction | 3 |
| Report of Independent Accountants | 4 |
| Facebook's Privacy Program Overview | 6 |
| PwC's Privacy Assessment Approach | 14 |
| PwC's Assessment of Part IV A, B, C, D and E. of the Order | 18 |
| Facebook's Privacy Program: Assertions, Control Activities and PwC's Tests Performed and Results | 21 |
| Management's Assertion | 77 |
| Appendix A – Assessment Interviews Summary | 79 |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 2 of 79 **HIGHLY CONFIDENTIAL**



Introduction

Facebook, Inc. and the Federal Trade Commission (FTC) entered into Agreement Containing Consent Order File No: 0923184 ("the Order"), which was served on August 15, 2012.

Part IV of the Order requires Facebook to establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information.

Part V of the Order requires Facebook to obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Facebook engaged PricewaterhouseCoopers LLP ("PwC") to perform the initial assessment.

As described on pages 6-13, Facebook established its privacy program by implementing privacy controls to meet or exceed the protections required by Part IV of the Order. As described on pages 14-17, PwC performed inquiry, observation, and inspection/examination procedures to assess the effectiveness of the Facebook privacy controls implemented to meet or exceed the protections required by Part IV of the Order during the first 180 day period ended February 11, 2013, and our conclusions are on pages 4-5.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 3 of 78 **HIGHLY CONFIDENTIAL**



Report of Independent Accountants

To the Management of Facebook, Inc.:

We have examined Management's Assertion, that as of and for the 180 days ended February 11, 2013 (the "Reporting Period"), in accordance with Parts IV and V of the Agreement Containing Consent Order (the "Order") with an effective date of service of August 15, 2012, between Facebook, Inc. ("Facebook" or "the Company") and the United States of America, acting upon notification and authorization by the Federal Trade Commission ("FTC"), the Company had established and implemented a comprehensive Privacy Program, as described in Management's Assertion ("the Facebook Privacy Program"), based on Company-specific criteria, and the privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the Reporting Period.

The Company's management is responsible for the assertion. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and accordingly, included examining, on a test basis, evidence supporting the effectiveness of the Facebook Privacy Program as described above and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

We are not responsible for Facebook's interpretation of, or compliance with, information security or privacy-related laws, statutes, and regulations applicable to Facebook in the jurisdictions within which Facebook operates. We are also not responsible for Facebook's interpretation of, or compliance with, information security or privacy-related self-regulatory frameworks. Therefore, our examination did not extend to the evaluation of Facebook's interpretation of or compliance with information security or privacy-related laws, statutes, regulations, and privacy-related self-regulatory frameworks with which Facebook has committed to comply.

In our opinion, Facebook's privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the Reporting Period, in all material respects as of and for the 180 days ended February 11, 2013, based upon the Facebook Privacy Program set forth in Management's Assertion.

(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 4 of 79 **HIGHLY CONFIDENTIAL**



This report is intended solely for the information and use of the management of Facebook and the United States Federal Trade Commission and is not intended to be and should not be used by anyone other than these specified parties.

PricewaterhouseCoopers L.L.P.

San Jose

April 16, 2013

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 5 of 79 **HIGHLY CONFIDENTIAL**



Facebook's Privacy Program Overview

Company Overview

Founded in 2004, Facebook's mission is to give people the power to share and make the world more open and connected. Facebook has been working on privacy since its inception and consistently strives to enhance various elements of its internal privacy programs. For example, Facebook now has a Privacy Cross-Functional ("XFN") internal team (comprised of experts with a range of privacy expertise) that vets and reviews products during the development cycle and before launch. Facebook also created two new corporate officer roles— Chief Privacy Officer, Product and Chief Privacy Officer, Policy—who are charged with ensuring that Facebook's commitments are reflected in all of its activities.

Facebook supports its mission by developing useful and engaging tools that enable people to connect, share, discover, and communicate with each other on mobile devices and computers. Facebook's products include News Feed, Timeline, Platform, Graph Search, Messages, Photos and Video, Groups, Events, and Pages. These products are available through Facebook's website, Facebook.com. They are also accessible through certain Facebook mobile applications or "apps", including Facebook, Camera, Messenger, Pages, and Poke. Versions of Facebook's mobile apps are available for multiple operating systems, such as iOS and Android operating systems. These products and services allow people all over the world to share, and communicate with each other in new and innovate ways, connecting people in ways not possible before these tools were offered.

Facebook Platform ("Platform") is a set of development tools and application programming interfaces ("APIs") that enable developers to build their own social apps, websites, and devices that integrate with Facebook. The Facebook's Developer Operations team is focused on supporting successful applications, driving platform adoption, and maintaining the user experience through developer education and policy enforcement. The Platform Principles that Facebook imposes on all developers are: (1) Create a great user experience (Build social and engaging applications; Give users choice and control; and Help users share expressive and relevant content); and (2) Be trustworthy (Respect privacy; Don't mislead, confuse, defraud, or surprise users; and Don't spam - encourage authentic communications). Additionally, Facebook's Statement of Rights and Responsibilities and Platform Policies outline a variety of developer obligations, including those around privacy, such as providing notice and obtaining consent for certain data uses and restrictions on sharing user information.

Most products and services Facebook offers are free. Facebook is able to do this by providing value for marketers, including brand marketers, small and medium-sized businesses, and developers. Facebook offers a unique combination of reach, relevance, social context, and engagement. Marketers can also use Facebook's analytics platform, Facebook Ad Analytics, to understand and optimize the performance of their campaigns.

In addition to Facebook created products and services, Facebook acquired Instagram on August 31, 2012. Instagram is a photo sharing service that enables users to take photos, apply digital filters to the photos, share them with others, and comment on photos posted by themselves or by others. At the time of acquisition, Instagram had approximately 13 employees. During the reporting period subsequent to the acquisition, Instagram was

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 6 of 79

HIGHLY CONFIDENTIAL



available on the web at Instagram.com and as an app on the iOS and Android operating systems.

Facebook Privacy Program Scope

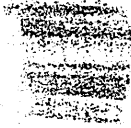
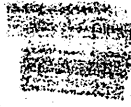
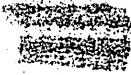
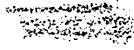
Facebook designed the Privacy Program to accomplish two primary objectives: (a) to address privacy risks related to the development, management, and use of new and existing products; and (b) to protect the privacy and confidentiality of the information Facebook receives from or about consumers. Facebook leveraged the Generally Accepted Privacy Principles ("GAPP") framework, set forth by the American Institute of Certified Public Accountants ("AICPA") and Canadian Institute of Chartered Accountants ("CICA"), to define company-specific criteria for the foundation of the Facebook Privacy Program. The GAPP framework is globally recognized as a leading and comprehensive standard for privacy programs.

The ten GAPP principles, which are derived from internationally recognized information practices, are as follows:

1. **Management.** The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.
2. **Notice.** The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
3. **Choice and consent.** The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
4. **Collection.** The entity collects personal information only for the purposes identified in the notice.
5. **Use, retention, and disposal.** The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.
6. **Access.** The entity provides individuals with access to their personal information for review and update.
7. **Disclosure to third parties.** The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
8. **Security for privacy.** The entity protects personal information against unauthorized access (both physical and logical).
9. **Quality.** The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
10. **Monitoring and enforcement.** The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related complaints and disputes.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 7 of 79

HIGHLY CONFIDENTIAL





The following is a brief description of the Facebook Privacy Program.

Facebook has designated a team of employees who are directly responsible for the Facebook Privacy Program (the "Privacy Governance Team"). Facebook's Chief Privacy Officer, Product leads the Privacy Governance Team. Other team members include the Chief Privacy Officer, Policy; Chief Security Officer, Associate General Counsel, Privacy; Associate General Counsel, Privacy and Product; Associate General Counsel, Advertising and Product; and Associate General Counsel, Regulatory. While the Chief Privacy Officer, Product provides leadership responsibility for coordinating the Privacy Program, the entire Privacy Governance Team and many employees (including engineers, product managers, etc.) are responsible for various aspects of the Privacy Program and play a crucial role driving and implementing decisions made by the Privacy Governance Team. Of particular note are the Privacy Program Managers who work directly under Chief Privacy Officer, Product. This team is embedded in the product organization and is responsible for: (1) engaging closely with legal, policy, and other members of the Privacy XFN Team to drive privacy decisions; (2) coordinating and presenting privacy issues to the Privacy XFN Team; and (3) maintaining records of privacy decisions and reviews.

A central aspect of Facebook's Privacy Program is a continuous assessment of privacy risks. As part of this risk assessment process, members of the Privacy Governance Team work with relevant Facebook stakeholders, including representatives of Facebook's Privacy, Engineering, Security, Internal Audit, Marketing, Legal, Public Policy, Communications, Finance, Platform Operations, and User Operations teams, to identify reasonably foreseeable, material risks, both internal and external, that could result in the unauthorized collection, use or disclosure of covered information. This process is enriched by input from the Chief Privacy Officer, Policy and her team, which engage with industry stakeholders and regulators and integrate external feedback into Facebook's program.

The team considers risks in each relevant area of operation, including governance, product design, and engineering (including product development and research), user operations (including third-party developers), advertising, service providers, employee awareness and training, employee management, and security for privacy. The team also considers the sufficiency of the safeguards in place to control the identified risks. Through this process, Facebook has documented reasonably foreseeable material risks to user privacy and has put in place reasonable privacy processes and controls to address those risks.

As part of Facebook's on-going privacy risk assessment process, Facebook holds an annual "Privacy Summit" of relevant stakeholders, including key representatives from the Privacy XFN Team. The Privacy XFN Team includes representatives from each major segment of Facebook, including Facebook's Privacy, Public Policy, Legal, Marketing, Product, Engineering, Security, and Communications teams. Attendees of the annual Privacy Summit review and update the privacy risk assessment, focusing on significant material risks identified by the Privacy Governance Team. Attendees evaluate those privacy risks in light of changing internal and external threats, changes in operations, and changes in laws and regulations. Attendees also examine the sufficiency of existing privacy controls in mitigating those risks, as well as new potential risks. Finally, attendees engage in discussion around ways to improve the work performed by the Privacy XFN Team. The last Privacy Summit occurred on (b)(4), (b)(3):6

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 8 of 79 **HIGHLY CONFIDENTIAL**



As indicated above, Facebook's Privacy Governance Team, led by the Chief Privacy Officer, Product is responsible for the design, implementation, and maintenance of the Privacy Program, which is documented in written policies and procedures. Highlights of the program are detailed below.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 9 of 79 **HIGHLY CONFIDENTIAL**



Privacy and Security Awareness Activities

Facebook communicates Privacy and Security awareness matters to new and existing employees and tailors such communications according to role and responsibility. For example, as part of its regular training for new project managers, Facebook trains project managers about the privacy program and key privacy considerations during the product development cycle. This training involves representatives from the Privacy XFN Team presenting to the project managers (the Privacy XFN process covers those directly involved in the development and management of new products, enhancements to existing products and services for consumers, as described below under "Product Design, Development and Research Activities). As a further example, engineers at Facebook spend their first six weeks in bootcamp, an immersive, cross-functional orientation program. During bootcamp, engineers are instructed on the importance of privacy and security at Facebook, along with their obligations to protect user information as it relates to their roles and responsibilities. Similar group-specific trainings are held for other constituents in the Company (e.g., user operations).

Facebook also holds "Hacktober" annually in October. Hacktober is a month-long event intended to increase employee privacy and security awareness. A series of simulated security threats (e.g., phishing scams) are presented to employees to determine how the employees would respond. If employees report the security threat, they receive a reward, such as Facebook-branded merchandise. If the security threat goes unreported, or if vulnerability is exploited, the employees undergo further education and awareness.

To further promote recognition and understanding of privacy issues and obligations among all Facebook employees, Facebook recently deployed, in addition to initiatives described above, a computer-based privacy training program to all employees. This training provides an overview of applicable privacy laws and Facebook's privacy commitments. All new employees are now required to complete the privacy training within 30 days of employment, while all existing employees are required to complete the privacy training annually. Facebook employees are quizzed on their understanding of Facebook's privacy practices during the training.

Product Design, Development, and Research Activities

The Privacy XFN Team considers privacy from the earliest stages in the product development process (i.e., "privacy by design"). The Chief Privacy Officer, Product and his team spearhead this review and lead a number of key functions and responsibilities. First, as described above, employees, including engineers, product managers, content strategists, and product marketing managers, are educated on Facebook's privacy framework. This education includes an overview of Facebook's processes and corresponding legal obligations, and may involve other members of the Privacy XFN team, such as Privacy and Product Counsel.

Second, the Chief Privacy Officer, Product and his team host weekly reviews of key product-related decisions and material changes to Facebook's privacy framework, which are attended by members of the Privacy XFN Team. The Chief Privacy Officer, Product and his team also review all new product proposals and any material changes to existing products from a privacy perspective and involve the Privacy XFN Team for broader review and feedback. The impact of privacy principles such as notice, choice, consent, access, security,

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 10 of 79

HIGHLY CONFIDENTIAL



retention, deletion, and disclosure are considered as part of this review. Product launches are added to the Privacy Launch Calendar to ensure on-going review and consideration of privacy issues by the Privacy XFN Team throughout the development process. Members of the Privacy XFN Team also communicate back to their respective teams on issues covered in the weekly reviews. This review process helps ensure that privacy is considered throughout the product development process, and maintains consistency on privacy issues across all Facebook products and services.

The following products, available on the platforms and devices indicated, are included in the scope of Facebook's Privacy Program and the Order:

- Facebook: Facebook.com (internet/web), m.facebook.com, iOS, Android, Facebook for Every Phone, Facebook for Blackberry, Facebook for Windows;
- Messenger: iOS, Android;
- Camera: iOS;
- Pages Manager: iOS, Android;
- Poke: iOS; and
- Instagram: Instagram.com (internet/web), iOS, Android.

Facebook Platform

Platform applications and developers are required to comply with, and are subject to, Facebook's Statement of Rights and Responsibilities, Platform Principles, and Platform Policies. These terms and policies outline a variety of privacy obligations and restrictions, such as limits on an application's use of data received through Facebook, requirements that an application obtain consent for certain data uses, and restrictions on sharing user data. Facebook's Platform privacy setting and Granular Data Permissions ("GDP") process allows users to authorize the transfer of Facebook user information to third-party applications. Monitoring controls are in place to detect material misuse of the Platform (e.g., user complaints, third-party applications that do not have active privacy policy links).

Security for Privacy

Facebook has implemented technical, physical, and administrative security controls designed to protect user data from unauthorized access, as well as to prevent, detect, and respond to security threats and vulnerabilities. Facebook's security program is led by the Chief Security Officer ("CSO") and supported by a dedicated Security Team. As mentioned above, the CSO is a key and active member of the Privacy Governance team. Facebook's security and privacy employees work closely on an on-going basis to protect user data and Facebook's systems.

Monitoring Activities

In order to ensure that the effectiveness of its controls and procedures are regularly monitored, Facebook has designated an "owner" for each of the controls included in the Privacy Program. Facebook utilizes the annual Privacy Summit to monitor the effectiveness of controls and procedures in light of changing internal and external risks. In addition, members of Facebook's Legal team periodically review the Privacy Program to ensure it, including the controls and procedures contained therein, remains effective. These Legal team members also will serve as point of contacts for control owners and will update the Privacy Program to reflect any changes or updates surfaced.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 11 of 79 **HIGHLY CONFIDENTIAL**



Service Providers

Facebook has implemented controls with respect to third-party service providers, including implementing policies to select and retain service providers capable of appropriately protecting the privacy of covered information received from Facebook.

Facebook's Security team has a process for conducting due diligence on service providers who may receive covered information in order to evaluate whether their data security standards are aligned with Facebook's commitments to protect covered information. As part of the due diligence process, Facebook asks prospective service providers to complete a security architecture questionnaire or vendor security questionnaire to assess whether the provider meets Facebook's functional security requirements to protect the privacy of user data. Based upon the service provider's responses to the vendor security questionnaire and other data points, Facebook's Security team determines whether further security auditing is required. Facebook partners with an outside security consulting firm to conduct security audits, which may include testing of the service provider's controls, a vulnerability scanning program, a web application penetration test, and/or a code review for security defects. The security consulting firm reports its findings to Facebook, and Facebook requires that the prospective service provider fix critical issues before being on-boarded. Depending on the sensitivity of Facebook data shared with the service provider and other factors, Facebook may require that the service provider undergo a periodic or random security and/or privacy audit.

Facebook also has a contract policy (the "Contract Policy"), which governs the review, approval, and execution of contracts for Facebook. Facebook's pre-approved contract templates require service providers to implement and maintain appropriate protections for covered information. Facebook reviews contracts that deviate from the pre-approved templates to help ensure that contracts with applicable service providers contain the required privacy protections. Facebook Legal documents review of any such contracts through formal approval prior to contract execution.

Monitoring

Facebook's Privacy Program is designed with procedures for evaluating and adjusting the Privacy Program in light of the results of testing and monitoring of the program as well as other relevant circumstances. As mentioned above, Facebook's annual Privacy Summit is designed to identify, discuss, and assess compliance with privacy policies and procedures, and applicable laws and regulations, as well as identify new or changed risks and recommend responsive controls. The Privacy XFN Team assesses risks and controls on an on-going basis through weekly meetings and review processes. Members of Facebook's Legal team support the Privacy Program and serve as points of contact for all relevant control owners to communicate recommended adjustments to the Privacy Program based on regular monitoring of the controls for which they are responsible, as well as any internal or external changes that affect those controls. Additionally, the Privacy Governance Team regularly discusses the Privacy Program in the context of various product and operational discussions. During these discussions, the effectiveness and efficiency of the Privacy Program are considered and reviewed and, when appropriate, adjustments are made to maintain a strong program.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 12 of 79 **HIGHLY CONFIDENTIAL**



Facebook also continuously evaluates acquisitions for inclusion in the Privacy Program, based on the nature of the acquisition (e.g., talent or people, intellectual property, product or infrastructure). Specifically, Facebook takes steps, as appropriate, to integrate acquisitions into the Privacy Program and reviews products and features developed by acquisitions with the same level of rigor applied to Facebook's products and services. The acquisitions in the current Reporting Period were primarily talent acquisitions, except for Instagram. Instagram's people, product, and supporting infrastructure were acquired on August 31, 2012.

Facebook assessed the privacy risks associated with Instagram's people, process, and technology upon acquisition. In comparison to Facebook, Instagram has significantly fewer users, employees, and products. As described in the Company Overview above, Instagram's products focus on photo taking, filtering, and sharing. From a privacy perspective, Instagram users have one binary choice - to make all photos private or all photos public by setting the "Photos are Private" on/off slider. Once private, the user approves any "follower" requests. After obtaining approval, the follower can access posted photos and related comments. The Privacy XFN Team also was involved in reviewing Instagram's January 19, 2013 privacy policy update.



PwC's Privacy Assessment Approach

PwC's Assessment Standards

Part V of the Order requires that the Assessments be performed by a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. This report was issued by PwC under professional standards which meet these requirements.

As a public accounting firm, PwC must comply with the public accounting profession's technical and ethical standards, which are enforced through various mechanisms created by the American Institute of Certified Public Accountants ("AICPA"). Membership in the AICPA requires adherence to the Institute's Code of Professional Conduct. The AICPA's Code of Professional Conduct and its enforcement are designed to ensure that CPAs who are members of the AICPA accept and achieve a high level of responsibility to the public, clients, and colleagues. (b)(4), (b)(3):6(f)

(b)(4), (b)(3):6(f)

In performing this assessment, PwC complied with all of these Standards.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 14 of 79 **HIGHLY CONFIDENTIAL**



Independence

(b)(4),(b)(3):6(f)

PwC is independent with respect to the Standards required for this engagement.

PwC Assessor Qualifications

PwC assembled an experienced, cross-disciplinary team of PwC team members with privacy, assessment, and technology industry expertise to perform the Assessor role for the Order. (b)(4),(b)(3):6(f)

(b)(4),(b)(3):6(f)

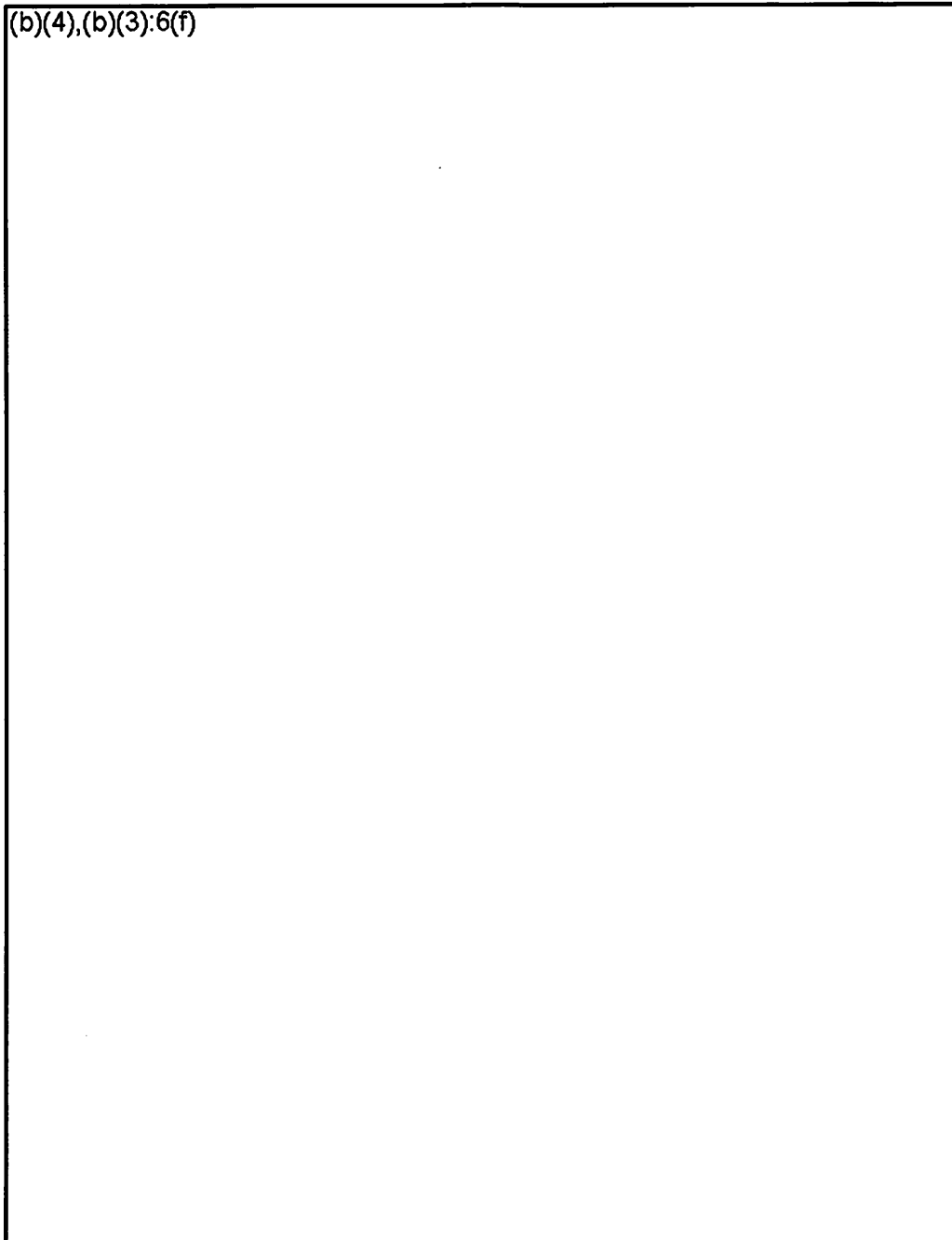
PwC Assessment Process Overview

(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 15 of 79 **HIGHLY CONFIDENTIAL**



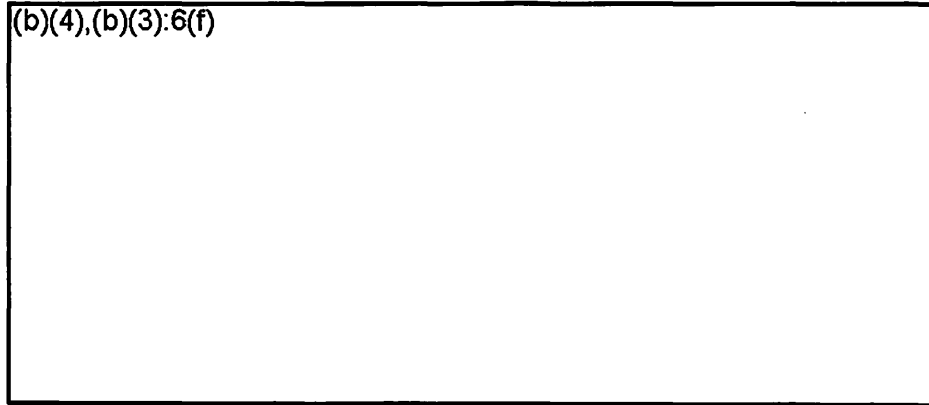
(b)(4),(b)(3):6(f)



Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 18 of 79 **HIGHLY CONFIDENTIAL**



(b)(4),(b)(3):6(f)



Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 17 of 79 **HIGHLY CONFIDENTIAL**



PwC's Assessment of Part IV A, B, C, D and E, of the Order

The tables in section "Facebook's Privacy Program: Assertions, Control Activities and PwC's Tests Performed and Results" of this report describe the scope of Facebook's Privacy Program referenced in the Management Assertion on pages 77-78. Facebook established its privacy program by implementing privacy controls to meet or exceed the protections required by Part IV of the Order. The table also includes PwC's inquiry, observation, and inspection/examination test procedures to assess the effectiveness of Facebook's program and test results. PwC's final conclusions are detailed on pages 4-5 of this document.

A. Set forth the specific privacy controls that respondent has implemented and maintained during the reporting period.

As depicted within the table on pages 21-76, Facebook has listed the privacy controls that were implemented and maintained during the reporting period.

B. Explain how such privacy controls are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered information.

Based on the size and complexity of the organization, the nature and scope of Facebook's activities, and the sensitivity of the covered information (as defined in by the order), Facebook management developed the company-specific criteria (assertions) detailed on pages 77-78 as the basis for its Privacy Program. The management assertions and the related control activities are intended to be implemented to address the risks identified by Facebook's privacy risk assessment.

C. Explain how the privacy controls that have been implemented meet or exceed the protections required by Part IV of the Order.

As summarized in the Facebook's Privacy Program on pages 6-13, Facebook has implemented the following protections:

A. Designation of an employee or employees to coordinate and be responsible for the privacy program.

As described above, Facebook has designated a team of employees to coordinate and be responsible for the Privacy Program as required by Part IV of the Order. As described on pages 21-23 (Management's Assertion A), PwC performed test procedures to assess the effectiveness of the Facebook privacy controls implemented to meet or exceed the protections required by Part IV of the Order.

B. The identification of reasonably foreseeable, material risks, both internal and external, that could result in Respondent's unauthorized collection, use, or disclosure of covered information and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk assessment should include consideration of risks in each area of relevant operation.



including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research.

As described above, Facebook has identified reasonably foreseeable, material risks, both internal and external, that could result in Facebook's unauthorized collection, use, or disclosure of covered information, and assessed the sufficiency of any safeguards in place to control these risks as required by Part IV of the Order. As described on page 24 (Management's Assertion B), PwC performed test procedures to assess the effectiveness of the Facebook privacy controls implemented to meet or exceed the protections required by Part IV of the Order.

C. 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.

As described above, Facebook has designed and implemented 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 as required by Part IV of the Order. As described on pages 25-65 (Management's Assertions C, D, E, F, and G), PwC performed test procedures to assess the effectiveness of the Facebook privacy controls implemented to meet or exceed the protections required by Part IV of the Order.

D. 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 Respondent and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information.

As described above, Facebook has developed and implemented reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from Facebook as required by Part IV of the Order. Facebook also includes terms in contracts with service providers requiring that such service providers implement and maintain appropriate privacy protections. As described on pages 66-70 (Management's Assertion H), PwC performed test procedures to assess the effectiveness of the Facebook privacy controls implemented to meet or exceed the protections required by Part IV of the Order.

E. The evaluation and adjustment of Respondent's privacy program in light of the results of the testing and monitoring required by subpart C, any material changes to Respondent's operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have a material impact on the effectiveness of its privacy program.

As described above, Facebook has evaluated and adjusted its Privacy Program in light of the results of the testing and monitoring required by subpart C within Part IV of the Order, any material changes to Facebook's operations or business arrangements, or any other circumstances that Facebook knows or has reason to



know may have a material impact on the effectiveness of its privacy program as required by Part IV of the Order. As described on pages 71-76 (Management's Assertion D), PwC performed test procedures to assess the effectiveness of the Facebook privacy controls implemented to meet or exceed the protections required by Paragraph IV of the Order.

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.

As described in the PwC Assessment Process Overview section above, PwC performed its assessment of Facebook's Privacy Program in accordance with AICPA Attestation Standards. Refer to pages 4-5 of this document for PwC's conclusions.

(b)(4),(b)(3):6(f)

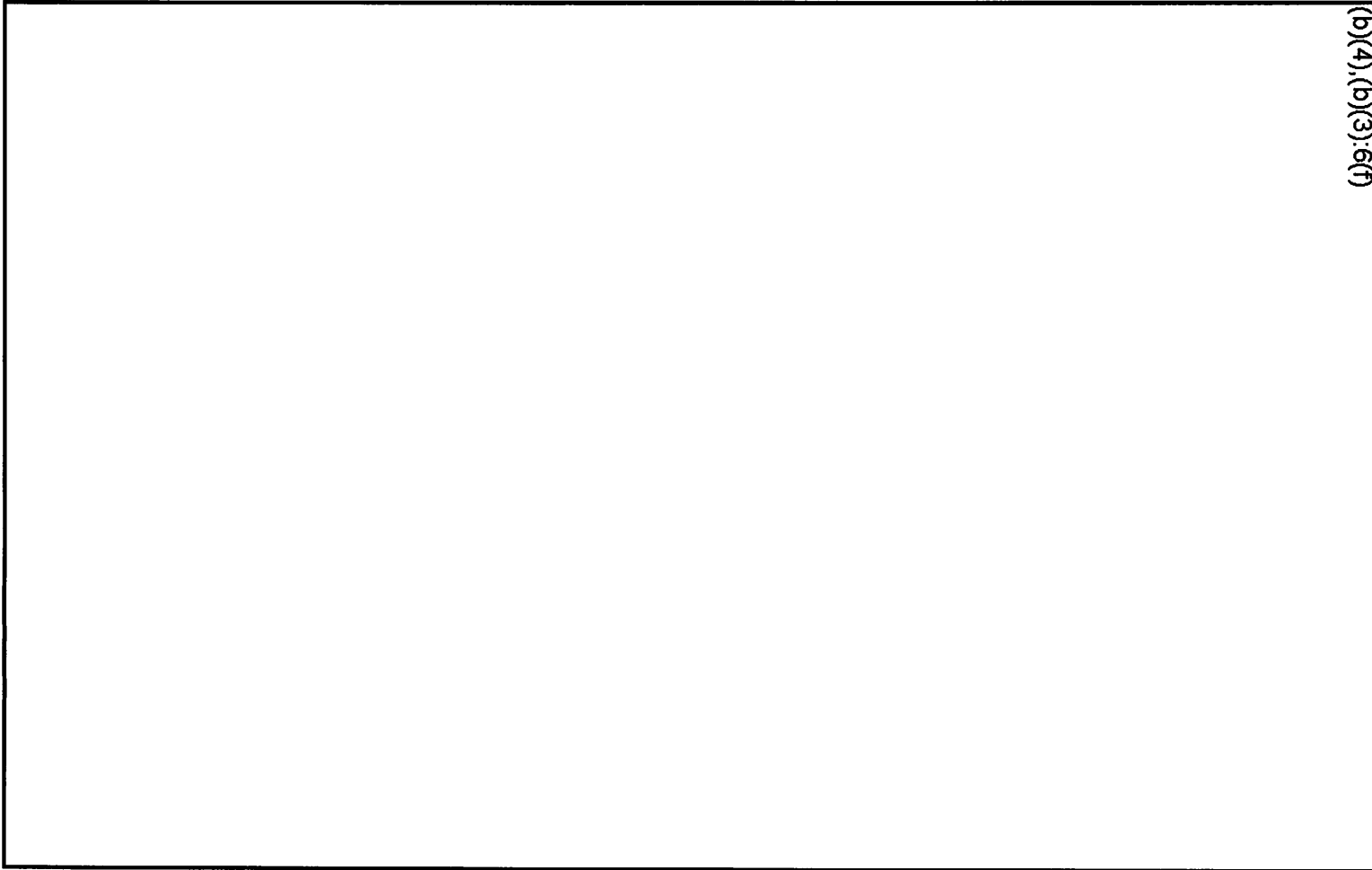

DM/C

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
HIGHLY CONFIDENTIAL

epic.org



EPIC-13-04-26-FTC-FOIA-20130612-Production-2



(b)(4), (b)(3), (b)(7)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 22 of 79
HIGHLY CONFIDENTIAL

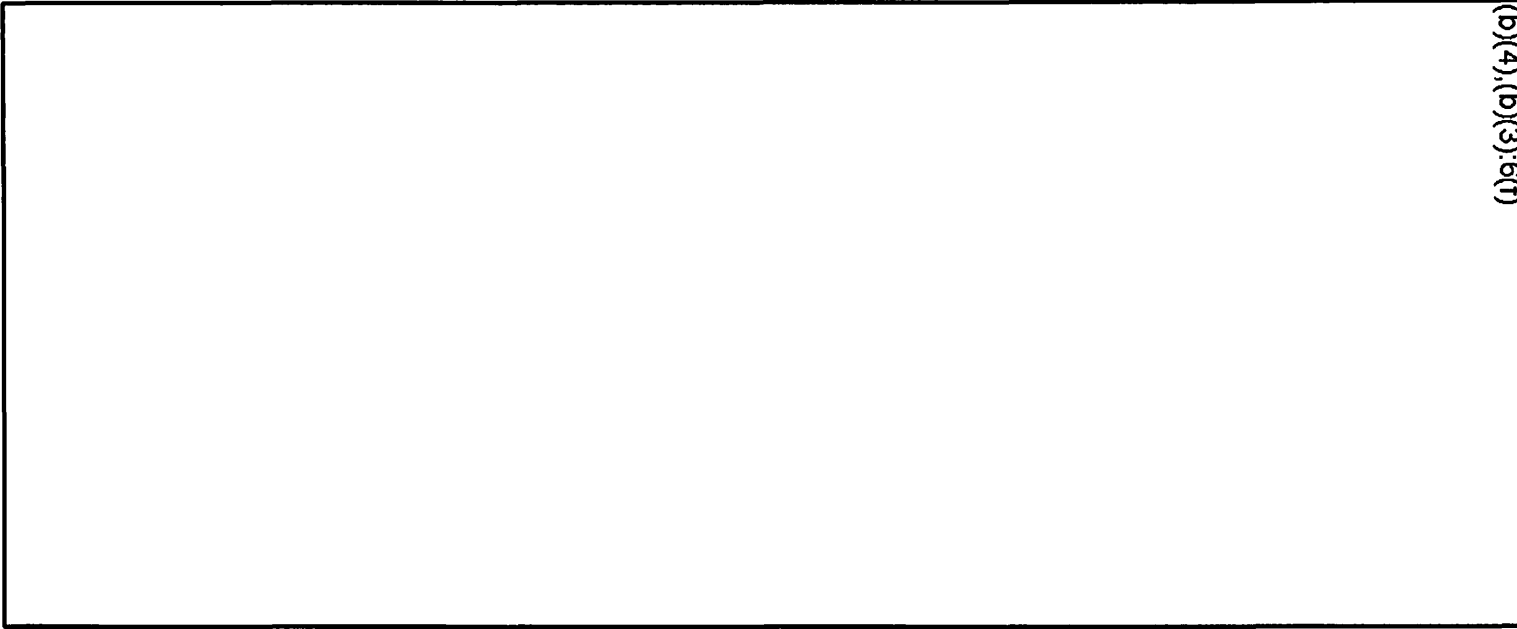
000026



(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
HIGHLY CONFIDENTIAL

epic.org



(b)(4), (b)(3), (b)(1)

EPIC-13-04-26-FTC-FOIA-20130612-Production-2

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 24 of 79 **HIGHLY CONFIDENTIAL**

000028



(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
HIGHLY CONFIDENTIAL



(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 26 of 79
HIGHLY CONFIDENTIAL

epic.org



EPIC-13-04-Z6-FTC-FA-20130612-PRODUCTION-Z

(b)(4), (b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 27 of 79

HIGHLY CONFIDENTIAL

000031



(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
HIGHLY CONFIDENTIAL

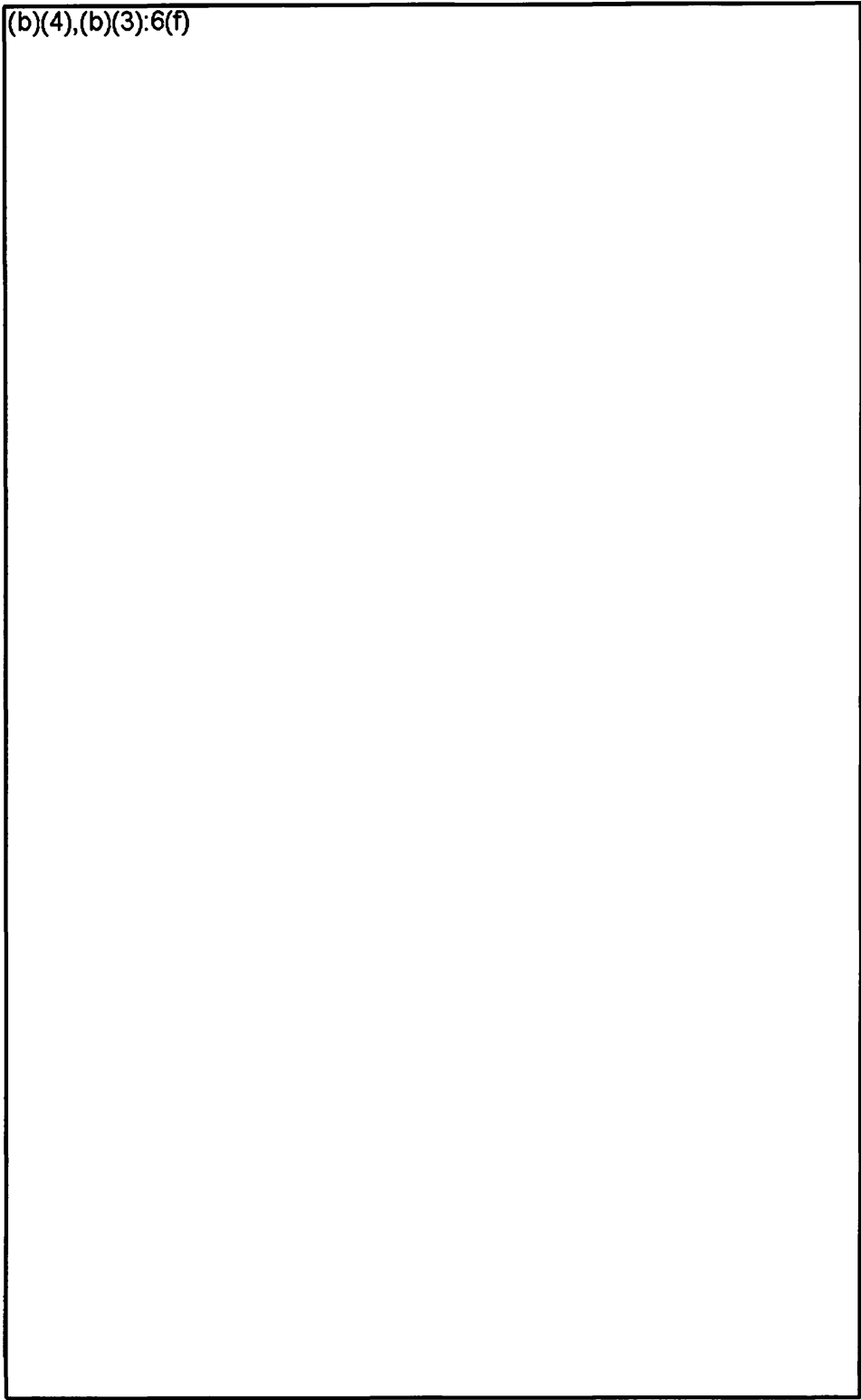


(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
HIGHLY CONFIDENTIAL

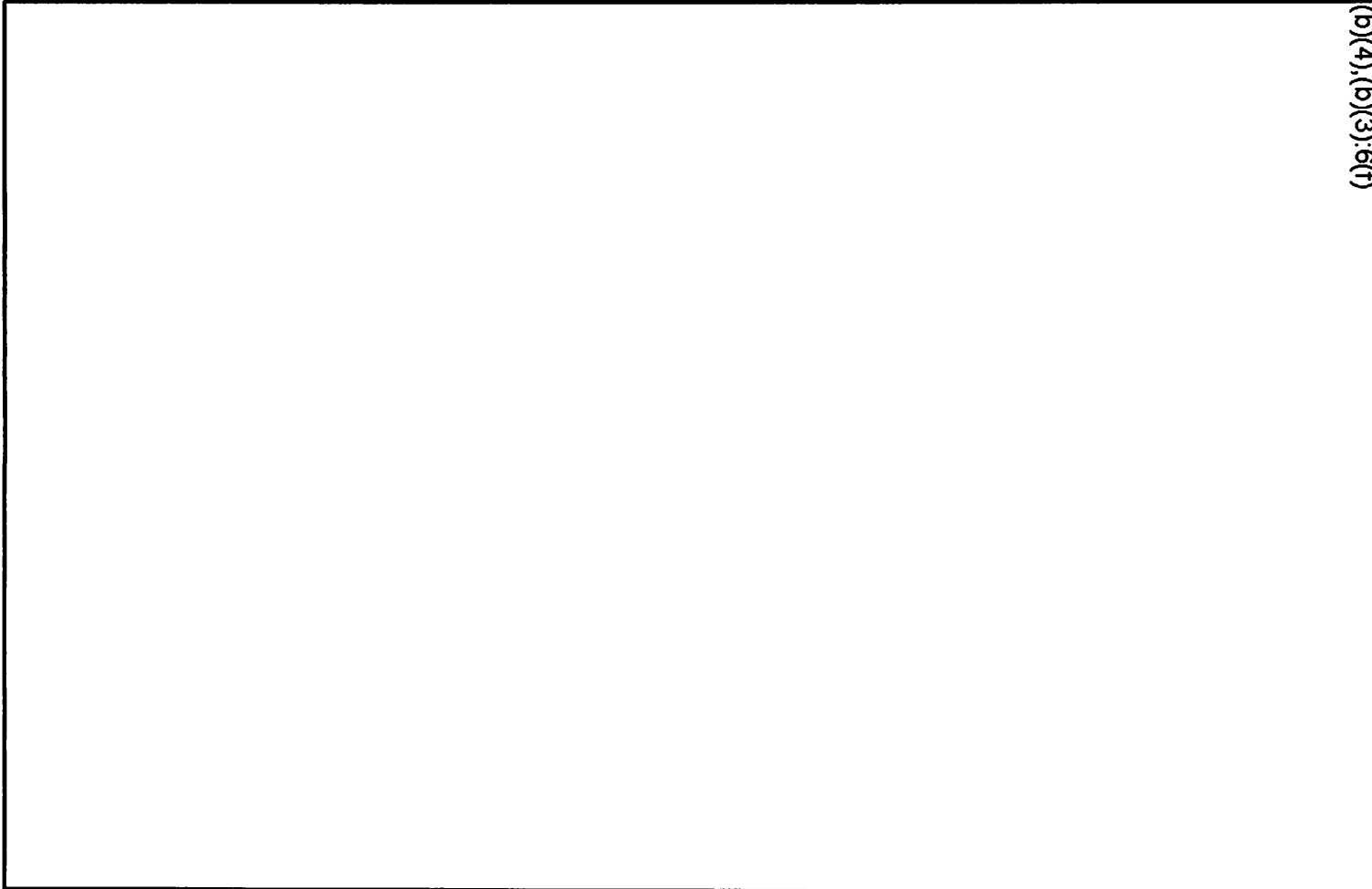


(b)(4),(b)(3):6(f)



Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
HIGHLY CONFIDENTIAL

epic.org



(b)(4), (b)(3), 6(f)

EPIC-13-04-26-FTC-FOIA-20130612-Production-2

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 31 of 79 **HIGHLY CONFIDENTIAL**

000035



(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 32 of 79
HIGHLY CONFIDENTIAL

The logo for DWIC (Data Working Interest Center) features a stylized bar chart with three bars of increasing height, positioned above the letters "DWIC" in a bold, sans-serif font.

(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 33 of 79
HIGHLY CONFIDENTIAL



(b)(4),(b)(3):6(f)

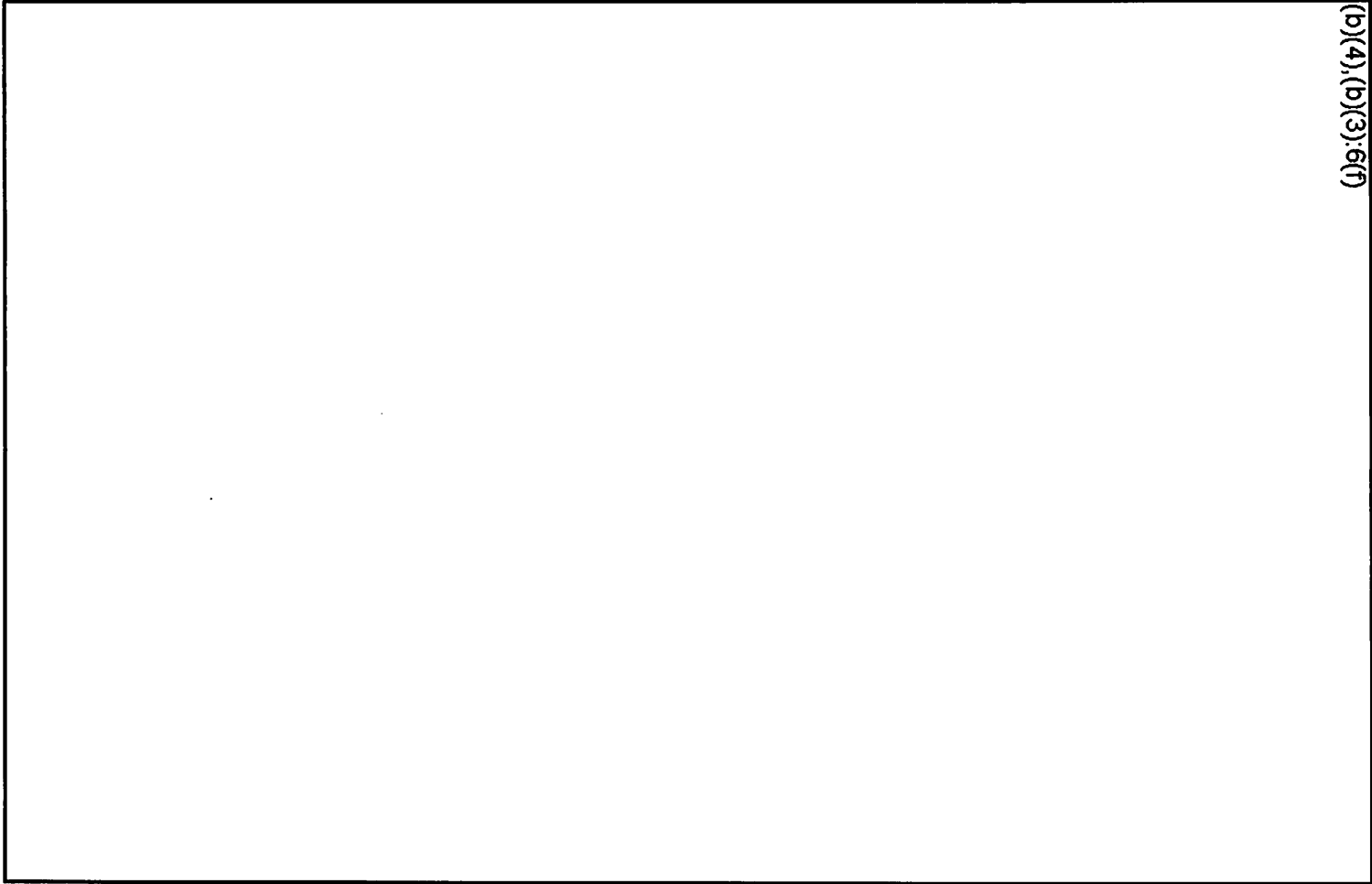
Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 34 of 78
HIGHLY CONFIDENTIAL



(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
HIGHLY CONFIDENTIAL

epic.org



(b)(4), (b)(3), 6(f)

EPIC-13-04-26-FTC-FOIA-20130612-Production-2

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 36 of 79
HIGHLY CONFIDENTIAL

000040

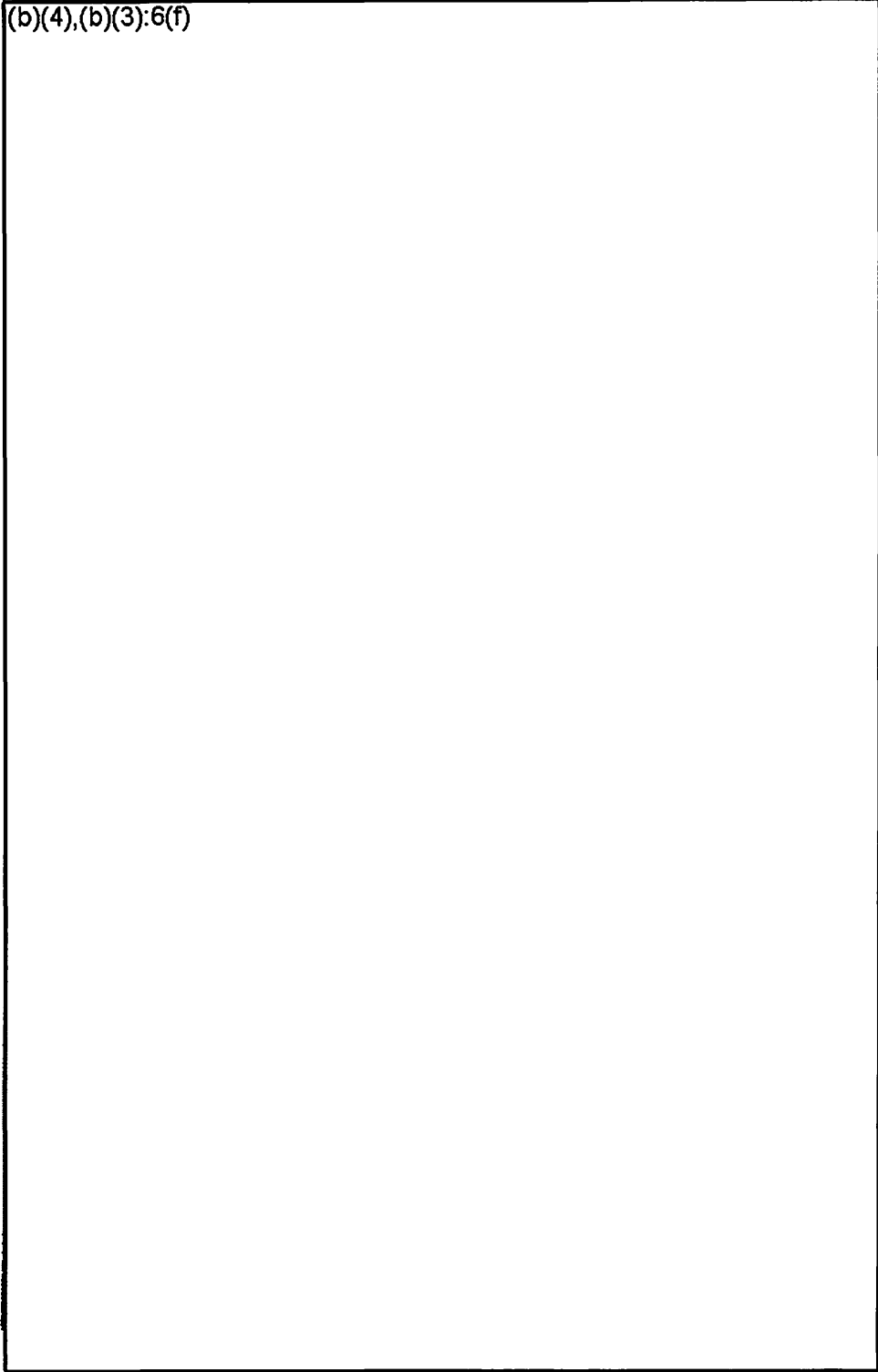


(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
HIGHLY CONFIDENTIAL



(b)(4),(b)(3):6(f)



Use or disclosure of data contained on this page is subject to the restriction on the title page of this report
HIGHLY CONFIDENTIAL

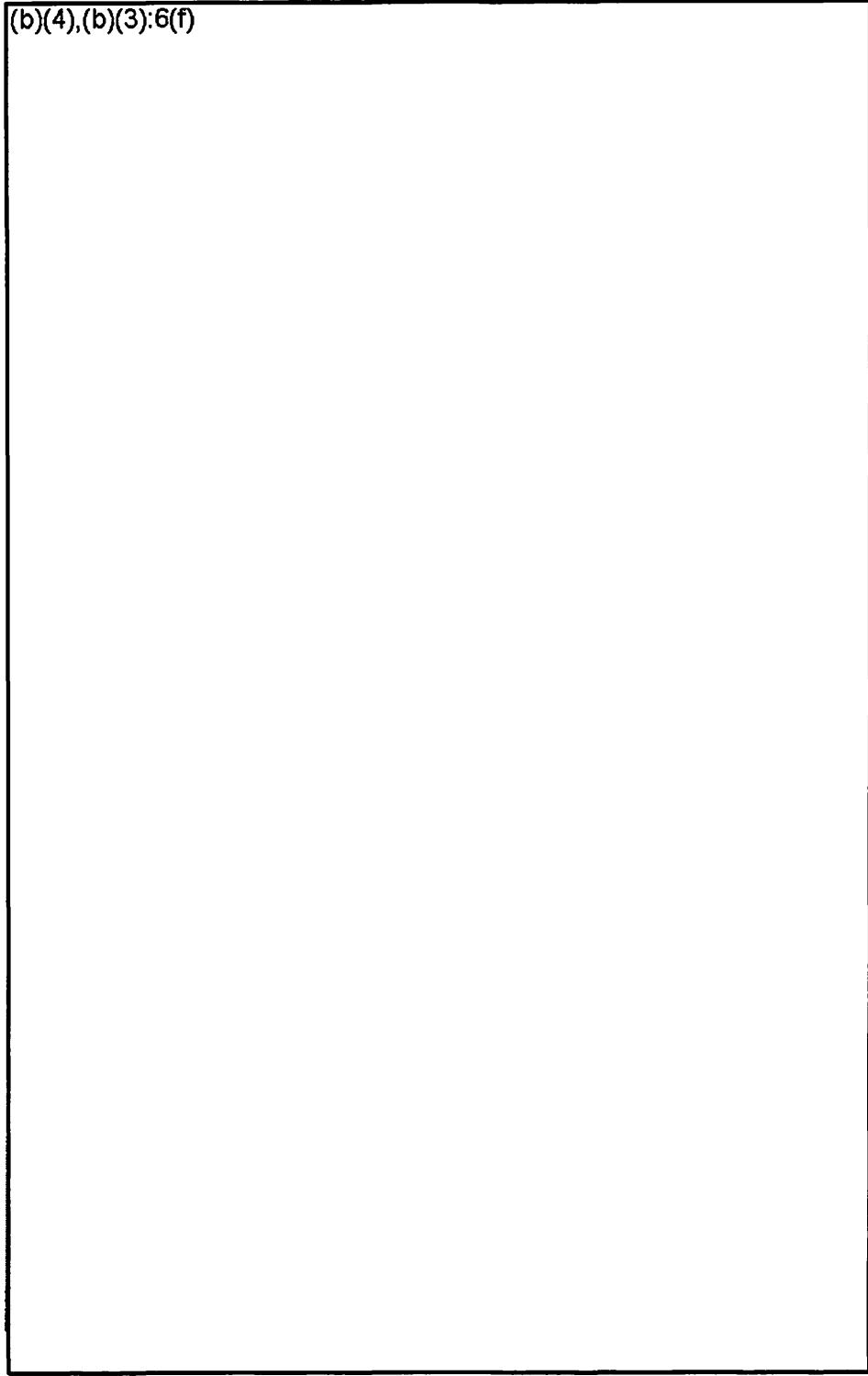


(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 30 of 79
HIGHLY CONFIDENTIAL



(b)(4),(b)(3):6(f)



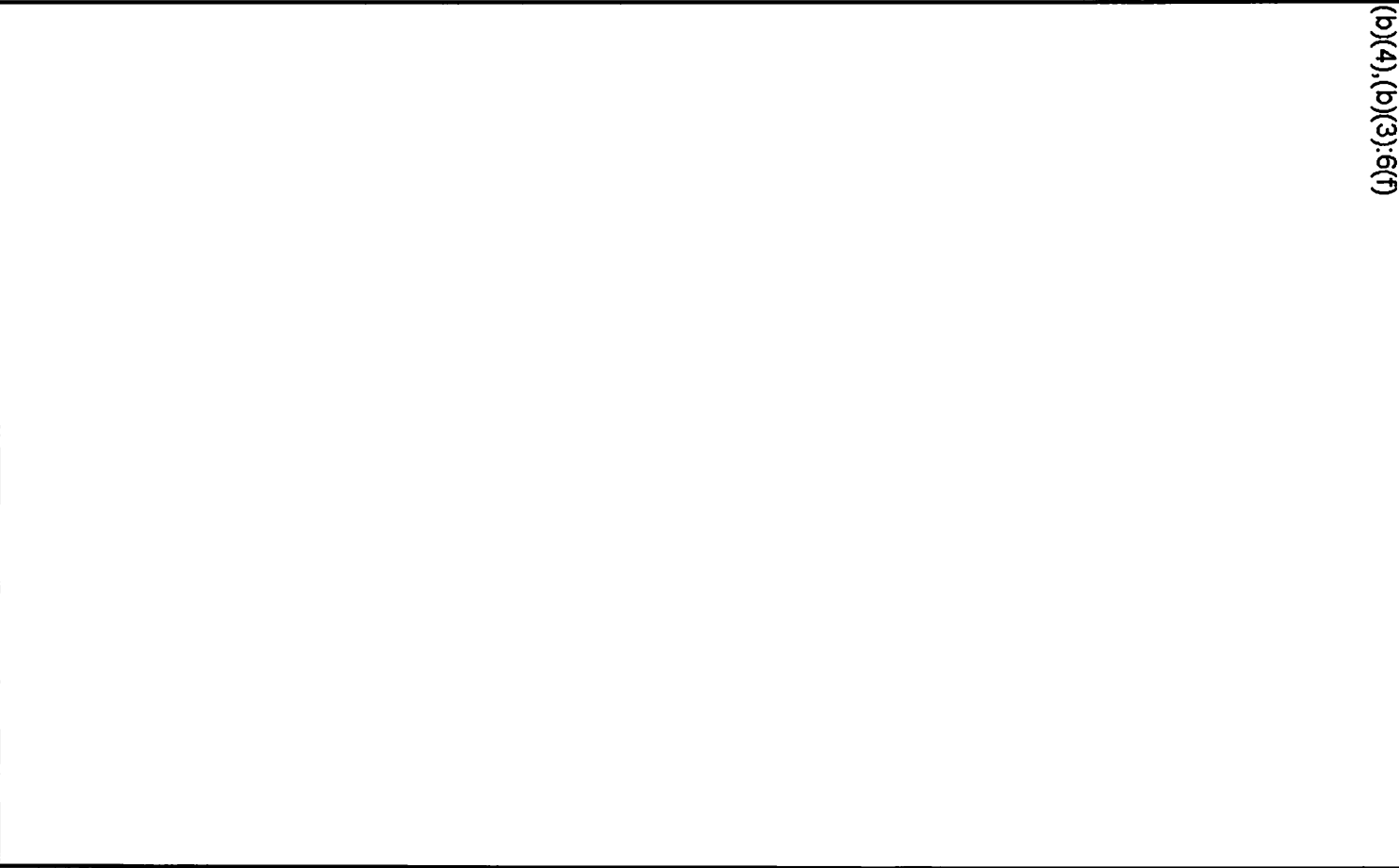
Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
HIGHLY CONFIDENTIAL



(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
HIGHLY CONFIDENTIAL

epic.org



(b)(4), (b)(3), (b)(7)

EPIC-13-04-26-FTC-FOIA-20130612-Production-2

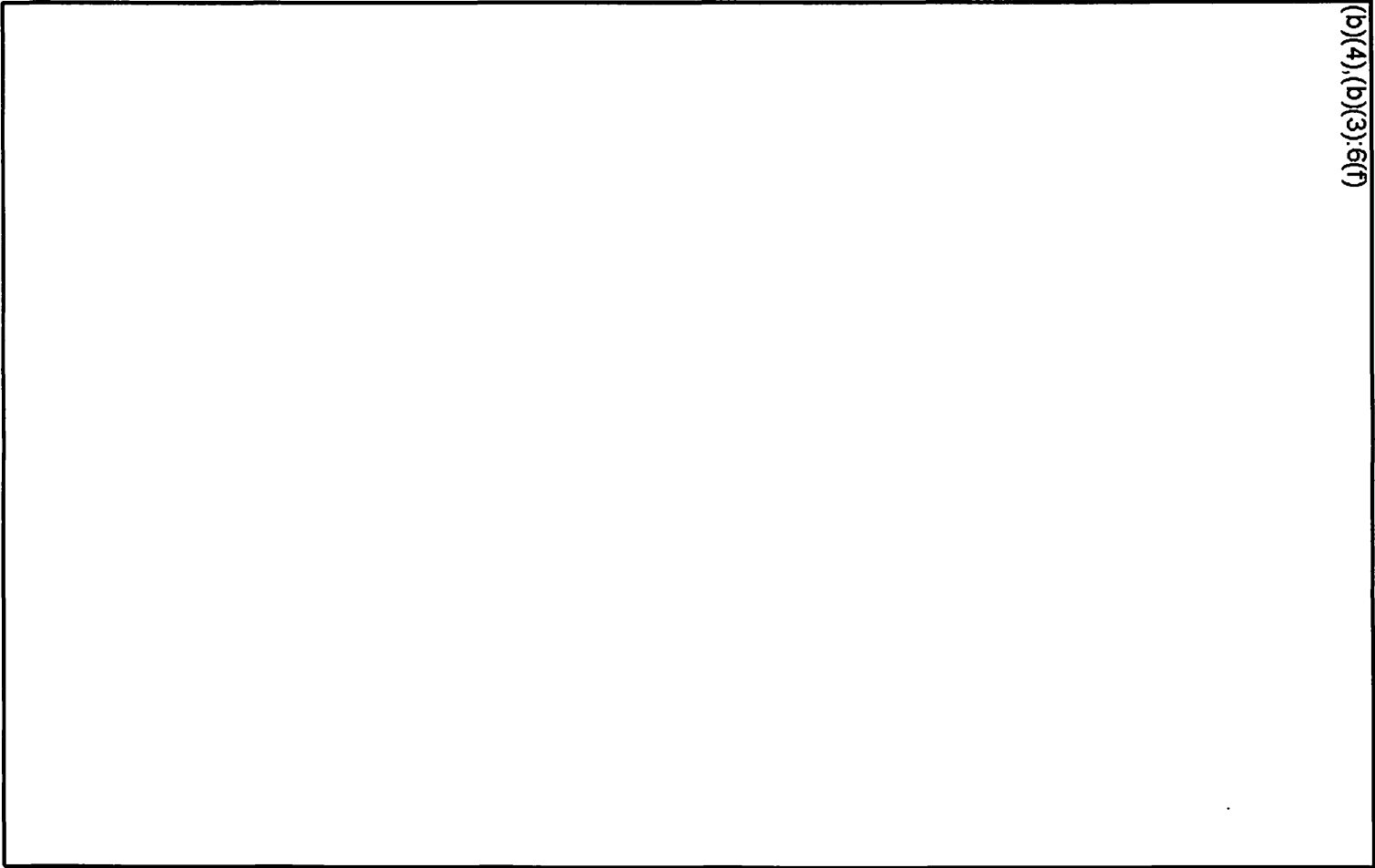
Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 42 of 79
HIGHLY CONFIDENTIAL

000046

epic.org



EPIC-13-04-26-FTC-FOIA-20130612-Production-2



(b)(4), (b)(3), 6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 43 of 79 **HIGHLY CONFIDENTIAL**

000047

epic.org



(b)(4),(b)(3):6(f)

EPIC-13-04-26-FTC-FOIA-20130612-Production-2

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 44 of 79
HIGHLY CONFIDENTIAL

000048

(b)(4),(b)(3):6(f)



Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 45 of 79
HIGHLY CONFIDENTIAL



(b)(4),(b)(3):6(f)

Use of disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 46 of 79
HIGHLY CONFIDENTIAL

epic.org



(b)(4),(b)(3):6(f)

EPIC-13-04-26-FTC-FOIA-20130612-Production-2

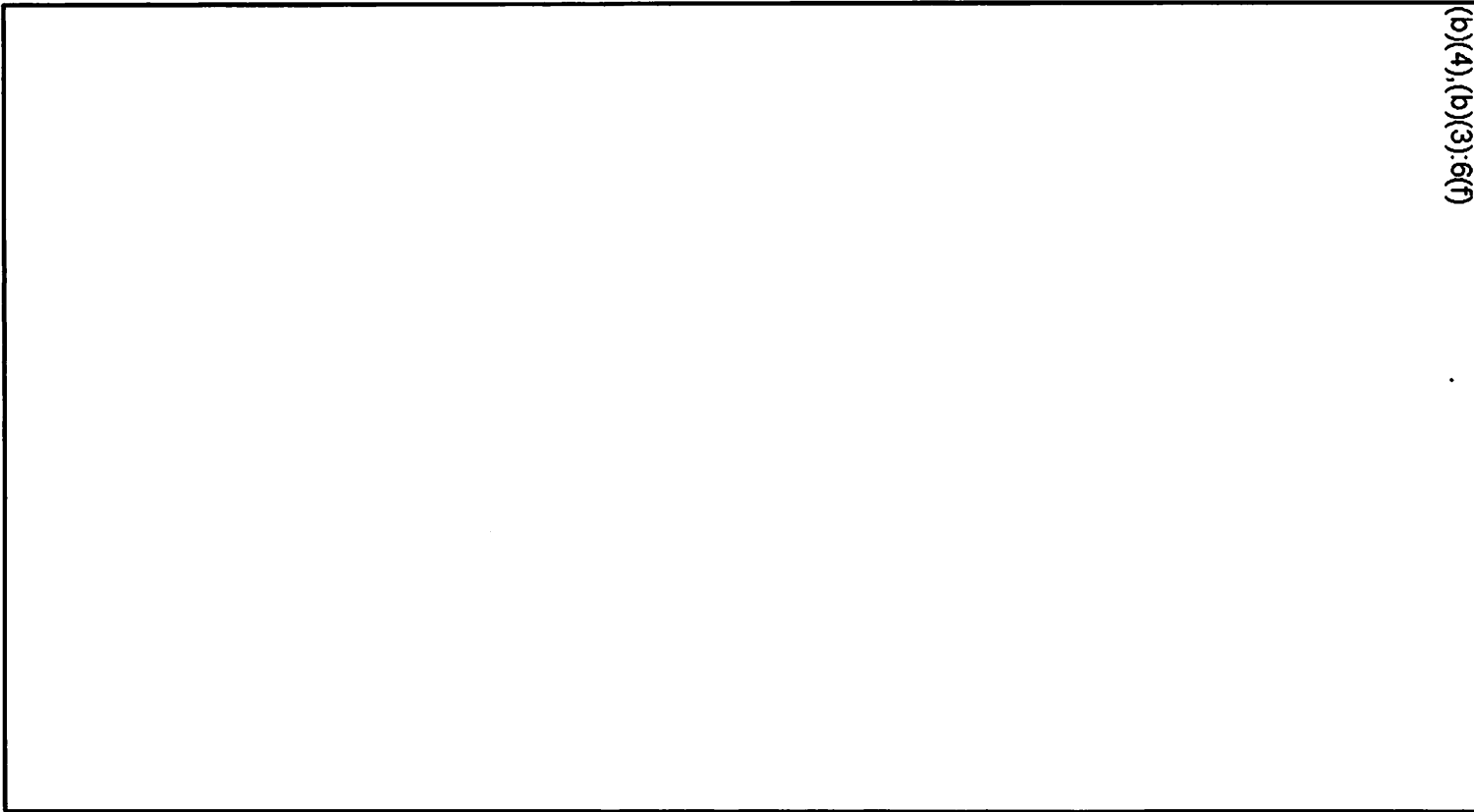
Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 47 of 79 **HIGHLY CONFIDENTIAL**

000051

epic.org



EPI-C-13-04-26-FTC-FOIA-20130612-Production-2



(b)(4),(b)(3),6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 48 of 79
HIGHLY CONFIDENTIAL

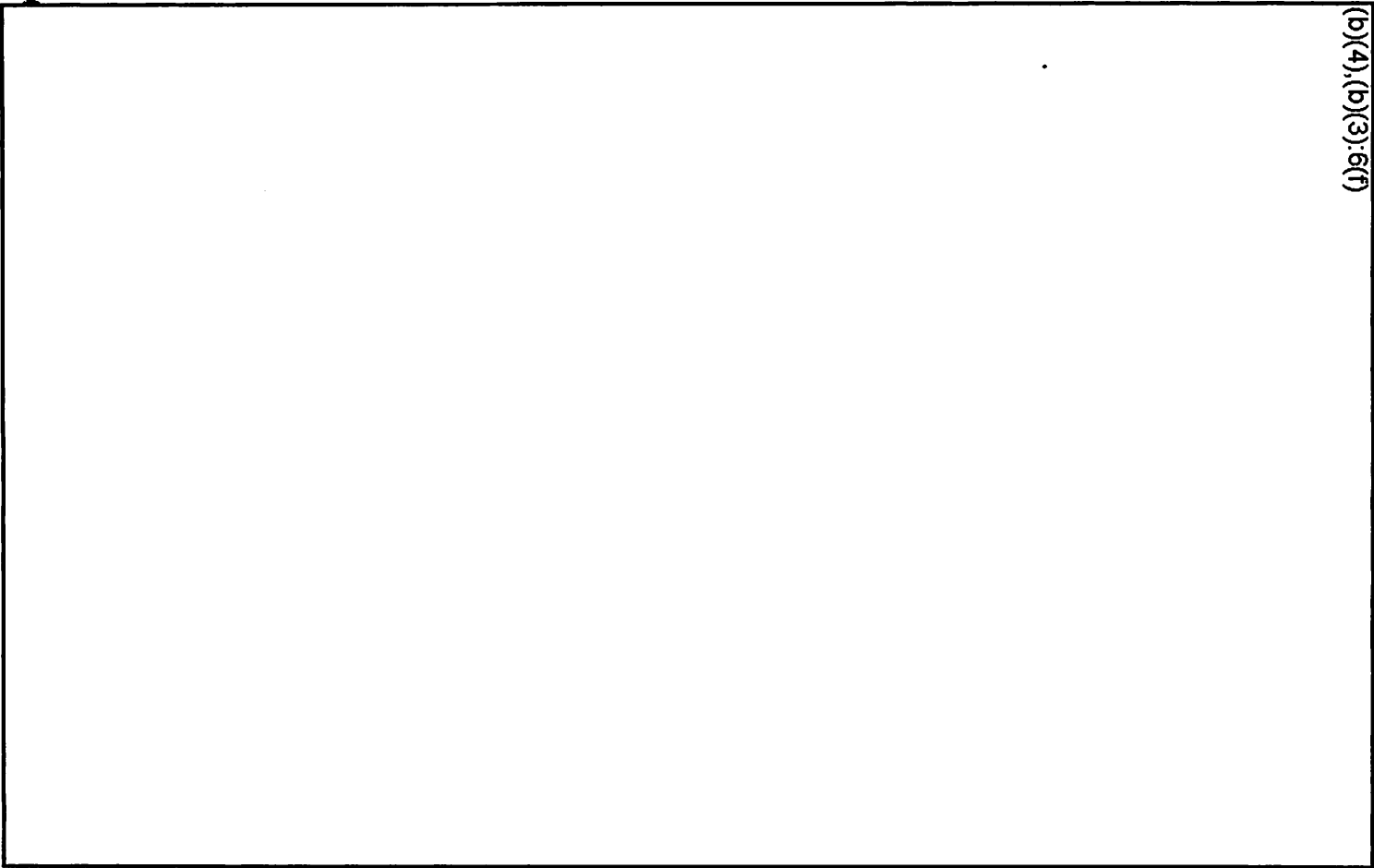
000052

epic.org

EPIC-13-04-26-FTC-FOIA-20130612-Production-2



pwc



(b)(4),(b)(3),(6)(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 49 of 70

HIGHLY CONFIDENTIAL

000053



(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 50 of 79
HIGHLY CONFIDENTIAL



(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
HIGHLY CONFIDENTIAL



(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
HIGHLY CONFIDENTIAL



(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
HIGHLY CONFIDENTIAL



(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 54 of 79
HIGHLY CONFIDENTIAL

(b)(4),(b)(3):6(f)


DWC

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 55 of 78
HIGHLY CONFIDENTIAL



(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 56 of 79
HIGHLY CONFIDENTIAL



(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
HIGHLY CONFIDENTIAL



(b)(4),(b)(3):6(f)

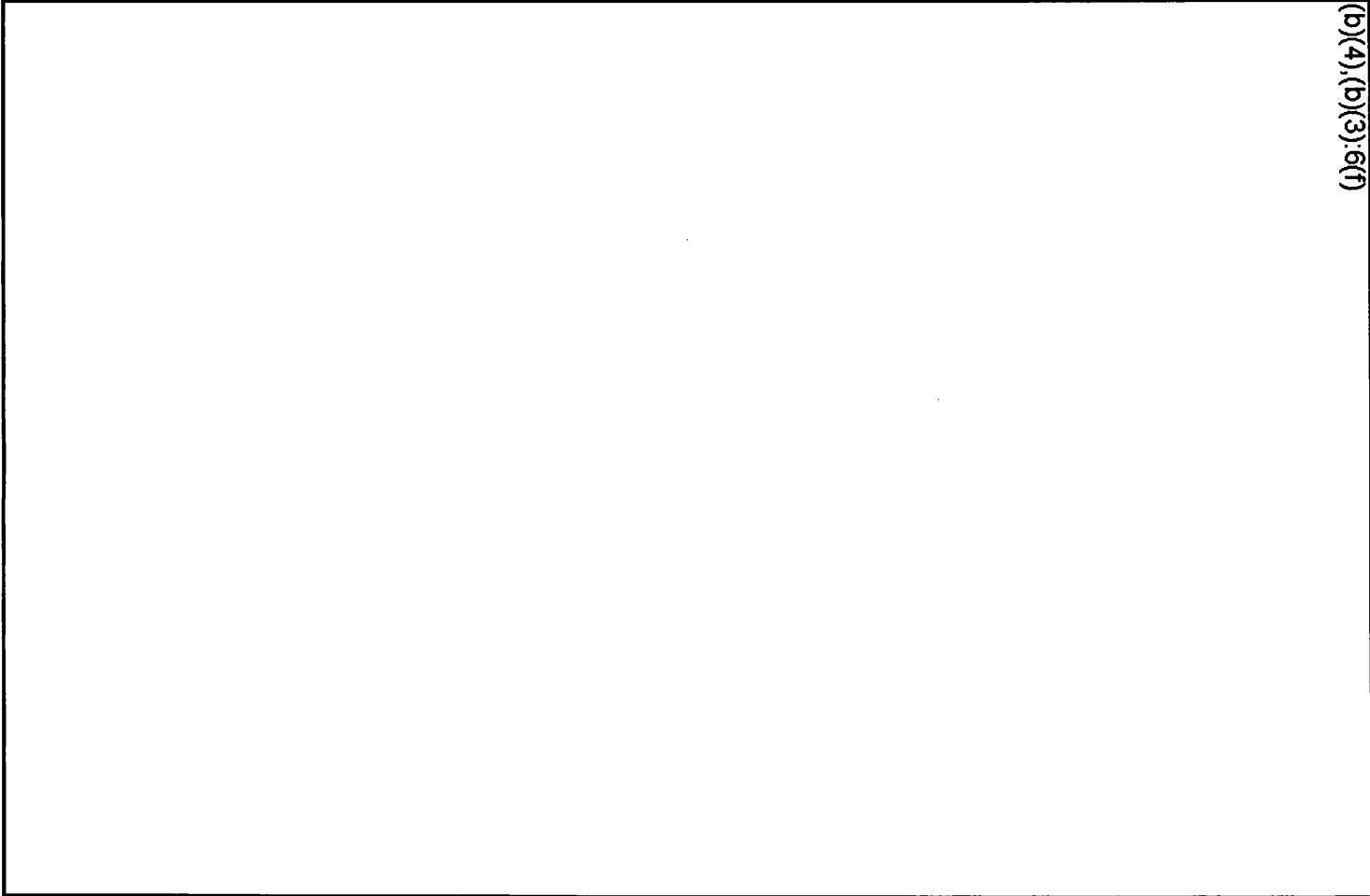
Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
HIGHLY CONFIDENTIAL



(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
HIGHLY CONFIDENTIAL

epic.org



(b)(4), (b)(3), 6(f)

EPIC-13-04-26-FTC-FOIA-20130612-Production-2

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 60 of 70

HIGHLY CONFIDENTIAL

000064



(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 61 of 79
HIGHLY CONFIDENTIAL



(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 62 of 79
HIGHLY CONFIDENTIAL



(b)(4),(b)(3):6(f)

[A large rectangular area of the page is redacted with a black border.]

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 63 of 78
HIGHLY CONFIDENTIAL

epic.org



(b)(4), (b)(3), 6(f)

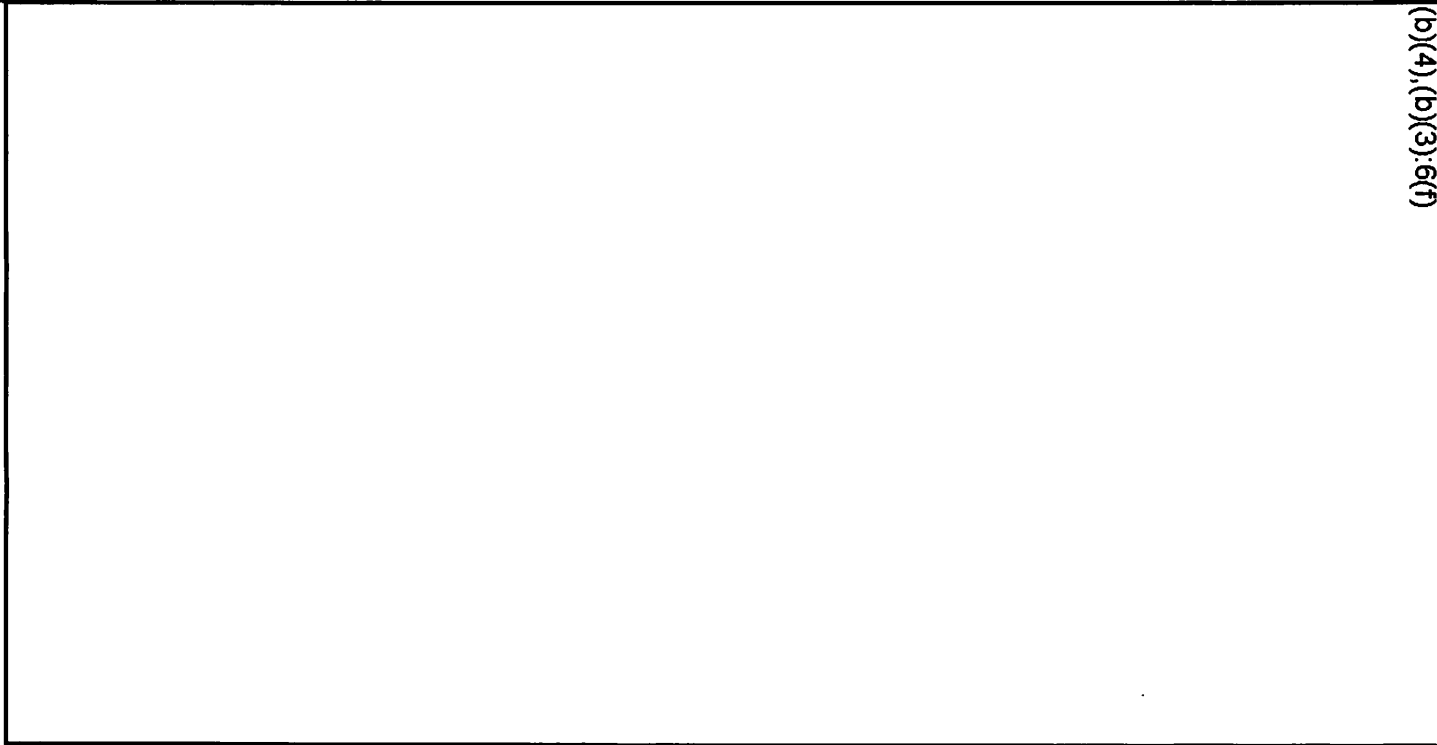
EPIC-13-04-26-FTC-FOIA-20130612-Production-2

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 64 of 79
HIGHLY CONFIDENTIAL

000068

epic.org

EPI-C-13-04-26-FTC-FOIA-20130612-Production-2



(b)(4), (b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 65 of 79

HIGHLY CONFIDENTIAL

000069



(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
HIGHLY CONFIDENTIAL

(b)(4),(b)(3):6(f)



Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 67 of 78
HIGHLY CONFIDENTIAL



(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
HIGHLY CONFIDENTIAL



(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
HIGHLY CONFIDENTIAL



(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 70 of 79
HIGHLY CONFIDENTIAL

(b)(4),(b)(3):6(f)


DM/C

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 71 of 79
HIGHLY CONFIDENTIAL



(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
HIGHLY CONFIDENTIAL



(b)(4),(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
HIGHLY CONFIDENTIAL

epic.org



(b)(4), (b)(3), 6(f)

EPIC-13-04-26-FTC-FOIA-20130612-Production-2

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 74 of 79 **HIGHLY CONFIDENTIAL**

000078

epic.org



(b)(4), (b)(3), 6(f)

EPIC-13-04-26-FTC-FOIA-20130612-Production-2

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 75 of 79

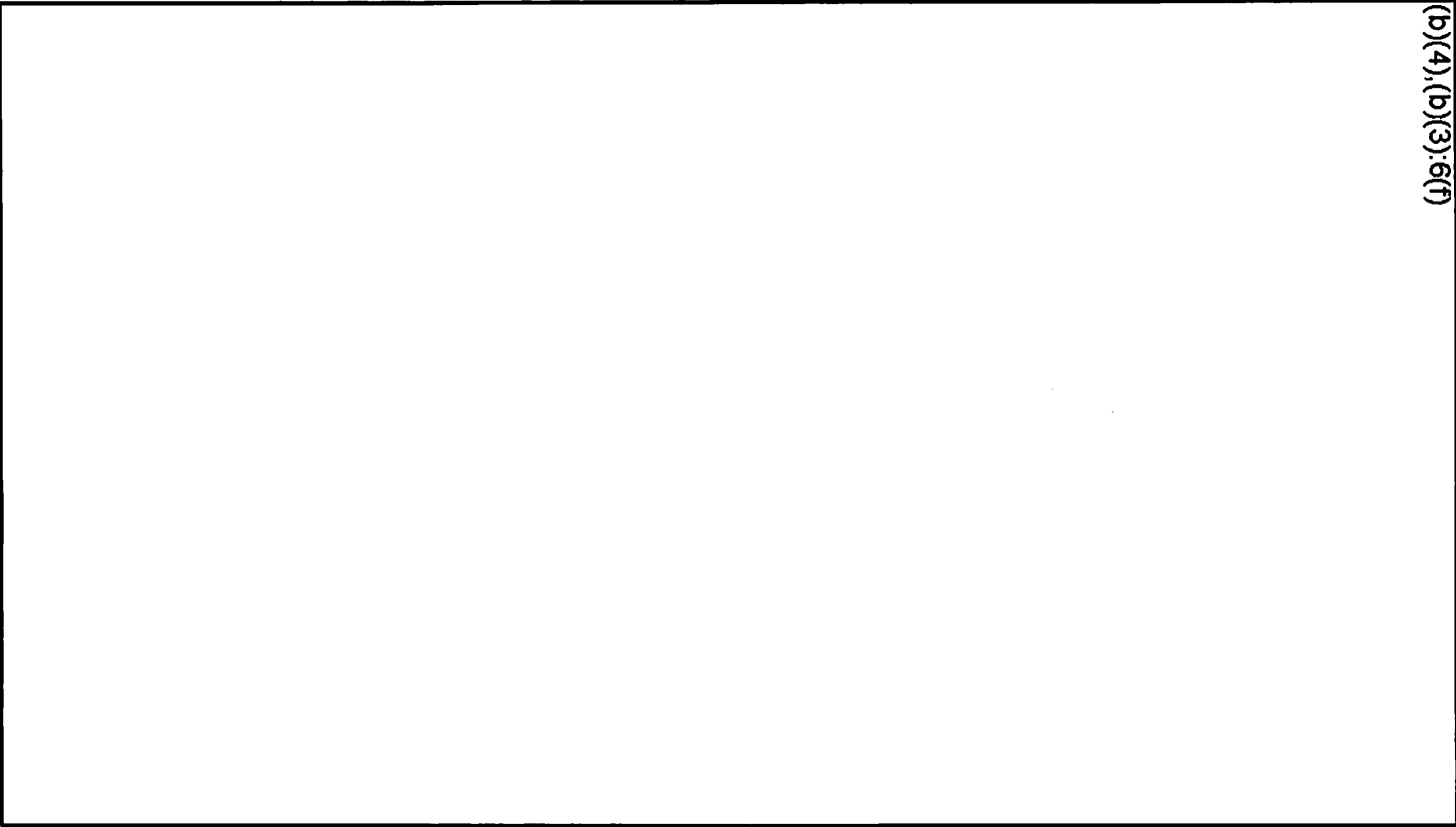
HIGHLY CONFIDENTIAL

000079

epic.org



(b)(4), (b)(3), 6(f)



EPIC-13-04-26-FTC-FOIA-20130612-Production-2

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 76 of 79 **HIGHLY CONFIDENTIAL**

000080



Management's Assertion

The management of Facebook represents that as of and for the 180 days ended February 11, 2013 ("the Reporting Period"), in accordance with Parts IV and V of the Agreement Containing Consent Order ("The Order"), with a service date of August 15, 2012, between Facebook, Inc. ("the Company") and the United States of America, acting upon notification and authorization by the Federal Trade Commission ("FTC"), the Company had established and implemented a comprehensive Privacy Program, ("the Facebook Privacy Program"), based on Company specific criteria (described in paragraph two of this assertion); and the privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the Reporting Period.

The company specific criteria ("assertions") used as the basis for Facebook's Privacy Program are described below. The below assertions have corresponding controls on pages 21-76.

Assertion A - Responsibility for the Facebook Privacy Program, which is "Facebook has designated an employee or employees to coordinate and be responsible for the privacy program."

Assertion B - Privacy Risk Assessment, which is "Facebook has identified reasonably foreseeable, material risks, both internal and external, 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. This privacy risk assessment includes consideration of risks in areas of relevant operations, including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research."

Assertion C - Privacy and Security Awareness, which is "Facebook has a privacy and security for privacy awareness program in place which is defined and documented in privacy and security for privacy policies. The extent of communications to employees is based on their role and responsibility and may include internal communications through various channels, training, and the Privacy Cross-Functional ("XFN") team process."

Assertion D - Notice, Choice, Consent, Collection and Access, which is "Facebook provides notice about its privacy policies and procedures and terms of service to users which identifies the purposes for which personal information is collected and used, describes the choices available to users, obtains implicit or explicit consent, collects personal information only for the purposes identified in the notices and provides users with access to their personal information for review and update."

Assertion E - Use, Retention, Deletion and Quality, which is "Facebook limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. Facebook retains personal information for as long as necessary to provide services or fulfil the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information. Facebook maintains accurate, complete, and relevant personal information for the purposes identified in the notice."

1601 Willow Road, Menlo Park, California 94025
650.543.4800 - tel 650.543.4801 - fax

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 77 of 79 **HIGHLY CONFIDENTIAL**



Assertion F - Security for Privacy, which is "Facebook protects personal information of users against unauthorized access."

Assertion G - Third-party developers, which is "Facebook discloses personal information to third-party developers only for the purposes identified in the notice and with the implicit or explicit consent of the individual."

Assertion H - Service Providers, which is "Facebook has developed and used reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from the Company and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information."

Assertion I - On-going Monitoring of the Privacy Program, which is "Facebook evaluates and adjusts the Company's privacy program in light of the results of monitoring activities, any material changes to the Company's operations or business arrangements, or any other circumstances that the Company knows or has reason to know may have a material impact on the effectiveness of its privacy program."

Facebook, Inc.

By: _____

Edward Palmieri
Associate General Counsel, Privacy
Facebook, Inc.

By: _____

Daniel Li
Product Counsel
Facebook, Inc.

1601 Willow Road, Menlo Park, California 94025
650.543.4800 - tel 650.543.4801 - fax

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 78 of 79 **HIGHLY CONFIDENTIAL**



Appendix A – Assessment Interviews Summary

The primary Facebook individuals interviewed by PwC, as a part of the above Assessment procedures, include, but are not limited to, those individuals listed in the table below.

| Title | Team |
|---|--------------------------------|
| Chief Privacy Officer, Product | Privacy |
| Chief Privacy Officer, Policy | Public Policy |
| VP & Deputy General Counsel | Legal |
| Associate General Counsel, Privacy | Legal |
| Privacy & Product Counsel | Legal |
| Lead Contracts Manager | Legal |
| Compliance Associate | Legal |
| Privacy Program Manager | Identity |
| Specialist, User Operations | User Operations |
| Engineering Manager | Engineering |
| Software Engineer | Engineering |
| Developer Policy Enforcement Manager | Developer Operations |
| Platform Operations Analyst | Developer Operations |
| Chief Security Officer | Security |
| Manager, Information Security | Security |
| Policy and Operations Analyst | Security |
| Security Manager, Incident Response | Security |
| Mobile Program Manager | Mobile Partner Management |
| Recruiting Process Manager | Human Resources |
| US Data Center Operations Director | Infrastructure |
| Group Technical Program Manager | Infrastructure |
| Engineering Manager (formerly Instagram Chief Technology Officer) | Instagram - Engineering |
| User Operations Manager | Instagram - User Operations |
| Product Manager | Instagram - Product Management |

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.
Page 79 of 79 **HIGHLY CONFIDENTIAL**

EXHIBIT 7

United States Senate
WASHINGTON, DC 20510

COMMITTEES:
AGING
ARMED SERVICES
COMMERCE, SCIENCE, AND TRANSPORTATION
JUDICIARY
VETERANS' AFFAIRS

April 19, 2018

The Honorable Maureen Ohlhausen
Acting Chairman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Acting Chairman Ohlhausen,

I am pleased that the Federal Trade Commission (FTC) has opened an investigation into the privacy practices and policies at Facebook. Recent revelations about the illegitimate harvesting of personal data on tens of millions of Americans have shed new light on the systemic failure of Facebook to address privacy risks and keep its promises to users. Despite Mark Zuckerberg's recent apology tour, Facebook's history of negligence demonstrates that the company can no longer be trusted to self-regulate. I write to draw attention to information that may be relevant to your investigation, including evidence that Facebook may have violated its consent decree. I also encourage the FTC to pursue strong legal remedies to compensate consumers harmed and set enforceable rules on its future conduct.

In November 2011, Facebook agreed to a proposed settlement containing a consent decree after the FTC found that the company had deceived consumers by sharing personal data with advertisers and making public information previously designated as private. Under the settlement, Facebook was barred from misrepresenting the privacy of personal information and was required to obtain affirmative express consent before enacting changes would override privacy preferences. The FTC also required Facebook to establish "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."

Facebook's adherence to the consent decree has been called into question based on recent reports that the political consulting firm Cambridge Analytica and Global Science Research (GSR) had harvested a large-scale dataset of Facebook users based on a third-party app. The GSR app would collect demographic details, private communications, and other profile metrics of those who installed the app and their friends. Based on Facebook's permissive, default privacy settings, Cambridge Analytica was able to obtain information from up to 87 million profiles based on only about 300,000 users installing the GSR app.

This should have never happened. The FTC put Facebook on notice about the privacy risks of third-party apps in its complaint. Three of the FTC's claims concerned the misrepresentation of verification and privacy preferences of third-party apps. In 2008, shortly after the launch of its developer platform, Facebook introduced a "Verified Apps" program, which would provide a badge that Facebook had certified the security, privacy, trustworthiness, and transparency of an app.¹ When Facebook announced it would be ending the program the following year, it claimed that it would be extending these trust standards into *all* apps. However, in its 2011 complaint, the FTC found that despite claims of auditing, Facebook took no steps to verify either the security or protections for collected user information. Seven years later, exactly how Facebook verifies third-party apps is still murky.

The Cambridge Analytica revelations demonstrate that Facebook continued to turn a blind eye to third-party apps despite the FTC mandated privacy program. Facebook should have been aware that GSR was planning to violate developer platform rules based on the policies that developers are required to submit. GSR's terms of service ("Attachment 1") stated explicitly that it reserved the right to sell user data and would collect profile information from friends. These terms of service should have put Facebook on notice that GSR may be seeking to sell user data. At this month's Senate hearing on Facebook, Mr. Zuckerberg informed me that its app review team would have been responsible for vetting the policy and acknowledged that Facebook "should have been aware that this application developer submitted a [terms of service] that was in conflict with the rules of the platform."

Even the most rudimentary oversight would have uncovered these problematic terms of service. Moreover, Facebook knew as early as 2010 that third-party app developers were selling information to data brokers.² The fact that Facebook did not uncover these non-compliant terms strongly suggests that its "comprehensive privacy program" established pursuant to the FTC consent decree was either inadequate to address threats or not followed in practice. This willful blindness left users vulnerable to the actions of Cambridge Analytica.

The Cambridge Analytica matter also calls into question Facebook's compliance with the consent decree's requirements to respect privacy settings and protect private information. Three years after Facebook agreed to the consent decree, Facebook by default continued to provide broad access to personal data to third party apps, data that may not have been marked as public. In evaluating claims of deception and misrepresentation of privacy controls, the FTC has typically considered what a consumer would have reasonably understood their settings to mean. No information was readily provided to users about this permissive sharing to third-party apps or how to opt out. Nor were users informed about which apps accessed their profiles or given the ability to resolve unwanted intrusions. While users could be judicious about their privacy settings and the apps they installed, the actions of only one friend could thwart their efforts without their knowledge. The ease with which the GSR app was able to harvest data on 87 million users

¹ "Guiding Principles." Facebook Developers.

https://web.archive.org/web/20080902015608/http://developers.facebook.com/get_started.php?tab=principles

² "Facebook Shuts Down Apps That Sold User Data, Bans Rappleaf." AdAge. October 29, 2010.

www.adweek.com/digital/facebook-shuts-down-apps-that-sold-user-data-bans-rappleaf/

demonstrates that third parties were effectively able to override privacy preferences without express consent.

It is also noteworthy that the relaxation of data retention policies for third party developers may have contributed to the illegitimate collection of data. In a version of its Developer Principles and Policies dated December 1, 2009, Facebook mandated that developers “must not store or cache any data you receive from us for more than 24 hours” and “must not give data you receive from us to any third party.”³ In April 2010, Facebook changed this policy to permit developers to keep user information with significantly reduced restrictions on the sharing of data.⁴ There is no indication that Facebook informed its users that third parties would now be allowed to store their data or share it.

Facebook had multiple opportunities to prevent this harvesting and notify users before March 2018, but failed to do so. According to former Cambridge Analytica employee Christopher Wylie, the GSR app had collected data so aggressively that it triggered Facebook’s security protocols.⁵ However, there is no indication Facebook took steps to investigate or limit the collection despite the problematic terms of service.

Facebook finally acted on the GSR app after *The Guardian* reported on Cambridge Analytica’s plans in December 2015. While Facebook removed the application and contacted both companies to request the destruction of user information, its response continued to be inadequate. Facebook did not take any steps to prevent Cambridge Analytica and its partners from continuing to use its platform for advertising or analytics services, even working alongside the company within campaigns. It did not provide notice to users about how their information has been harvested by Cambridge Analytica, nor did it inform the FTC about the collection of data without user consent. Facebook did not contact Christopher Wylie to request the deletion of user data until the following August – at least nine months after the initial report. Facebook took no further action to assess whether data had been deleted. The ineffective response calls into question how seriously the company took this incident and others like it.

Former Facebook employees have told me that its staff were not empowered to effectively enforce privacy policies. For example, Sandy Parakilas, who led efforts to fix privacy problems on its developer platform from June 2011 to August 2012, describes Facebook as a company that would not commit resources or attention to protecting users against violations from third-party apps. Mr. Parakilas’ letter to me (“Attachment 2”) along with his November 19, 2017 *New York Times* op-ed and April 10, 2018 interview with *New York Magazine*, highlight a deeply disturbing pattern of disregard by Facebook to the privacy risks posed by third-party apps. Mr. Parakilas recounts how one executive told him, after proposing a deeper audit of

³ “Developer Principles and Policies.” Facebook Developers. December 1, 2009. <https://web.archive.org/web/20091223051700/http://developers.facebook.com/policy/>

⁴ “A New Data Model.” Facebook. April 21, 2010. <https://web.archive.org/web/20120502125823/http://developers.facebook.com/blog/post/378/>

⁵ Cadwalladr, Carole. “I made Steve Bannon’s psychological warfare tool’: meet the data war whistleblower.” *The Observer*. March 17, 2018. <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>

developers' use of data, "Do you really want to see what you'll find?" Had Facebook taken such requests more seriously at the time, the GSR app might have been caught earlier.

Facebook has acknowledged it has neglected its privacy controls, which had non-functional settings and often outdated descriptions did not reflect how the platform operates.⁶ Overall Facebook's privacy controls were arcane and difficult to navigate, preventing users from effectuating their preferences. Such deficiencies indicate that Facebook did not maintain an adequate privacy program that was sufficient to protect users and enable them to exercise informed consent.

We may never know the full extent of the damage caused by the failure to provide adequate controls and protection to users. A month after the recent Cambridge Analytica reports, Facebook has not disclosed information on how many applications engaged in similar data collection, but has stated that it expects to have to audit thousands of suspicious applications. As before, it remains only externally reactive to public reports, for example suspending the company CubeYou after media covered its commercial activities. The Facebook developer platform was launched in 2007 and stronger protections for consumers were not implemented until 2015. Presumably many of those companies that developed platform application have shut down, contact details changed, and record trails lost. While Mr. Zuckerberg has committed to audit suspicious apps, it is clear that Facebook will never be able to fully assess the impact of its years of neglect.

Facebook now bears little resemblance to the company it was at the time of the consent decree, necessitating a vigorous investigation into its privacy practices across its range of products and activities. Since November 2011, its expansion and acquisitions have strengthened the company's dominance in the social networking market and increased the significance of the challenges posed to consumers. Consumers, civil society, and members of Congress have raised an expansive set of privacy concerns, including its collection of Internet traffic for surveilling competitors; purchase of personal information from data brokers; tracking of non-Facebook users across the web; and harvesting of communications metadata from phones. These allegations raise new issues relevant to the consent decree that should be in the scope of the FTC's review.

The FTC ordered the consent decree in response to Facebook's repeated failures to address privacy risks, and put into place rules on how the company should act to protect users. If its investigation find that Facebook has violated the consent decree or engaged in further unfair or deceptive acts and practices, it should seek both monetary penalties that provide redress for consumers and impose stricter oversight on Facebook. The FTC should consider further measures that rigorously protects consumers, such as:

- data minimization standards that requires Facebook to retain and use data only for services expressly requested by users;
- limits on the combining and sharing of data between Facebook-owned services;

⁶ "It's Time to Make Our Privacy Tools Easier to Find." Facebook. March 28, 2018. <https://newsroom.fb.com/news/2018/03/privacy-shortcuts/>

- transparency on the types of data that Facebook collects from users and from other sources, and to publicly account for how that data is used;
- restrictions on collection of data from its “social plug-ins,” cross-device tracking, and or data brokers;
- appointment of a third-party monitor to oversee changes to Facebook’s privacy and data use policies and practices, with periodic reinvestigation; and,
- organizational changes to ensure that privacy and data use is protected at all levels.

While the Cambridge Analytica revelations have raised awareness to Facebook’s failure to provide users with adequate information or safeguards to protect privacy, many have raised legitimate and broad-reaching concerns about the company’s practices beyond a single ‘bad actor’ problem. Mr. Zuckerberg has acknowledged that the incident was a breach of trust between Facebook and its users, a broken promise that requires redress for consumers and enforceable commitments that deter further breaches. It is time for the FTC to thoroughly and rigorously reassess Facebook’s privacy practices and put into place rules that finally protect consumers.

Thank you for your attention to this important matter.

Sincerely,



Richard Blumenthal
United States Senate

Attachment 1

Global Science Research (GSR) Terms of Service

GSRApp APPLICATION END USER TERMS AND CONDITIONS

1. **The Parties:** This Agreement (“Agreement”) is between Global Science Research (“We”, “Us” or “GSR”), which is a research organisation registered in England and Wales (Number: 9060785) with its registered office based at Magdelene College, Cambridge, UK CB3 0AG, and the User of the Application (“You” or “User”).
2. **Agreement to Terms:** By using GSRApp APP (“Application”), by clicking “OKAY” or by accepting any payment, compensation, remuneration or any other valid consideration, you consent to using the Application, you consent to sharing information about you with us and you also accept to be bound by the Terms contained herein.
3. **Purpose of the Application:** We use this Application as part of our research on understanding how people's Facebook data can predict different aspects of their lives. Your contribution and data will help us better understand relationships between human psychology and online behaviour.
4. **Data Security and Storage:** Data security is very important to us. All data is stored on an encrypted server that is compliant with EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data.
5. **Your Statutory Rights:** Depending on the server location, your data may be stored within the United States or in the United Kingdom. If your data is stored in the United States, American laws will regulate your rights. If your data is stored within the United Kingdom (UK), British and European Union laws will regulate how the data is processed, even if you live in the United States. Specifically, data protection and processing falls under a law called the Data Protection Act 1998. Under British and European Union law, you are considered to be a “Data Subject”, which means you have certain legal rights. These rights include the ability to see what data is stored about you. Where data held in the EU is transferred to the United States, GSR will respect any safe harbour principles agreed between the United States Department of Commerce and the European Commission. The GSR Data Controller can be contacted by e-mail at alexbkogan@gmail.com.
6. **Information Collected:** We collect any information that you choose to share with us by using the Application. This may include, inter alia, the name, demographics, status updates and Facebook likes of your profile and of your network.
7. **Intellectual Property Rights:** If you click “OKAY” or otherwise use the Application or accept payment, you permit GSR to edit, copy, disseminate, publish, transfer, append or merge with other databases, sell, licence (by whatever means and on whatever terms) and archive your contribution and data. Specifically, agreement to these Terms also means you waive any copyright and other intellectual property rights in your data and contribution to GSR, and grant GSR an irrevocable, sublicenceable, assignable, non-

exclusive, transferrable and worldwide license to use your data and contribution for any purpose. You acknowledge that any and all intellectual property rights and database rights held in your data or contribution that is acquired by GSR or the Application will vest with GSR and that you will not have any claim in copyright, contract or otherwise. Nothing in this Agreement shall inhibit, limit or restrict GSR's ability to exploit, assert, transfer or enforce any database rights or intellectual property rights anywhere in the world. You also agree not attempt to appropriate, assert claim to, restrict or encumber the rights held in, interfere with, deconstruct, discover, decompile, disassemble, reconstruct or otherwise reverse-engineer the Application, the data collected by the Application or any other GSR technology, algorithms, databases, methods, formulae, compositions, designs, source code, underlying ideas, file formats, programming interfaces, inventions and conceptions of inventions whether patentable or un-patentable.

8. **Informed Consent:** By signing this form, you indicate that you have read, understand, been informed about and agree to these Terms. You also are consenting to have your responses, opinions, likes, social network and other related data recorded and for the data collected from you to be used by GSR. If you do not understand these Terms, or if you do not agree to them, then we strongly advise that you do not continue, do not click "OKAY", do not use the Application and do not to collect any compensation from us.
9. **Variation of Terms:** You permit GSR to vary these Terms from time to time to comply with relevant legislation, for the protection of your privacy or for commercial reasons. If you choose to provide us with your e-mail address, notice of any variation will be sent to that e-mail address. If you do not provide us with an e-mail address, you waive your right to be notified of any variation of terms.
10. **Rights of Third Parties:** A person who is not a Party to this Agreement will not have any rights under or in connection with it.

THISISYOURDIGITALLIFE APP APPLICATION END USER TERMS AND CONDITIONS

1. The Parties: This Agreement ("Agreement") is between Global Science Research ("We", "Us" or "GSR"), which is a research organisation registered in England and Wales (Number: 9060785) with its registered office based at St John's Innovation Centre, Cowley Road, Cambridge, CB4 0WS, and the User of the Application ("You" or "User").

2. Agreement to Terms: By using THISISYOURDIGITALLIFE APP ("Application"), by clicking "OKAY" or by accepting any payment, compensation, remuneration or any other valid consideration, you consent to using the Application, you consent to sharing information about you with us and you also accept to be bound by the Terms contained herein.

3. Purpose of the Application: We use this Application to (a) provide people an opportunity to see their predicted personalities based on their Facebook information, and (b) as part of our research on understanding how people's Facebook data can predict different aspects of their lives. Your contribution and data will help us better understand relationships between human psychology and online behaviour.

4. Data Security and Storage: Data security is very important to us. All data is stored on an encrypted server that is compliant with EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data.

5. Your Statutory Rights: Depending on the server location, your data may be stored within the United States or in the United Kingdom. If your data is stored in the United States, American laws will regulate your rights. If your data is stored within the United Kingdom (UK), British and European Union laws will regulate how the data is processed, even if you live in the United States. Specifically, data protection and processing falls under a law called the Data Protection Act 1998. Under British and European Union law, you are considered to be a "Data Subject", which means you have certain legal rights. These rights include the ability to see what data is stored about you. Where data held in the EU is transferred to the United States, GSR will respect any safe harbour principles agreed between the United States Department of Commerce and the European Commission. The GSR Data Controller can be contacted by e-mail at info@globalscienceresearch.com.

6. Information Collected: We collect any information that you choose to share with us by using the Application. This may include, inter alia, the name, demographics, status updates and Facebook likes of your profile and of your network.

7. Intellectual Property Rights: If you click "OKAY" or otherwise use the Application or accept payment, you permit GSR to edit, copy, disseminate, publish, transfer, append or merge with other databases, sell, licence (by whatever means and on whatever terms) and archive your contribution and data. Specifically, agreement to these Terms also means you waive any copyright and other intellectual property rights in your data and contribution to GSR, and grant GSR an irrevocable, sublicenceable, assignable, non-exclusive, transferrable and worldwide license to use your data and contribution for any purpose. You acknowledge that any and all intellectual property rights and database rights held in your data or contribution that is acquired by GSR or the Application will vest with GSR and that you will not have any claim in copyright, contract or otherwise. Nothing in this Agreement shall inhibit, limit or restrict GSR's ability to exploit, assert, transfer or enforce any database rights or intellectual property rights anywhere in the world. You also agree not attempt to appropriate, assert claim to, restrict or encumber the rights held in, interfere with, deconstruct, discover, decompile, disassemble, reconstruct or otherwise reverse-engineer the Application, the data collected by the Application or any other GSR technology, algorithms, databases, methods, formulae, compositions, designs, source code, underlying ideas, file formats, programming interfaces, inventions and conceptions of inventions whether patentable or un-patentable.

8. Informed Consent: By signing this form, you indicate that you have read, understand, been informed about and agree to these Terms. You also are consenting to have your responses, opinions, likes, social network and other related data recorded and for the data collected from you to be used by GSR. If you do not understand these Terms, or if you do not agree to them, then we strongly advise that you do not continue, do not click "OKAY", do not use the Application and do not to collect any compensation from us.

9. Variation of Terms: You permit GSR to vary these Terms from time to time to comply with relevant legislation, for the protection of your privacy or for commercial reasons. If you choose to provide us with your e-mail address, notice of any variation will be sent to that e-mail address. If you do not provide us with an e-mail address, you waive your right to be notified of any variation of terms. 10. Rights of Third Parties: A person who is not a Party to this Agreement will not have any rights under or in connection with it.

- [Privacy Policy](#)

- Powered by Global Science Research

© 2014 Global Science Research LTD. All content is copyrighted. St John's Innovation Centre,
Cowley Road, Cambridge, CB4 0WS

Email: info@globalscienceresearch.com

Attachment 2

Sandy Parakilas Letter

Sandy Parakilas

Dear Senator Blumenthal,

In 2011 and 2012, I led the team responsible for overseeing Facebook's data policy enforcement efforts governing third-party application developers who were using Facebook's App Platform, and responding to violations of that policy.

In my first week on the job, I was told about a troubling feature of the App Platform: there was no way to track the use of data after it left Facebook's servers. That is, once Facebook transferred user data to the developer, Facebook lost all insight into or control over it. To prevent abuse, Facebook created a set of platform policies that forbade certain kinds of activity, such as selling the data or passing it to an ad network or data broker such as Cambridge Analytica.

Facebook had the following tools to deal with developers who abused the platform policies: it could call the developer and demand answers; it could demand an audit of the developer's application and associated data storage, a right granted in the platform policies; it could ban the developer from the platform; it could sue the developer for breach of the policies; or it could do some combination of the above. During my sixteen months at Facebook, I called many developers and demanded compliance, but I don't recall the company conducting a single audit of a developer where the company inspected the developer's data storage. Lawsuits and outright bans for data policy violations were also very rare.

Despite the fact that executives at Facebook were well aware that developers could, without detection, pass data to unauthorized fourth parties (such as what happened with Cambridge Analytica), little was done to protect users. A similar, well-publicized incident happened in 2010, where Facebook user IDs were passed by apps to a company called Rapleaf, which was a data broker. Despite my attempts to raise awareness about this issue, nothing was done to close the vulnerability. It was difficult to get any engineering resources assigned to build or maintain critical features to protect users.

Unfortunately, Facebook's failure to address this clear weakness, during my time there or after I left, led to Cambridge Analytica's misappropriation of tens of millions of Americans' data.

Sincerely,

A handwritten signature in black ink, appearing to read "Sandy Parakilas". The signature is written in a cursive, flowing style.

Sandy Parakilas