

Lesley E. Weaver (SBN 191305)  
BLEICHMAR FONTI & AULD LLP  
555 12th Street, Suite 1600  
Oakland, CA 94607  
Tel.: (415) 445-4003  
Fax: (415) 445-4020  
lweaver@bfalaw.com

Derek W. Loeser (admitted *pro hac vice*)  
KELLER ROHRBACK L.L.P.  
1201 Third Avenue, Suite 3200  
Seattle, WA 98101  
Tel.: (206) 623-1900  
Fax: (206) 623-3384  
dloeser@kellerrohrback.com

*Plaintiffs' Co-Lead Counsel*

*Additional counsel listed on signature page*

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA**

IN RE: FACEBOOK, INC. CONSUMER  
PRIVACY USER PROFILE LITIGATION

MDL No. 2843  
Case No. 18-md-02843-VC

This document relates to:

ALL ACTIONS

**SECOND AMENDED CONSOLIDATED  
COMPLAINT**

Judge: Hon. Vince Chhabria

## TABLE OF CONTENTS

I.	INTRODUCTION .....	1
II.	JURISDICTION, VENUE, AND CHOICE OF LAW .....	5
III.	PARTIES .....	6
A.	Plaintiffs .....	6
B.	Defendants and Co-Conspirators .....	85
1.	Prioritized Defendant and Doe Defendants: .....	85
2.	Non-Prioritized Defendants (Individual Defendants Named in Actions Consolidated in this MDL as to Whom Co-Lead Counsel Seek a Stay) .....	86
C.	Interested Parties .....	86
D.	Unnamed Co-Conspirators: Cambridge-Analytica-Related Entities .....	87
E.	Other Non-Defendant Co-Conspirator .....	89
IV.	FACTUAL BACKGROUND .....	89
A.	Facebook’s Transition from Social Media Company to Data Broker .....	89
1.	Facebook Encouraged User Engagement to Drive Advertising Revenues .....	91
2.	User Engagement Increased When Facebook Gave App Developers Users’ Content and Information .....	93
3.	Facebook’s Partnerships with Data Brokers Resulted in Aggregated, Deanonymized User Information .....	101
4.	The Wealth of Data About Users Enabled Highly Invasive Forms of Psychographic Marketing .....	103
B.	Facebook Made It Difficult and Sometimes Impossible for Users to Prevent Facebook from Publishing Their Content and Information to Third-Party Applications. ....	107
1.	Overview of the Facebook User Platform .....	107
2.	Facebook Falsely Promised Users That Their Privacy Controls Limited Sharing of Their Content and Information to the Audiences They Selected .....	108

3.	Facebook’s “Privacy Controls” Misled Users About How to Control the Information and Content That They Shared with Applications.....	109
4.	To Control Sharing with Applications, Facebook Required Users to Hunt for, Find, and Change the Default Preferences of Their App Settings. ....	117
5.	Facebook Changed the Default Privacy Settings from 2010-2014 to Make More Content Public, Prompting FTC Action. ....	124
C.	Facebook Allowed Third Parties to Access Facebook Users’ Content and Information Without or Beyond the Scope of Users’ Consent. ....	127
1.	Facebook Developed an Interface That Allowed App Developers to Access a Facebook User’s Content and Information Via That User’s Friend. ....	127
2.	Graph API Allows App Developers to Access Users’ Video Information....	134
3.	To Allow Third Parties Unfettered Access to Users’ Content and Information, Facebook Stripped Users’ Privacy Designations for Certain Content Available on Graph API. ....	137
4.	Cambridge Analytica Used Facebook’s Graph API Interface to Take Users’ Content and Information. ....	141
5.	The Cambridge Analytica Scandal Has Triggered Additional Revelations of Apps’ Misuse of User Content and Information.....	153
6.	Facebook Also Enabled Device Makers and Other Business Partners to Access Users’ Content and Information Through Friends.....	155
7.	Facebook Extended Certain “Whitelisted” Companies Access to Friends’ Information Despite Facebook’s Contrary Representations to Users.....	159
D.	Facebook Failed to Monitor and to Protect User Content and Information from Third Parties’ Unauthorized Use. ....	166
1.	Facebook Has a History of Discarding Its Promises to Protect User Privacy in Reckless Pursuit of Growth. ....	167
2.	Facebook Ignored Internal Warnings Regarding Risks Posed by Third Parties’ Access to Users’ Content and Information. ....	171
3.	Facebook Failed to Monitor Business Partners’ and Whitelisted Companies’ Use of Users’ Content and Information. ....	175
4.	Facebook Failed to Limit Business Partners’ and Whitelisted Companies’ Access to Users’ Content and Information. ....	177

5. Facebook Allowed Business Partners and Whitelisted Companies to Deceive Users About Their Access to Users’ Content and Information. ....	178
6. Facebook Also Took No Action to Ensure App Developers Followed Its Platform and Privacy Policies. ....	180
7. Facebook Failed to Adequately Mitigate Harm Caused by Kogan and Cambridge Analytica or to Prevent Further Risk of Harm. ....	181
8. Facebook’s Failure to Notify Plaintiffs of the Misuse of Their Data Hindered User’s Ability to Take Remedial Measures. ....	183
E. Plaintiffs Did Not Consent to Facebook’s Misconduct. ....	184
1. Facebook’s SRR and Data Policy Did Not Create Consent. ....	184
a. Facebook’s SRR and Data Policy Did Not Create Consent with Respect to the VPPA. ....	185
b. Facebook’s SRR and Data Policy Did Not Create Consent to Conduct that Violated the SRR and Data Policy. ....	186
(i) By Allowing Users No Control over Sharing with Business Partners, Facebook Violated Its Pledge That Users Would Have Control over How Their Content and Information Was Shared. ....	186
(ii) Facebook Violated Its Pledge That Apps and Websites Would Use Users’ Content and Information Merely “in Connection with” Their Friends. ....	186
(iii) By Continuing to Allow Whitelisted Apps and Business Partners’ Apps to Have Access Even to Users That Had Turned off All App Access, Facebook Violated Its Pledge That Users Could Bar Apps from Accessing Their Data. ....	187
(iv) Facebook Violated Its Pledge Not to Give Content and Information to Advertisers by Permitting Access by Apps, Websites, and Business Partners That Were Also Advertisers. ....	188
(v) By Stripping Metadata from Content and Information, Facebook Violated Its Pledge That Apps Would Respect Users’ Privacy. ....	190
c. Users Did Not Consent to Misconduct That the Documents Wholly Failed to Disclose. ....	190
(i) Facebook Failed to Disclose Its Data Sharing with Business Partners ....	191
(ii) Facebook Failed to Disclose Psychographic Profiling. ....	192

(iii)Facebook Failed to Disclose That When Apps and Websites Accessed Data from the Friends of Users, Those Friends’ Privacy Metadata Was Stripped. ....	192
d. Users Who Were Not Notified of New Disclosures After Initiating Their Accounts Did Not Provide Consent to the Newly Disclosed Conduct. ....	192
(i) Facebook did not notify users of updates to the Data Policy or SRR. ....	192
(ii) Users who signed up before December 9, 2009 did not consent to allowing third-party Apps and websites to access their content and information via their Friends. ....	193
(iii)Users who signed up from December 9, 2009 to April 22, 2010 did not consent to the broad access that applications and websites had to users’ content and information via their Friends. ....	194
(iv)Users who signed up before September 7, 2011 did not consent to any sharing with Business Partners. ....	195
e. Because the Data Policy Was Not Part of a Contract and Was Not Reasonably Prominent or Accessible, Users Did Not Consent to Two Matters That the Data Policy, but Not the SRR, Disclosed. ....	195
(i) Users Did Not Expressly Consent to Sharing with Third-Party Apps and Websites Because the Data Policy Was Not Incorporated into a Binding Contract. ....	196
(ii) The Data Policy Did Not Create Implied Consent Because It Was Not Reasonably Prominent or Accessible. ....	201
2. Nothing Outside the SRR and Data Policy Created Consent Either—to the Contrary, Statements That Facebook Made Lulled Users into Believing Their Privacy Was Protected. ....	204
F. Facebook’s Sharing User Content and Information with Third Parties Without Users’ Consent Violates the 2012 Federal Trade Commission Consent Decree .....	205
G. Facebook Has Faced Numerous Regulatory and Governmental Agency Investigations for Disregarding the Privacy of Its Users. ....	213
H. In the Wake of the Cambridge Analytica Scandal, Facebook Has Acknowledged That It Breached Users’ Trust. ....	222
I. Facebook’s CEO Authorized Decisions That Gave Rise to Privacy Violations .....	224
1. Statements by Facebook’s CEO Give Rise to a Duty to Disclose and Admit to Injury from Lack of Disclosure. ....	224

J.	Facebook’s CEO Drove Initiatives to Erode Privacy and Monetize Access to Content and Information.....	230
V.	PLAINTIFFS SUFFERED INJURY AND DAMAGES AS A DIRECT RESULT OF FACEBOOK’S CONDUCT .....	233
A.	Plaintiffs Suffered Invasions of Their Privacy.....	233
	1. Facebook Has Subjected Its Users to Highly Offensive, Harmful, and Invasive Forms of Psychographic Marketing.....	234
B.	Plaintiffs Suffered Economic Injury. ....	243
VI.	PLAINTIFFS COULD NOT HAVE DISCOVERED THEIR CLAIMS UNTIL 2018 ..	250
VII.	CHOICE OF LAW .....	252
VIII.	CLASS ACTION ALLEGATIONS .....	252
IX.	CAUSES OF ACTION .....	268
A.	Prioritized Claims .....	268
	Claim I. Violation of the Stored Communications Act (“SCA”), 18 U.S.C. §§ 2701 <i>et seq.</i> ....	268
	Claim II. Violation of Video Privacy Protection Act, 18 U.S.C. § 2710272	
	Claim III. Deceit by Concealment or Omission Cal. Civ. Code §§ 1709 & 1710.....	276
	Claim IV. Invasion of Privacy – Intrusion into Private Affairs .....	281
	Claim V. Invasion of Privacy – Public Disclosure of Private Facts .....	283
	Claim VI. Breach of Contract .....	286
	Claim VII. Negligence and Gross Negligence .....	288
	Claim VIII. Violations of the California Unfair Competition Law Cal. Bus. & Prof. Code §§ 17200 <i>et seq.</i> .....	293
	Claim IX. Violation of Article I, Section 1 of the California Constitution.....	297
	Claim X. Violation of California Common Law Right of Publicity .....	300
	Claim XI. Breach of the Implied Covenant of Good Faith and Fair Dealing .....	301
	Claim XII. Quantum Meruit to Recover Sums Had by Unjust Enrichment.....	304
B.	Priority Consumer Protection Act Claims Alleged in the Alternative.....	305
	Claim XIII. Violations of the Alabama Deceptive Trade Practices Act Ala. Code §§ 8-19-1 <i>et seq.</i> (2018).....	305

Claim XIV.	Violations of the Colorado Consumer Protection Act Colo. Rev. Stat. Ann. §§ 6-1-101 <i>et seq.</i> .....	307
Claim XV.	Violations of the Illinois Consumer Fraud and Deceptive Business Practices Act 815 Ill. comp. stat. Ann. §§ 505 <i>et seq.</i> .....	309
Claim XVI.	Violations of the Iowa Private Right of Action for Consumer Frauds Act Iowa Code Ann. § 714H.....	311
Claim XVII.	Violations of the Kansas Consumer Protection Act Kan. Stat. Ann. §§ 50-623 <i>et seq.</i> .....	313
Claim XVIII.	Violations of the Michigan Consumer Protection Act Mich. Comp. Laws Ann. §§ 445.901 <i>et seq.</i> .....	315
Claim XIX.	Violations of the New York General Business Law N.Y. Gen. Bus. Law §§ 349 <i>et seq.</i> .....	317
Claim XX.	Violations of the Washington Consumer Protection Act Wash. Rev. Code Ann. §§ 19.86.010 <i>et seq.</i> .....	319
Claim XXI.	Violations of the West Virginia Consumer Credit and Protection Act.....	320
C.	Non-Prioritized Claims .....	324
Claim XXII.	Racketeer Influence and Corrupt Organizations Act, 18 U.S.C. § 1962(c) .....	324
Claim XXIII.	Misappropriation of Valuable Property (Against Prioritized Defendant Facebook and Doe Defendants) .....	328
Claim XXIV.	Fraudulent Misrepresentation .....	328
Claim XXV.	Negligent Misrepresentation .....	329
Claim XXVI.	Trespass to Personal Property .....	330
Claim XXVII.	Conversion .....	331
Claim XXVIII.	Violation of California Consumer Record Act .....	331
Claim XXIX.	Violation of California Invasion of Privacy Act (Cal. Pen. Code § 637.7) .....	333
Claim XXX.	Violation of the California Consumers Legal Remedies Act .....	334
Claim XXXI.	Violation of California's Computer Data Access and Fraud Act .....	335
Claim XXXII.	Violations of Common Law Right to Privacy in the Following States: Alabama; Arizona; Colorado; Florida; Georgia; Idaho; Indiana; Iowa; Kansas; Maryland; Michigan; Missouri; Ohio; Oklahoma; Pennsylvania; Tennessee; Texas; Washington; West Virginia; and Wisconsin .....	336
Claim XXXIII.	Violations of Alabama Right of Publicity Statute, Ala. Code § 6-5-772.....	337

Claim XXXIV.	Violations of Florida Unauthorized Publication Statute, Fla. State Code § 540.08 .....	338
Claim XXXV.	Violations of Illinois Right of Publicity Statute, Ill. Comp. Stat. § 1075/10 .....	339
Claim XXXVI.	Violations of Indiana Rights of Publicity Code, Ind. Code § 32-36-1-8 .....	340
Claim XXXVII.	Violations of New York Right to Privacy Statute, N.Y. Civ. Rights Law § 51 .....	341
Claim XXXVIII.	Violations of Ohio Right of Publicity Statute, Ohio Code § 2741.02 .....	342
Claim XXXIX.	Violations of Oklahoma Rights of Publicity Statute, Okl. St. § 1449.....	343
Claim XL.	Violations of Pennsylvania Unauthorized Use Statute, 42 Pa. Stat. § 8316.....	343
Claim XLI.	Violations of Tennessee Protection of Personal Rights Statute T.C.A. § 47-25-1105 .....	344
Claim XLII.	Violations of Virginia Unauthorized Use Statute, Va. Code § 8.01-40.....	345
Claim XLIII.	Violations of Washington Personality Right Statue, Wash. Code § 63.60.050.....	346
Claim XLIV.	Violations of Wisconsin Right of Publicity Statute, Wis. Stat. § 995.50.....	347
Claim XLV.	Violations of California Right of Publicity Statute, Cal. Civil Code § 3344.....	348
Claim XLVI.	Violations of the Fair Credit Reporting Act 15 U.S.C. §§ 1681 <i>et seq.</i> .....	349
Claim XLVII.	Unlawful Interception of Communications, 11 Del. Code § 2401 .....	350
Claim XLVIII.	Violation of New Jersey Consumer Fraud Act, N.J. Stat. Ann. §§ 56:8-1 <i>et seq.</i> .....	352
Claim XLIX.	Intentional Misrepresentation .....	353
X.	PRAYER FOR RELIEF .....	354
XI.	DEMAND FOR JURY TRIAL .....	355



Plaintiffs Steven Akins, Rafael Amezcua, Jason Ariciu, Samuel Armstrong, Anthony Bell, Bridgett Burk, Naomi Butler, Peter Christley, Terry Fischer, Shelly Forman, Brandon Herman, Tabielle Holsinger, Tyler King, William Lloyd, Jordan O'Hara, Kimberly Robertson, Scott Schinder, Cheryl Senko, Dustin Short, Tonya Smith, Charnae Tutt, Juliana Watson, and Annie Wenz, individually and as representatives of Classes of similarly situated persons, by their undersigned counsel, allege as follows:

## I. INTRODUCTION

1. Just fifteen years after its founding, Facebook, Inc. (“Facebook” or the “Company”) has become one of the world’s most influential companies. Its reach today is immense. More than 2.2 billion people around the world use its platform to connect with each other and it is no exaggeration that this connectivity has transformed the world. For many people, the platform has become an indispensable tool in keeping up with friends, running a business, advancing in a career, or remaining informed about current events.

2. Facebook’s indispensability and ubiquity are precisely what make its misconduct so damaging. It sold access to users’ private information—content that users had designated as nonpublic—without users’ consent. In doing so, Facebook caused users’ privacy to be invaded and inflicted economic harm on them. This action seeks appropriate remedies for those injuries.

3. In 2018, journalists uncovered that Cambridge Analytica, a British political consulting firm, paid a Facebook application developer<sup>1</sup> to collect and analyze the content and information<sup>2</sup> of approximately eighty-seven million Facebook users (the “Cambridge Analytica Scandal” or “Scandal”). Cambridge Analytica then used this data during the 2016 election season to target voters and lobby them, both on and off Facebook, with messages about political candidates.

---

<sup>1</sup> An “Application Developer” is a developer of Facebook applications.

<sup>2</sup> As used here, “content and information” means “content” and “information” as Facebook’s Statements of Rights and Responsibilities have defined those terms. In brief, Facebook has generally used “information” to mean facts and other information about Facebook users, including the actions they take, and “content” to mean anything users post on Facebook that would not be included in the definition of “information.” In addition, as used in this complaint, the terms include both personally identifiable content and information *and* anonymized content and information that is capable of being de-anonymized.

4. Cambridge Analytica's abuse of user content and information was neither isolated nor unusual. Facebook allowed tens of thousands of third-party apps ("Apps")<sup>3</sup> to download user content and information, and was willfully indifferent to monitoring them.

5. Facebook also sold access to users' information to a wide range of business partners—a diverse group that included not only device makers but media and entertainment companies like Netflix, the car service Lyft, the Russian search engine Yandex, the rental service Airbnb, and many more ("Business Partners").

6. These revelations have shown that Facebook is not just a social media company, but also a data broker and surveillance firm. Facebook encourages users to share their content so that Facebook can harvest it, aggregate it, and sell access to it. That content and information has tremendous economic value, and although Facebook tells users the content is their property, in fact Facebook is keeping all of its value. Facebook will not even disclose to users what it has amassed and what it makes available to its Business Partners. That is, Facebook is more transparent with its actual customers than with its users.

7. If Facebook wishes to be a data broker and surveillance firm, it must gain users' consent. Users could not consent to much of this misconduct because it remained secret until recently. In many cases, Facebook's misconduct affirmatively violated the pledges it made to users. Other aspects of its misconduct were simply never disclosed anywhere—necessarily precluding consent. Even when Facebook began to disclose some small part of its behavior, it at most notified only *new* users that it was engaging in such behavior. It did not notify existing users. And the document in which Facebook began to disclose some of what it was doing was never part of a contract—and even if it were contractual, was never prominent or accessible enough to have put a reasonably prudent user on notice.

8. Any assessment of users' consent must also take into account Facebook's misleading privacy controls and Facebook's manipulation of the default settings of those controls.

9. To encourage people to join and engage on its platform, Facebook misled users into believing that they controlled their content and information through certain affirmative "Privacy Settings and Tools."

---

<sup>3</sup> An "Application" is an interactive software application, such as a game, survey, or quiz.

10. Contrary to Facebook’s express promises, these settings did not prevent access by third-party Apps, websites, and Business Partners to users’ information. Users were not aware, and to a large extent are still not aware, that if a friend<sup>4</sup> interacts on a website with whom Facebook has an undisclosed business relationship, all of the content and information shared with that friend, even if shared with nonpublic settings between a few people, falls unrestricted into the hands of those companies.

11. In fact, investigation of counsel in this case has revealed that when Facebook allowed third parties to download user content and information, Facebook stripped users’ privacy settings from photos and videos before delivering it to the third parties. This means that the parties buying access to those photos and videos were not informed of users’ privacy restrictions. By doing this, Facebook made it possible for third parties to use this content without restrictions.

12. Facebook also manipulated users’ default privacy settings. In April 2010, Facebook unilaterally changed users’ default Profile Privacy Settings so that the default settings shared certain information publicly for new and existing users alike. This change sparked the concerns of privacy advocates and the Federal Trade Commission (“FTC”). The FTC sued Facebook, alleging that Facebook “deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public.”<sup>5</sup> Following the FTC’s intervention, Facebook and the FTC negotiated specific remedies, codified in the FTC’s consent decree, which was finalized in 2012.<sup>6</sup> Accordingly, in 2014, Facebook changed the default back to “friends only,” but only for new users. During all these manipulations, users’ expectations of privacy did not change merely because Facebook altered its default settings without first getting its users’ consent.

13. Facebook’s misconduct has inflicted serious tangible and intangible harms on Plaintiffs. The degree of harm they suffered bears a direct relation to the quantity and quality of the information

---

<sup>4</sup> A “Friend” is a connection between users on Facebook. To add a user as a Friend on Facebook, one user sends an invitation to another. Once a user accepts an invitation and becomes a Friend, that Friend can see content that the inviting user shares with that Friend.

<sup>5</sup> *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises*, Federal Trade Commission (Nov. 29, 2011), <https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep>.

<sup>6</sup> Decision and Order (“FTC Consent Decree” or “Consent Decree”), *In the Matter of Facebook, Inc.*, at 3-4, No. C-4365 (F.T.C. July 27, 2012).

Facebook gave to third parties. The content that users shared subject to privacy restrictions is incredibly intimate. Reasonably believing in Facebook's privacy controls, the representative plaintiffs all shared personally identifying information about relationships, whereabouts, moods, daily routines, videos, and photos with limited groups of Friends. The richness of the private information shared is what makes it so valuable to corporations and others who wish to personally target them.

14. Users are harmed not just by Facebook's disclosure of their private content and information to third parties. It is the way that Facebook collects, analyzes, and uses that information that inflicts a novel and more invasive kind of harm than just a breach of "data." Facebook's aggregation of user information allows de-anonymization of that information so that it can be connected to specific users, by name—contrary to Facebook's explicit pledge not to give content and information to advertisers.

15. The fundamental pieces of a Facebook profile—names, profile pictures, phone numbers, email addresses, and the kind of corroborating personal information used for passwords and security questions—serve as critical starter kits for identity theft and other malicious online activity. Experts agree that this aggregated information makes people much more vulnerable to voter fraud, medical fraud, phishing, and other identity-based harms. The disclosure of such content "allow[s] bad actors to tie raw data to people's real identities and build fuller profiles of them." Two plaintiffs have now found their information for sale on the dark web. Others have suffered phishing and other breach attempts.

16. The harm is not only limited to identity theft. The ability to analyze and de-anonymize user data allows third parties to personally and psychologically target Facebook users with greater precision. This is called "psychographic marketing." For example, Cambridge Analytica exploited users' information to target individual voters with content tailored to their predicted psychological proclivities. Facebook and other data brokers compile dossiers on Facebook users based on this aggregated content. The dossiers make assumptions about users' health, financial risk, employability, and other factors. Brokers, like Facebook, then make that information accessible to third parties to target people based on analyses of their temperament and vulnerabilities. The transparency, however, is one way.

17. Even before the revelations that led to this action, Facebook was no stranger to scandal—

perhaps not surprising given its Class Period mantra, “move fast and break things.” The Company has bounced from one scandal to another over the years, typically involving its troubled relationship with user privacy. Facebook weathered these scandals by expressly assuring its users and the public repeatedly that user privacy is central to its operation, and that whatever mistakes were made in Facebook’s zeal to “improve the user experience” would not be made again.

18. Facebook has repeatedly professed remorse for violating users’ privacy over the past seven years. Following entry of the 2011 Consent Decree, Chief Executive Officer Mark Zuckerberg stated, “we’ve made a bunch of mistakes.”<sup>7</sup> But he assured users of the Company’s commitment to providing its users with “complete control over who they share with at all times.”<sup>8</sup> For Facebook, Zuckerberg wrote, “this means we’re making a clear and formal long-term commitment to do the things we’ve always tried to do and planned to keep doing — giving you tools to control who can see your information and then making sure only those people you intend can see it.”<sup>9</sup>

19. Since the Cambridge Analytica scandal, Mr. Zuckerberg has continued to apologize. For example, on April 18, 2018, Zuckerberg admitted, “We didn’t focus enough on preventing abuse and thinking through how people could use these tools to do harm as well. That goes for fake news, foreign interference in elections, hate speech, in addition to developers and data privacy. We didn’t take a broad enough view of what our responsibility is, and that was a huge mistake. It was my mistake.”<sup>10</sup>

20. The time for pro forma apologies has long since passed. Only the legal process can put Plaintiffs back in the position they would occupy had Facebook properly disclosed its activities or not engaged in them at all. That is the relief they ask for, and are entitled to, under the law.

## II. JURISDICTION, VENUE, AND CHOICE OF LAW

21. Pursuant to 28 U.S.C. § 1331, this Court has original subject matter jurisdiction over the

---

<sup>7</sup> Mark Zuckerberg, *Our Commitment to the Facebook Community*, Facebook Newsroom (Nov. 29, 2011), <https://newsroom.fb.com/news/2011/11/our-commitment-to-the-facebook-community/>.

<sup>8</sup> *Id.*

<sup>9</sup> *Id.*

<sup>10</sup> *Hard Questions: Q&A With Mark Zuckerberg on Protecting People’s Information*, Facebook Newsroom (Apr. 4, 2018), <https://newsroom.fb.com/news/2018/04/hard-questions-protecting-peoples-information/>.

claims that arise under the Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.* and the Video Privacy Protection Act, 18 U.S.C. § 2710.

22. This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

23. In addition to federal question jurisdiction, this Court also has diversity jurisdiction pursuant to 28 U.S.C. § 1332(d) under the Class Action Fairness Act (“CAFA”), because the amount in controversy exceeds \$5,000,000, exclusive of interest and costs, and at least one Class Member is a citizen of a state different from Defendants.

24. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendants do business in and are subject to personal jurisdiction in this District. Venue is also proper because a substantial part of the events or omissions giving rise to the claim occurred in or emanated from this District.

25. The relevant terms of Plaintiffs’ contracts with Facebook provide that the exclusive venues for litigating any claim with Facebook are either the United States District Court for the Northern District of California or a state court located in San Mateo County. These contracts also provided that all claims that might arise between the user and Facebook would be governed by the laws of California, without regard to conflict-of-law provisions.

26. The venue provision provides an additional reason that venue is proper in this District. The choice-of-law provision establishes that California law applies to Plaintiffs’ claims.

### III. PARTIES

#### A. Plaintiffs

27. **Plaintiff Steven Akins** is a citizen and resident of the State of Tennessee. Plaintiff Akins created his Facebook account in 2008 via a personal computer and maintains his Facebook account to the present day. Plaintiff Akins has accessed his Facebook account from mobile phones and personal computers. Plaintiff Akins also uses Facebook Messenger and/or Facebook Chat. On or through Facebook, Facebook Messenger, and/or Facebook Chat, Plaintiff Akins has watched videos, “liked”

videos, “shared” videos, “posted” videos, “liked” pages on Facebook that contain videos, and “shared” pages on Facebook that contain videos. These videos were hosted on Facebook’s video streaming services, and included videos that were not posted by Plaintiff Akins or his Friends, videos that were selected and published by Facebook to Plaintiff Akins’s News Feed, and videos that were posted, shared, or liked to a non-public audience such as Friends.

28. Plaintiff Akins does not recall specific details regarding the account registration process. Plaintiff Akins does not recall being prompted to read or reading the Terms of Service or the Data Policy during the registration process. He does not recall seeing updates to the Terms of Service or the Data Policy since registering for his account. He did not subscribe to, has never visited, and is not aware of the Facebook Site Governance page.

29. On information and belief, Plaintiff Akins’ Privacy Settings for personal information, including birthday, were set to the default setting of Friends of Friends when he created his account. Plaintiff Akins later changed those settings to Friends in approximately 2010. On information and belief, Plaintiff Akins’ Privacy Settings for posts, including status updates, photos, and videos, were set to the default setting of Friends of Friends when he created his account. On information and belief, Plaintiff Akins did not change those settings, but started customizing his privacy on a post-by-post, photo-by-photo, video-by-video basis. On information and belief, Plaintiff Akins’ Privacy Settings for Likes, including page likes, interests, and favorites, were set to the default setting of Friends of Friends at first. Plaintiff Akins later changed those settings to Friends in approximately 2010. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Akins did not know that Facebook allowed advertisers to target him directly, using information such as his email address or Facebook User ID. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Akins did not know that there were separate Privacy Settings to limit the information obtained by Apps used by his Friends. Until 2018, post-Cambridge Analytica



Scandal, Plaintiff Akins did not know that there were separate Privacy Settings to disable advertisements targeting him on the basis of data from third parties such as data brokers.

30. Plaintiff Akins shared private content and information, including personal information, posts, and Likes, with a non-public audience such as Friends on Facebook. Plaintiff Akins expected Facebook to protect and secure that private content and information against access by or disclosure to unauthorized parties. This information included personal family photographs, personal family videos, as well as personal perspectives regarding politics, religion, relationships, work, and family that he wanted to remain private and non-public. Plaintiff Akins also shared private content and information with Friends through Facebook Messenger and/or Facebook Chat. This information included personal family photographs, personal family videos, as well as personal perspectives regarding politics, religion, relationships, work, and family that he wanted to remain private and non-public.

31. Plaintiff Akins believed that when he shared private content and information with a non-public audience such as Friends, by either restricting access to a non-public audience at the time of posting or through his Privacy Settings, he was preventing third parties from accessing his content and information. Plaintiff Akins was not aware of and did not understand that, when he shared content and information with a non-public audience such as Friends, Facebook would disclose such content and information to: (a) Apps used by his Friends; (b) “Business Partners” such as Apple, Amazon, and Samsung; and (c) advertisers. Plaintiff Akins was not aware of and did not understand that Facebook maintained a separate set of Privacy Settings for limiting the disclosure of his content and information to Apps used by his Facebook Friends. Plaintiff Akins was not aware of and did not understand that he could not control, with any settings made available by Facebook, the disclosure of his content and information with Business Partners such as Apple, Amazon, and Samsung. Further, Plaintiff Akins was not aware of and did not understand that Facebook would allow third parties to obtain his content and



information and use it to construct a psychographic profile of him for the purpose of attempting to manipulate his voting decisions or other decisions. Plaintiff Akins similarly was not aware of and did not understand that Facebook would allow third parties to access his content and information and combine it with content and information from other sources, including sources outside of Facebook, to create a unique profile of him (as distinct from the individualized profile that he created for his Facebook account).

32. If Plaintiff Akins had learned what he knows now about Facebook's data sharing policies before signing up for Facebook, he would not have signed up for Facebook at all. If, after signing up for Facebook, he learned what he knows now, he would have immediately restricted his profile Privacy Settings, limited sharing with Apps used by his Friends, and would have disabled Platform Apps entirely. He also would have altered and reduced his Facebook usage, including being more circumspect regarding sharing personal information.

33. On information and belief, Plaintiff Akins asserts his content and information was disclosed without his consent to the This Is Your Digital Life App or other third-party Apps Facebook is investigating for misusing users' content and information. Plaintiff Akins was not aware of and did not consent to the sharing of his content and information with the This Is Your Digital Life App or other third parties. Moreover, Plaintiff Akins did not consent to any third-parties accessing his content and information through his Facebook Friends and had no knowledge that Facebook had authorized this disclosure of his content and information without his consent.

34. During the 2016 U.S. Presidential election, Plaintiff Akins frequently received political advertisements while using Facebook. On information and belief, Plaintiff Akins was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of his content and information, Plaintiff Akins has experienced an increase in phone solicitations as well

as unauthorized access to his bank account. Additionally, as a result of the release of his content and information, Plaintiff Akins has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using his content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Akins's private affairs and concerns, as detailed herein. Plaintiff Akins fears that he is at risk of identity theft and fraud, and now spends approximately two hours each month monitoring his credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

35. **Plaintiff Rafael Amezcua** is a citizen and resident of California in the United States. Plaintiff Amezcua created his Facebook account in August 2009 via a personal computer and maintains his Facebook account to the present day. In August 2009, Plaintiff Amezcua was a minor. Plaintiff Amezcua has accessed his Facebook account from a mobile phone and a personal computer. Plaintiff Amezcua also uses Facebook Messenger and/or instant messaging through Facebook. On or through Facebook, Facebook Messenger, and/or Facebook instant messaging, Plaintiff Amezcua has watched videos, "liked" videos, "shared" videos, "posted" videos, "liked" pages on Facebook that contain videos, and "shared" pages on Facebook that contain videos.

36. Plaintiff Amezcua does not recall specific details regarding the account registration process. Plaintiff Amezcua does not recall being prompted to read the Terms of Service or the Data Policy during the registration process. He does not recall seeing updates to the Terms of Service or the Data Policy since registering for his account. He did not subscribe to, has never visited, and is not aware of the Facebook Site Governance page.

37. On information and belief, Plaintiff Amezcua's Privacy Settings for personal information, including birthday, were set to the default setting of Friends when he created his account. On information and belief, Plaintiff Amezcua's Privacy Settings for posts, including status updates, photos, and videos, were set to the default setting of Friends when he created his account. On information and belief, Plaintiff Amezcua's Privacy Settings for Likes, including page likes, interests, and favorites,

were set to the default setting of Friends when he created his account. Plaintiff Amezcua has since changed these Like settings to Only Me in approximately 2014. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Amezcua did not know that Facebook allowed advertisers to target him directly, using information such as his email address or Facebook ID. Since learning of the Cambridge Analytica Scandal, Plaintiff Amezcua has changed the Privacy Settings for certain photos and photo albums to specific Friends and to Only Me.

38. Plaintiff Amezcua shared private content and information, including personal information, posts, and Likes, with a non-public audience such as Friends Only on Facebook or through Facebook Messenger and/or Facebook instant messaging. Plaintiff Amezcua expected Facebook to protect and secure that private content and information against access by or disclosure to unauthorized parties. This information included personal photographs, personal videos, as well as personal perspectives regarding politics, relationships, and family that he wanted to remain private and non-public. Plaintiff Amezcua also shared private content and information with Friends through Facebook Messenger and/or Facebook instant messaging. This information included personal videos, messages, as well as personal perspectives regarding politics, relationships, and family that he wanted to remain private and non-public.

39. Plaintiff Amezcua believed that when he shared private content and information with a non-public audience such as Friends Only, by either restricting access to a non-public audience at the time of posting or through his Privacy Settings, he was preventing third parties from accessing his content and information. Plaintiff Amezcua was not aware of and did not understand that Facebook would disclose content and information when he shared content and information with a non-public audience such as Friends Only to: (a) Apps used by his Friends; (b) “Business Partners” such as Apple, Amazon, and Samsung; and (c) advertisers. Plaintiff Amezcua was not aware of and did not understand that Facebook maintained a separate set of Privacy Settings for limiting the disclosure of his content and information to Apps used by his Facebook Friends. Plaintiff Amezcua was not aware of and did not understand that he could not control, with any settings made available by Facebook, the disclosure of his content and information with Business Partners such as Apple, Amazon, and Samsung. Further,

Plaintiff Amezcua was not aware of and did not understand that Facebook would allow third parties to obtain his content and information and use it to construct a psychographic profile of him for the purpose of attempting to manipulate his voting decisions or other decisions. Plaintiff Amezcua similarly was not aware of and did not understand that Facebook would allow third parties to access his content and information and combine it with personally identifiable information from other sources, including sources outside of Facebook, to create a unique profile of him (as distinct from the individualized profile that he created for his Facebook account).

40. If Plaintiff Amezcua had learned what he knows now about Facebook's data sharing policies before signing up for Facebook, he believes that he would not have signed up for Facebook at all. If, after signing up for Facebook, he learned what he knows now, he would have immediately restricted his profile privacy settings, limited sharing with Apps used by his Friends, and would have disabled Platform Apps entirely. Plaintiff Amezcua also would have reduced his Facebook usage, including being more circumspect regarding sharing personal information.

41. On information and belief, Plaintiff Amezcua believes that his content and information may have been "shared" with and "misused" by the This Is Your Digital Life app, because one of Plaintiff Amezcua's Facebook Friends downloaded the This Is Your Digital Life app. Plaintiff Amezcua did not consent to the sharing of his content and information with the This Is Your Digital Life app.

42. During the 2016 U.S. Presidential election, Plaintiff Amezcua frequently received political advertisements while using Facebook. On information and belief, Plaintiff Amezcua was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal.

43. As a result of the release of his content and information, Plaintiff Amezcua has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using his content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Amezcua's private affairs and concerns, as detailed herein. Plaintiff Amezcua fears that he is at risk of identity theft and fraud, and now spends approximately thirty minutes each month monitoring his credit, bank, and other account statements for evidence of identity

theft and fraud, and anticipates continuing to do so for the foreseeable future.

44. **Plaintiff Jason Ariciu** is a citizen and resident of the State of Missouri. Plaintiff Ariciu created his Facebook account in 2005 via a personal computer and maintains his Facebook account to the present day. Plaintiff Ariciu has accessed his Facebook account from a personal computer, a tablet, and a mobile phone. Plaintiff Ariciu also uses Facebook Messenger and/or Facebook Chat. On or through Facebook, Facebook Messenger, and/or Facebook Chat, Plaintiff Ariciu has watched videos, “liked” videos, “shared” videos, “posted” videos, “liked” pages on Facebook that contain videos, and “shared” pages on Facebook that contain videos. These videos were hosted on Facebook’s video streaming services, and included videos that were not posted by Plaintiff Ariciu or his Friends, videos that were selected and published by Facebook to Plaintiff Ariciu’s News Feed, and videos that were posted, shared, or liked to a non-public audience such as Friends. Plaintiff Ariciu has enabled location access while using Facebook, Facebook Messenger, and/or Facebook Chat.

45. Plaintiff Ariciu does not recall specific details regarding the account registration process. Plaintiff Ariciu does not recall being prompted to read or reading the Terms of Service or the Data Policy during the registration process. He does not recall seeing updates to the Terms of Service or the Data Policy since registering for his account. He did not subscribe to, has never visited, and is not aware of the Facebook Site Governance page.

46. On information and belief, Plaintiff Ariciu’s Privacy Settings for personal information, including birthday, were set to the default setting of Friends when he created his account. On information and belief, Plaintiff Ariciu’s Privacy Settings for posts, including status updates, photos, and videos, were set to the default setting of Friends of Friends when he created his account. Plaintiff Ariciu later changed those settings to Friends in approximately 2009. On information and belief, Plaintiff Ariciu’s Privacy Settings for Likes, including page likes, interests, and favorites, were set to the default setting of Friends of Friends at first. Plaintiff Ariciu later changed those settings to Friends in

approximately 2009. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Ariciu did not know that Facebook allowed advertisers to target him directly, using information such as his email address or Facebook User ID. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Ariciu did not know that there were separate Privacy Settings to limit the information obtained by Apps used by his Friends. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Ariciu did not know he could disable advertisements targeting him on the basis of data from third parties such as data brokers.

47. Plaintiff Ariciu shared private content and information, including personal information, posts, and Likes, with a non-public audience such as Friends on Facebook. Plaintiff Ariciu expected Facebook to protect and secure that private content and information against access by or disclosure to unauthorized parties. This information included personal family photographs, personal family videos, as well as personal perspectives regarding politics, religion, relationships, work, and family that he wanted to remain private and non-public. Plaintiff Ariciu also shared private content and information with Friends through Facebook Messenger and/or Facebook Chat. This information included personal family photographs as well as personal perspectives regarding politics, religion, relationships, work, and family that he wanted to remain private and non-public.

48. Plaintiff Ariciu believed that when he shared private content and information with a non-public audience such as Friends, by either restricting access to a non-public audience at the time of posting or through his Privacy Settings, he was preventing third parties from accessing his content and information. Plaintiff Ariciu was not aware of and did not understand that when he shared content and information with a non-public audience such as Friends, Facebook would disclose such content and information to: (a) Apps used by his Friends; (b) “Business Partners” such as Apple, Amazon, and Samsung; and (c) advertisers. Plaintiff Ariciu was not aware of and did not understand that Facebook maintained a separate set of Privacy Settings for limiting the disclosure of his content and information to

Apps used by his Facebook Friends. Plaintiff Ariciu was not aware of and did not understand that he could not control, with any settings made available by Facebook, the disclosure of his content and information with Business Partners such as Apple, Amazon, and Samsung. Further, Plaintiff Ariciu was not aware of and did not understand that Facebook would allow third parties to obtain his content and information and use it to construct a psychographic profile of him for the purpose of attempting to manipulate his voting decisions or other decisions. Plaintiff Ariciu similarly was not aware of and did not understand that Facebook would allow third parties to access his content and information and combine it with personally identifiable information from other sources, including sources outside of Facebook, to create a unique profile of him (as distinct from the individualized profile that he created for his Facebook account).

49. If Plaintiff Ariciu had learned what he knows now about Facebook's data sharing policies after signing up for Facebook, he would have immediately restricted his profile Privacy Settings, limited sharing with Apps used by his Friends, and would have disabled Platform Apps entirely. He also would have altered and reduced his Facebook usage, including being more circumspect regarding sharing personal and professional information.

50. Plaintiff Ariciu confirmed on Facebook that his content and information may have been "shared" with and "misused" by the This Is Your Digital Life App, because one of Plaintiff Ariciu's Facebook Friends downloaded the This Is Your Digital Life App. Plaintiff Ariciu did not consent to the sharing of his content and information with the This Is Your Digital Life App. Moreover, Plaintiff Ariciu did not consent to any third-parties accessing his content and information through his Facebook Friends and had no knowledge that Facebook had authorized this disclosure of his content and information without his consent.

51. During the 2016 U.S. Presidential election, Plaintiff Ariciu frequently received political advertisements while using Facebook. On information and belief, Plaintiff Ariciu was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of his content and information, Plaintiff Ariciu has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using his content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Ariciu's private affairs and concerns, as detailed herein. Plaintiff Ariciu fears that he is at risk of identity theft and fraud, and now spends approximately one to two hours each month monitoring his credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

52. **Plaintiff Samuel Armstrong** is a citizen and resident of the State of Indiana. Plaintiff Armstrong created his Facebook account in 2007 via a personal computer and maintains his Facebook account to the present day. Plaintiff Armstrong has accessed his Facebook account from a personal computer, a tablet, and a mobile phone. Plaintiff Armstrong also uses Facebook Messenger and/or Facebook Chat. On or through Facebook, Facebook Messenger, and/or Facebook Chat, Plaintiff Armstrong has watched videos, "liked" videos, "shared" videos, "posted" videos, "liked" pages on Facebook that contain videos, and "shared" pages on Facebook that contain videos. These videos were hosted on Facebook's video streaming services, and included videos that were not posted by Plaintiff Armstrong or his Friends, videos that were selected and published by Facebook to Plaintiff Armstrong's News Feed, and videos that were posted, shared, or liked to a non-public audience such as Friends.

53. Plaintiff Armstrong recalls that during the account registration process he had to provide his first name, last name, birthday, and email address. Plaintiff Armstrong does not recall being



prompted to read or reading the Terms of Service or the Data Policy during the registration process. He did not subscribe to, has never visited, and is not aware of the Facebook Site Governance page.

54. On information and belief, Plaintiff Armstrong's Privacy Settings for personal information, including birthday, were set to the default setting of Friends of Friends when he created his account. On information and belief, Plaintiff Armstrong's Privacy Settings for posts, including status updates, photos, and videos, were set to the default setting of Friends of Friends when he created his account. Plaintiff Armstrong later changed those settings to Friends in approximately 2012. On information and belief, Plaintiff Armstrong's Privacy Settings for Likes, including page likes, interests, and favorites, were set to the default setting of Friends of Friends at first. Plaintiff Armstrong later changed those settings to Friends in approximately 2012. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Armstrong did not know that Facebook allowed advertisers to target him directly, using information such as his email address or Facebook User ID. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Armstrong did not know that there were separate Privacy Settings to limit the information obtained by Apps used by his Friends. On information and belief, Plaintiff Armstrong disabled advertisements targeting him on the basis of data from third parties such as data brokers.

55. Plaintiff Armstrong shared private content and information, including personal information, posts, and Likes, with a non-public audience such as Friends on Facebook. Plaintiff Armstrong expected Facebook to protect and secure that private content and information against access by or disclosure to unauthorized parties. This information included personal family photographs, personal family videos, as well as personal perspectives regarding politics, religion, relationships, work, family, and health that he wanted to remain private and non-public. Plaintiff Armstrong also shared private content and information with Friends through Facebook Messenger and/or Facebook Chat. This information included personal family photographs, personal family videos, as well as personal

perspectives regarding politics, religion, relationships, work, and family that he wanted to remain private and non-public.

56. Plaintiff Armstrong believed that when he shared private content and information with a non-public audience such as Friends, by either restricting access to a non-public audience at the time of posting or through his Privacy Settings, he was preventing third parties from accessing his content and information. Plaintiff Armstrong was not aware of and did not understand that, when he shared content and information with a non-public audience such as Friends, Facebook would disclose such content and information to: (a) Apps used by his Friends; (b) “Business Partners” such as Apple, Amazon, and Samsung; and (c) advertisers. Plaintiff Armstrong was not aware of and did not understand that Facebook maintained a separate set of Privacy Settings for limiting the disclosure of his content and information to Apps used by his Facebook Friends. Plaintiff Armstrong was not aware of and did not understand that he could not control, with any settings made available by Facebook, the disclosure of his content and information with Business Partners such as Apple, Amazon, and Samsung. Further, Plaintiff Armstrong was not aware of and did not understand that Facebook would allow third parties to obtain his content and information and use it to construct a psychographic profile of him for the purpose of attempting to manipulate his voting decisions or other decisions. Plaintiff Armstrong similarly was not aware of and did not understand that Facebook would allow third parties to access his content and information and combine it with personally identifiable information from other sources, including sources outside of Facebook, to create a unique profile of him (as distinct from the individualized profile that he created for his Facebook account).

57. If Plaintiff Armstrong had learned what he knows now about Facebook’s data sharing policies before signing up for Facebook, particularly with respect to its influence on his voting decisions, he would not have signed up for Facebook at all. If, after signing up for Facebook, he learned

what he knows now, he would have immediately restricted his profile Privacy Settings, limited sharing with Apps used by his Friends, and would have reduced his Facebook usage regarding political subjects.

58. Plaintiff Armstrong confirmed on Facebook that his content and information may have been “shared” with and “misused” by the This Is Your Digital Life App, because one of Plaintiff Armstrong’s Facebook Friends downloaded the This Is Your Digital Life App. Plaintiff Armstrong did not consent to the sharing of his content and information with the This Is Your Digital Life App. Moreover, Plaintiff Armstrong did not consent to any third-parties accessing his content and information through his Facebook Friends and had no knowledge that Facebook had authorized this disclosure of his content and information without his consent.

59. During the 2016 U.S. Presidential election, Plaintiff Armstrong frequently received political advertisements while using Facebook. On information and belief, Plaintiff Armstrong was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. In particular, Plaintiff Armstrong recalls that he received highly offensive advertisements during the 2016 U.S. Presidential election, and believes that he was targeted with such advertisements because of his race and gender. He believes that these advertisements were designed to improperly influence his voting decisions, and recalls that these advertisements did in fact influence his voting decisions. As a result of the release of his content and information, Plaintiff Armstrong has experienced an increase in phone solicitations. Additionally, as a result of the release of his content and information, Plaintiff Armstrong has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using his content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Armstrong’s private affairs and concerns, as detailed herein. Plaintiff Armstrong fears that he is at risk of identity theft and fraud, and now spends approximately four

hours each month monitoring his credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

60. **Plaintiff Anthony Bell** is a citizen and resident of the State of California. Plaintiff Bell created his Facebook account in approximately 2005 via a computer and maintains his Facebook account to the present day. Plaintiff Bell has accessed his Facebook account from a computer and mobile phone. Plaintiff Bell also uses Facebook Messenger and/or Facebook Chat. On or through Facebook, Facebook Messenger, and/or Facebook Chat, Plaintiff Bell has obtained and viewed non-public videos, “liked” videos, “shared” videos, “posted” videos, “liked” pages on Facebook that contain videos, and “shared” pages on Facebook that contain videos.” These videos were delivered by Facebook, and included videos that were not posted by Plaintiff Bell or his Friends, videos that were selected and delivered by Facebook to Plaintiff Bell’s News Feed, and videos that were posted, shared, or liked to a non-public audience such as Friends. Plaintiff Bell is a pastor and Facebook has allowed him to post inspirational and religious videos for his parishioners. In addition, through Facebook Live, the service that allows users to broadcast live video streams to the News Feed using the Facebook Mentions App, Plaintiff Bell has broadcast inspirational and religious messages to parishioners. He believes the Facebook Live video was shared publicly when it was live, but after it ended and was posted to his page, he changed the video’s Privacy Settings to non-public (either Only Me or Friends). Via Facebook Chat and Messenger, Plaintiff Bell has also sent his church employees videos containing very sensitive business information that needed to remain private.

61. Plaintiff Bell does not recall specific details regarding the account registration process. Plaintiff Bell recalls reading parts of the Terms of Service and the Data Policy during the registration process. Plaintiff Bell recalls that the Terms of Service and the Data Policy were extremely long and complex and that he did not understand the terms. He does not recall seeing updates to the Terms of

Service or the Data Policy since registering for his account. He does not subscribe to, has never visited, and is not aware of the Facebook Site Governance page.

62. On information and belief, Plaintiff Bell's Privacy Settings for personal information, including birthday, were set to the default setting of Friends when he created his account. Plaintiff Bell later changed those settings to Friends. On information and belief, Plaintiff Bell's Privacy Settings for posts, including status updates, photos, and videos, were set to the default setting of Friends of Friends when he created his account. On information and belief, Plaintiff Bell's Privacy Settings for Likes, including page likes, interests, and favorites, were set to the default setting of Friends of Friends at first. Plaintiff Bell later changed all of those settings to Friends. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Bell did not know that Facebook allowed advertisers to target him directly, using information such as his email address or Facebook User ID. On information and belief, Plaintiff Bell disabled advertisements targeted on the basis of data from third parties such as data brokers. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Bell did not know that there were separate Privacy Settings to limit the information obtained by Apps used by his Friends. Plaintiff Bell later became aware of those settings and changed those settings to limit information sharing in approximately 2018.

63. Plaintiff Bell shared private content and information on Facebook, including personal information, posts, and Likes, with a non-public audience such as Friends and in private Facebook Groups. Plaintiff Bell expected Facebook to protect and secure that private content and information against access by or disclosure to unauthorized parties. This information included personal family photographs, personal family videos, as well as personal perspectives regarding politics, religion, relationships, work, and family that he wanted to remain private and non-public. For example, he often uses Facebook in the course of his work as a pastor to invite people to events—using Facebook's Events function—at his church. He also "Friends" his parishioners on Facebook so that they can communicate

with him easily, such as by posting on his page, and so that he could offer encouragement and support to parishioners. He expected those communications and related content and information to remain private and confidential.

64. Plaintiff Bell also shared private content and information with Friends through Facebook Messenger and/or Facebook Chat. This information included personal family photographs, personal family videos, as well as personal perspectives regarding politics, religion, relationships, work, and family that he wanted to remain private and non-public. Plaintiff Bell expected Facebook to protect and secure that private content and information against access by or disclosure to unauthorized parties. As one example, in trying to solve a family emergency that was endangering the safety and lives of some of his relatives, Plaintiff Bell shared highly sensitive information to his Facebook page and via Facebook Messenger that he believed would not be shared with people who were not his Friends. If that information had reached people other than his Friends, his relatives' lives would have been endangered. Facebook was his only option for communicating during this emergency due to poor phone service overseas. As another example, Plaintiff Bell, in the course of his work as a pastor, often counsels his parishioners through Facebook Messenger. As a pastor, he has an obligation to keep confidential information his parishioners share with him. He believes that Facebook's failure to keep his messages confidential have violated his duty of confidentiality as a pastor.

65. Plaintiff Bell believed that when he shared private content and information with a non-public audience such as Friends, by either restricting access to a non-public audience at the time of posting or through his Privacy Settings, he was preventing third parties from accessing his content and information. Plaintiff Bell was not aware of and did not understand that when he shared content and information with a non-public audience such as Friends, Facebook would disclose such content and information to: (a) Apps used by his Friends; (b) "Business Partners" such as Apple, Amazon, and

Samsung; and (c) advertisers. Plaintiff Bell was not aware of and did not understand that Facebook maintained a separate set of Privacy Settings for limiting the disclosure of his content and information to Apps used by his Facebook Friends. Plaintiff Bell was not aware of and did not understand that he could not control, with any settings made available by Facebook, the disclosure of his content and information with Business Partners such as Apple, Amazon, and Samsung. Further, Plaintiff Bell was not aware of and did not understand that Facebook would allow third parties to obtain his content and information and use it to construct a psychographic profile of him for the purpose of attempting to manipulate his voting decisions or other decisions. Plaintiff Bell similarly was not aware of and did not understand that Facebook would allow third parties to access his content and information and combine it with personally identifiable information from other sources, including sources outside of Facebook, to create a unique profile of him (as distinct from the individualized profile that he created for his Facebook account).

66. If Plaintiff Bell had learned what he knows now about Facebook's data sharing policies before signing up for Facebook, he would not have signed up for Facebook at all. If, after signing up for Facebook, he learned what he knows now, he would have immediately restricted his profile Privacy Settings, limited sharing with Apps used by his Friends, and would have disabled Platform Apps entirely. He also would have altered and reduced his Facebook usage, including being more circumspect regarding sharing personal information.

67. Plaintiff Bell confirmed on Facebook that his content and information may have been "shared" with and "misused" by the This Is Your Digital Life App, because one of Plaintiff Bell's Facebook Friends downloaded the This Is Your Digital Life App. Plaintiff Bell did not consent to the sharing of his content and information with the This Is Your Digital Life App. Moreover, Plaintiff Bell did not consent to any third-parties accessing his content and information through his Facebook Friends

and had no knowledge that Facebook had authorized this disclosure of his content and information without his consent.

68. During the 2016 U.S. Presidential election, Plaintiff Bell frequently received political advertisements while using Facebook. On information and belief, Plaintiff Bell was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of his content and information, Plaintiff Bell has experienced hacking of his email account and attempted unauthorized withdrawals from his bank account. Plaintiff Bell had to delete his email account and subsequently lost a large amount of information. Additionally, as a result of the release of his content and information, Plaintiff Bell has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using his content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Bell's private affairs and concerns, as detailed herein. Plaintiff Bell fears that he is at risk of identity theft and fraud, and now spends approximately five hours each month monitoring his credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future. Because of his heightened risk of identity theft and fraud, Plaintiff Bell has purchased credit monitoring and identity theft protection services, and anticipates continuing to pay for such services for the foreseeable future.

69. **Plaintiff Bridgett Burk** is a citizen and resident of the State of Florida. Plaintiff Burk created her Facebook account in 2006 via a personal computer and maintains her Facebook account to the present day. Plaintiff Burk has accessed her Facebook account from a mobile phone, a tablet, and a personal computer. Plaintiff Burk also uses Facebook Messenger and/or Facebook Chat. On or through Facebook, Facebook Messenger, and/or Facebook Chat, Plaintiff Burk has watched videos, "liked" videos, "shared" videos, "posted" videos, "liked" pages on Facebook that contain videos, and "shared"



pages on Facebook that contain videos. These videos were hosted on Facebook's video streaming services, and included videos that were not posted by Plaintiff Burk or her Friends, videos that were selected and published by Facebook to Plaintiff Burk's News Feed, and videos that were posted, shared, or liked to a non-public audience such as Friends. Plaintiff Burk has also purchased and/or sold items in the Facebook Marketplace.

70. Plaintiff Burk does not recall specific details regarding the account registration process. Plaintiff Burk does not recall being prompted to read or reading the Terms of Service or the Data Policy during the registration process. She does not recall seeing updates to the Terms of Service or the Data Policy since registering for her account. She did not subscribe to, has never visited, and is not aware of the Facebook Site Governance page.

71. On information and belief, Plaintiff Burk's Privacy Settings for personal information, including birthday, were set to the default setting of Friends when she created her account. Plaintiff Burk later confirmed that those settings were set to Friends in approximately 2009 or 2010. On information and belief, Plaintiff Burk's Privacy Settings for posts, including status updates, photos, and videos, were set to the default setting of Friends of Friends when she created her account. Plaintiff Burk later changed those settings to Friends in approximately 2009 or 2010. On information and belief, Plaintiff Burk's Privacy Settings for Likes, including page likes, interests, and favorites, were set to the default setting of Friends of Friends at first. Plaintiff Burk later changed those settings to Friends in approximately 2009 or 2010. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Burk did not know that Facebook allowed advertisers to target her directly, using information such as her email address or Facebook User ID. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Burk did not know that there were separate Privacy Settings to limit the information obtained by Apps used by her Friends. On information and

belief, Plaintiff Burk disabled advertisements targeting her on the basis of data from third parties such as data brokers.

72. Plaintiff Burk shared private content and information, including personal information, posts, and Likes, with a non-public audience such as Friends on Facebook. Plaintiff Burk expected Facebook to protect and secure that private content and information against access by or disclosure to unauthorized parties. This information included personal family photographs, personal family videos, as well as personal perspectives regarding politics, religion, relationships, work, and family that she wanted to remain private and non-public. Plaintiff Burk also shared private content and information with Friends through Facebook Messenger and/or Facebook Chat. This information included personal family photographs, as well as personal perspectives regarding politics, religion, relationships, work, and family that she wanted to remain private and non-public.

73. Plaintiff Burk believed that when she shared private content and information with a non-public audience such as Friends, by either restricting access to a non-public audience at the time of posting or through her Privacy Settings, she was preventing third parties from accessing her content and information. Plaintiff Burk was not aware of and did not understand that, when she shared content and information with a non-public audience such as Friends, Facebook would disclose such content and information to: (a) Apps used by her Friends; (b) “Business Partners” such as Apple, Amazon, and Samsung; and (c) advertisers. Plaintiff Burk was not aware of and did not understand that Facebook maintained a separate set of Privacy Settings for limiting the disclosure of her content and information to Apps used by her Facebook Friends. Plaintiff Burk was not aware of and did not understand that she could not control, with any settings made available by Facebook, the disclosure of her content and information with Business Partners such as Apple, Amazon, and Samsung. Further, Plaintiff Burk was not aware of and did not understand that Facebook would allow third parties to obtain her content and

information and use it to construct a psychographic profile of her for the purpose of attempting to manipulate her voting decisions or other decisions. Plaintiff Burk similarly was not aware of and did not understand that Facebook would allow third parties to access her content and information and combine it with personally identifiable information from other sources, including sources outside of Facebook, to create a unique profile of her (as distinct from the individualized profile that she created for her Facebook account).

74. If Plaintiff Burk had learned what she knows now about Facebook's data sharing policies before signing up for Facebook, she would not have signed up for Facebook at all. If, after signing up for Facebook, she learned what she knows now, she would have immediately restricted her profile Privacy Settings, limited sharing with Apps used by her Friends, and would have disabled Platform Apps entirely. She also would have altered and reduced her Facebook usage, including being more circumspect regarding sharing personal information.

75. Plaintiff Burk confirmed on Facebook that her content and information may have been "shared" with and "misused" by the This Is Your Digital Life App, because one of Plaintiff Burk's Facebook Friends downloaded the This Is Your Digital Life App. Plaintiff Burk was not aware of and did not consent to the sharing of her content and information with the This Is Your Digital Life App. Moreover, Plaintiff Burk did not consent to any third-parties accessing her content and information through her Facebook Friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

76. During the 2016 U.S. Presidential election, Plaintiff Burk frequently received political advertisements while using Facebook. On information and belief, Plaintiff Burk was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of her content and information, Plaintiff Burk has experienced an increase in phone solicitations.

Additionally, as a result of the release of her content and information, Plaintiff Burk has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Burk's private affairs and concerns, as detailed herein. Plaintiff Burk fears that she is at risk of identity theft and fraud, and now spends approximately thirty minutes each month monitoring her credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

77. **Plaintiff Naomi Butler** is a citizen and resident of Liverpool in the United Kingdom. Plaintiff Butler created her Facebook account in 2009 via a personal computer and maintains her Facebook account to the present day. Plaintiff Butler has accessed her Facebook account from a mobile phone and a personal computer. Plaintiff Butler also uses Facebook Messenger and/or instant messaging through Facebook. On or through Facebook, Facebook Messenger, and/or Facebook instant messaging, Plaintiff Butler has watched videos, "liked" videos, "shared" videos, "posted" videos, "liked" pages on Facebook that contain videos, and "shared" pages on Facebook that contain videos.

78. Plaintiff Butler does not recall specific details regarding the account registration process. Plaintiff Butler does not recall being prompted to read the Terms of Service or the Data Policy during the registration process. She does not recall seeing updates to the Terms of Service or the Data Policy since registering for her account. She did not subscribe to, has never visited, and is not aware of the Facebook Site Governance page.

79. On information and belief, Plaintiff Butler's Privacy Settings for personal information, including birthday, were set to the default setting when she created her account. Plaintiff Butler later changed those settings to Friends Only. On information and belief, Plaintiff Butler's Privacy Settings for posts, including status updates, photos, and videos, were set to the default setting when she created her account. On information and belief, Plaintiff Butler's Privacy Settings for Likes, including page likes, interests, and favorites, were set to the default setting when she created her account. Until 2018,

post-Cambridge Analytica Scandal and the enactment of the European Union’s General Data Protection Regulation (“GDPR”), Plaintiff Butler did not know that Facebook allowed advertisers to target her directly, using information such as her email address or Facebook ID. Until 2020, Plaintiff Butler did not know that there were separate Privacy Settings to limit the information that Apps used by Friends could obtain.

80. Plaintiff Butler shared private content and information, including personal information, posts, and Likes, with a non-public audience such as Friends Only on Facebook or through Facebook Messenger and/or Facebook instant messaging. Plaintiff Butler expected Facebook to protect and secure that private content and information against access by or disclosure to unauthorized parties. The information included personal family photographs, personal family videos, as well as personal perspectives regarding politics, religion, relationships, work, and family that she wanted to remain private and non-public. Plaintiff Butler also shared private content and information with Friends through Facebook Messenger and/or Facebook instant messaging. The information included personal perspectives regarding politics, religion, relationships, work and family that she wanted to remain private and non-public.

81. Plaintiff Butler believed that when she shared private content and information with a non-public audience such as Friends Only, by either restricting access to a non-public audience at the time of posting or through her Privacy Settings, she was preventing third parties from accessing her content and information. Plaintiff Butler was not aware of and did not understand that Facebook would disclose content and information when she shared content and information with a non-public audience such as Friends Only to: (a) Apps used by her Friends; (b) “Business Partners” such as Apple, Amazon, and Samsung; and (c) advertisers. Plaintiff Butler was not aware of and did not understand that Facebook maintained a separate set of Privacy Settings for limiting the disclosure of her content and information to Apps used by her Facebook Friends. Plaintiff Butler was not aware of and did not understand that she could not control, with any settings made available by Facebook, the disclosure of her content and information with Business Partners such as Apple, Amazon, and Samsung. Further, Plaintiff Butler was not aware of and did not understand that Facebook would allow third parties to obtain her content and

information and use it to construct a psychographic profile of her for the purpose of attempting to manipulate her voting decisions or other decisions. Plaintiff Butler similarly was not aware of and did not understand that Facebook would allow third parties to access her content and information and combine it with personally identifiable information from other sources, including sources outside of Facebook, to create a unique profile of her (as distinct from the individualized profile that she created for her Facebook account).

82. If Plaintiff Butler had learned what she knows now about Facebook's data sharing policies before signing up for Facebook, she believes that she would not have signed up for Facebook at all. If, after signing up for Facebook, she learned what she knows now, she would have immediately restricted her profile privacy settings, limited sharing with Apps used by her Friends, and would have disabled Platform Apps entirely. She also would have altered and reduced her Facebook usage, including being more circumspect regarding sharing personal information.

83. On information and belief, Plaintiff Butler believes that her content and information may have been "shared" with and "misused" by the This Is Your Digital Life app, because one of Plaintiff Butler's Facebook Friends downloaded the This Is Your Digital Life app. Plaintiff Butler did not consent to the sharing of her content and information with the This Is Your Digital Life app.

84. As a result of the release of her content and information, Plaintiff Butler has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Butler's private affairs and concerns, as detailed therein. Plaintiff Butler fears that she is at risk of identity theft and fraud, and now spends approximately one hour each month monitoring her credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

85. **Plaintiff Peter Christley** is a citizen and resident of Rhyl Denbighshire in the United Kingdom. Plaintiff Christley created his Facebook account in 2008 via a personal computer and maintains his Facebook account to the present day. Plaintiff Christley has accessed his Facebook account from a mobile phone and a personal computer. Plaintiff Christley also uses Facebook

Messenger and/or instant messaging through Facebook. On or through Facebook, Facebook Messenger, and/or Facebook instant messaging, Plaintiff Christley has watched videos, “liked” videos, “shared” videos, “posted” videos, “liked” pages on Facebook that contain videos, and “shared” pages on Facebook that contain videos. Plaintiff Christley has also purchased and/or sold items in the Facebook Marketplace.

86. Plaintiff Christley does not recall specific details regarding the account registration process. Plaintiff Christley does not recall being prompted to read the Terms of Service or the Data Policy during the registration process. He does not recall seeing updates to the Terms of Service or the Data Policy since registering for his account. He did not subscribe to, has never visited, and is not aware of the Facebook Site Governance page.

87. On information and belief, Plaintiff Christley’s Privacy Settings for personal information, including birthday, were set to the default setting of Friends when he created his account. Plaintiff Christley later changed those settings to Only Me in approximately 2020. On information and belief, Plaintiff Christley’s Privacy Settings for posts, including status updates, photos, and videos, were set to the default setting of Friends when he created his account. On information and belief, Plaintiff Christley’s Privacy Settings for Likes, including page likes, interests, and favorites, were set to the default setting of Friends when he created his account. Until 2018, post-Cambridge Analytica Scandal and the enactment of the European Union’s General Data Protection Regulation (“GDPR”), Plaintiff Christley did not know that Facebook allowed advertisers to target him directly, using information such as his email address or Facebook ID. Until 2020, Plaintiff Christley did not know that there were separate Privacy Settings to limit the information that Apps used by Friends could obtain.

88. Plaintiff Christley shared private content and information, including personal information, posts, and Likes, with a non-public audience such as Friends Only on Facebook or through Facebook Messenger and/or Facebook instant messaging. Plaintiff Christley expected Facebook to protect and secure that private content and information against access by or disclosure to unauthorized parties. This information included personal family photographs, personal family videos, as well as personal perspectives regarding politics, religion, relationships, work, and family that he wanted to

remain private and non-public. Plaintiff Christley also shared private content and information with Friends through Facebook Messenger and/or Facebook instant messaging. This information included personal family photographs, personal family videos, as well as personal perspectives regarding politics, religion, relationships, work and family that he wanted to remain private and non-public.

89. Plaintiff Christley believed that when he shared private content and information with a non-public audience such as Friends Only, by either restricting access to a non-public audience at the time of posting or through his Privacy Settings, he was preventing third parties from accessing his content and information. Plaintiff Christley was not aware of and did not understand that Facebook would disclose content and information when he shared content and information with a non-public audience such as Friends Only to: (a) Apps used by his Friends; (b) “Business Partners” such as Apple, Amazon, and Samsung; and (c) advertisers. Plaintiff Christley was not aware of and did not understand that Facebook maintained a separate set of Privacy Settings for limiting the disclosure of his content and information to Apps used by his Facebook Friends. Plaintiff Christley was not aware of and did not understand that he could not control, with any settings made available by Facebook, the disclosure of his content and information with Business Partners such as Apple, Amazon, and Samsung. Further, Plaintiff Christley was not aware of and did not understand that Facebook would allow third parties to obtain his content and information and use it to construct a psychographic profile of him for the purpose of attempting to manipulate his voting decisions or other decisions. Plaintiff Christley similarly was not aware of and did not understand that Facebook would allow third parties to access his content and information and combine it with personally identifiable information from other sources, including sources outside of Facebook, to create a unique profile of him (as distinct from the individualized profile that he created for his Facebook account).

90. If Plaintiff Christley had learned what he knows now about Facebook’s data sharing policies before signing up for Facebook, he believes that he would not have signed up for Facebook at all. If, after signing up for Facebook, he learned what he knows now, he would have immediately restricted his profile privacy settings, limited sharing with Apps used by his Friends, and would have disabled Platform Apps entirely. He also would have altered and reduced his Facebook usage, including



being more circumspect regarding sharing personal information.

91. On information and belief, Plaintiff Christley believes that his content and information may have been “shared” with and “misused” by the This Is Your Digital Life app, because one of Plaintiff Christley’s Facebook Friends downloaded the This Is Your Digital Life app. Plaintiff Christley did not consent to the sharing of his content and information with the This Is Your Digital Life app.

92. As a result of the release of his content and information, Plaintiff Christley has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using his content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Christley’s private affairs and concerns, as detailed herein. Plaintiff Christley fears that he is at risk of identity theft and fraud, and now spends approximately four hours each month monitoring his credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

93. **Plaintiff Terry Fischer** is a citizen and resident of the State of Washington. Plaintiff Fischer created her Facebook account in 2013 via a personal computer and maintains her Facebook account to the present day. Plaintiff Fischer has accessed her Facebook account from a mobile phone and a personal computer. Plaintiff Fischer also uses Facebook Messenger through Facebook. On or through Facebook, Facebook Messenger, and/or Facebook Chat, Plaintiff Fischer has watched videos, “liked” videos, “shared” videos, “posted” videos, “liked” pages on Facebook that contain videos, and “shared” pages on Facebook that contain videos. These videos were hosted on Facebook’s video streaming services, and included videos that were not posted by Plaintiff Fischer or her Friends, videos that were selected and published by Facebook to Plaintiff Fischer’s News Feed, and videos that were posted, shared, or liked to a non-public audience such as Friends.

94. Plaintiff Fischer recalls that during account registration process she entered her name, an email address, and a confirmation that she met the age requirements. Plaintiff Fischer does not recall being prompted to read or reading the Terms of Service or the Data Policy during the registration process. She does not recall seeing updates to the Terms of Service or the Data Policy since registering for her account. She did not subscribe to, has never visited, and is not aware of the Facebook Site Governance page.

95. On information and belief, Plaintiff Fischer's Privacy Settings for personal information, including birthday, were set to the default setting of Friends of Friends when she created her account. Plaintiff Fischer later changed those settings to Friends in approximately 2017. On information and belief, Plaintiff Fischer's Privacy Settings for posts, including status updates, photos, and videos, were set to the default setting of Public when she created her account. Plaintiff Fischer later changed those settings to Friends of Friends in approximately 2013 and then to Friends in approximately 2016. On information and belief, Plaintiff Fischer's Privacy Settings for Likes, including page likes, interests, and favorites, were set to the default setting of Public when she created her account. Plaintiff Fischer later changed those settings to Friends of Friends in approximately 2013 and then to Friends in approximately 2017. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Fischer did not know that Facebook allowed advertisers to target her directly, using information such as her email address or Facebook User ID. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Fischer did not know that there were separate Privacy Settings to limit the information obtained by Apps used by her Friends. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Fischer did not know that there were separate Privacy Settings to disable advertisements targeting her on the basis of data from third parties such as data brokers.

96. Plaintiff Fischer shared private content and information, including personal information, posts, and Likes, with a non-public audience such as Friends on Facebook. Plaintiff Fischer expected Facebook to protect and secure that private content and information against access by or disclosure to unauthorized parties. This information included personal family photographs, personal family videos, as well as personal perspectives regarding politics, religion, relationships, and family that she wanted to remain private and non-public. Plaintiff Fischer also shared private content and information with Friends through Facebook Messenger. This information included personal family photographs, personal family

videos, as well as personal perspectives regarding politics, religion, relationships, and family that she wanted to remain private and non-public.

97. Plaintiff Fischer believed that when she shared private content and information with a non-public audience such as Friends, by either restricting access to a non-public audience at the time of posting or through her Privacy Settings, she was preventing third parties from accessing her content and information. Plaintiff Fischer was not aware of and did not understand that, when she shared content and information with a non-public audience such as Friends, Facebook would disclose such content and information to: (a) Apps used by her Friends; (b) “Business Partners” such as Apple, Amazon, and Samsung; and (c) advertisers. Plaintiff Fischer was not aware of and did not understand that Facebook maintained a separate set of Privacy Settings for limiting the disclosure of her content and information to Apps used by her Facebook Friends. Plaintiff Fischer was not aware of and did not understand that she could not control, with any settings made available by Facebook, the disclosure of her content and information with Business Partners such as Apple, Amazon, and Samsung. Further, Plaintiff Fischer was not aware of and did not understand that Facebook would allow third parties to obtain her content and information and use it to construct a psychographic profile of her for the purpose of attempting to manipulate her voting decisions or other decisions. Plaintiff Fischer similarly was not aware of and did not understand that Facebook would allow third parties to access her content and information and combine it with personally identifiable information from other sources, including sources outside of Facebook, to create a unique profile of her (as distinct from the individualized profile that she created for her Facebook account).

98. If Plaintiff Fischer had learned what she knows now about Facebook’s data sharing policies before signing up for Facebook, she would not have signed up for Facebook at all. If, after signing up for Facebook, she learned what she knows now, she would have immediately restricted her

profile Privacy Settings, limited sharing with Apps used by Friends, and would have disabled Platform Apps entirely.

99. Plaintiff Fischer confirmed on Facebook that her content and information “was likely shared” with and may have been “misused” by the This Is Your Digital Life App, because Plaintiff Fischer downloaded and logged into the This Is Your Digital Life App. Plaintiff Fischer was not aware of and did not consent to the sharing of her content and information with the This Is Your Digital Life App. Moreover, Plaintiff Fischer did not consent to any third-parties accessing her content and information through her Facebook Friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

100. As a result of the release of her content and information, Plaintiff Fischer has experienced an increase in phone solicitations, Friends requests from trolls or imposter accounts, and other interference with her Facebook account. Additionally, as a result of the release of her content and information, Plaintiff Fischer has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Fischer’s private affairs and concerns, as detailed herein. Plaintiff Fischer fears that she is at risk of identity theft and fraud, and now spends approximately two to three hours each month monitoring her credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future. Because of her heightened risk of identity theft and fraud, Plaintiff Fischer has frozen credit and requested fraud alerts from the various credit monitoring agencies and anticipates continuing to utilize such services for the foreseeable future.

101. **Plaintiff Shelly Forman** is a citizen and resident of the State of Georgia. Plaintiff Forman created her Facebook account in 2008 via a computer to keep in touch with her family members.

She maintains her Facebook account to the present day. Plaintiff Forman has accessed her Facebook account from a computer and mobile phone. Plaintiff Forman also uses Facebook Messenger and/or Facebook Chat. On or through Facebook, Facebook Messenger, and/or Facebook Chat, Plaintiff Forman has obtained and viewed non-public videos, “liked” videos, “shared” videos, “posted” videos, “liked” pages on Facebook that contain videos, and “shared” pages on Facebook that contain videos.” These videos were delivered by Facebook, and included videos that were not posted by Plaintiff Forman or her Friends, videos that were selected and delivered by Facebook to Plaintiff Forman’s News Feed, and videos that were posted, shared, or liked to a non-public audience such as Friends. These videos included personal videos, memes, and videos from Vine, Vimeo, YouTube, and other streaming services. Through Facebook Live, the service that allows users to broadcast live video streams to the News Feed using the Facebook Mentions App, Plaintiff Forman broadcasted a public service announcement video to a private group regarding sensitive topics. Plaintiff Forman shared this Facebook Live video with Friends of Friends. She expected Facebook to protect and secure all of her private video activity against access by or disclosure to unauthorized parties. Plaintiff Forman has enabled location access while using Facebook, Facebook Messenger, and/or Facebook Chat. Plaintiff Forman has also purchased and sold items, including furniture, cars, and car trailers, through Facebook Marketplace. She shared personal information, including her location and phone number, through Facebook Marketplace.

102. Plaintiff Forman does not recall specific details regarding the account registration process. Plaintiff Forman does not recall being prompted to read or reading the Terms of Service or the Data Policy during the registration process. She does not recall seeing updates to the Terms of Service or the Data Policy since registering for her account. Plaintiff Forman does not subscribe to, has never visited, and is not aware of the Facebook Site Governance page.

103. On information and belief, Plaintiff Forman's Privacy Settings for personal information, including birthday, were set to the default setting of Friends of Friends when she created her account. Plaintiff Forman later changed those settings to Friends. On information and belief, Plaintiff Forman's Privacy Settings for posts, including status updates, photos, and videos, were set to the default setting of Friends of Friends when she created her account. Plaintiff Forman later changed those settings to Friends. On information and belief, Plaintiff Forman's Privacy Settings for Likes, including page likes, interests, and favorites, were set to the default setting of Friends of Friends at first. Plaintiff Forman later changed those settings to Friends. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Forman did not know that Facebook allowed advertisers to target her directly, using information such as her email address or Facebook User ID. On information and belief, Plaintiff Forman disabled advertisements targeted on the basis of data from third parties such as data brokers. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Forman did not know that there were separate Privacy Settings to limit the information obtained by Apps used by her Friends. She changed those settings to Friends in approximately 2019, when she became aware of those settings.

104. Plaintiff Forman shared private content and information, including personal information, posts, and Likes, with a non-public audience such as Friends on Facebook. Plaintiff Forman expected Facebook to protect and secure that private content and information against access by or disclosure to unauthorized parties. This information included personal photographs and videos of family and friends, as well as personal perspectives regarding politics, religion, relationships, work, and family that she wanted to remain private and non-public. She would be embarrassed and upset if Facebook had not kept this information private. Plaintiff Forman also shared private content and information with Friends through Facebook Messenger and/or Facebook Chat. Plaintiff Forman expected Facebook to protect and secure that private content and information against access by or disclosure to unauthorized parties. This

information included personal photographs and videos of family and friends, as well as personal perspectives regarding politics, religion, relationships, work, and family that she wanted to remain private and non-public. Via Facebook Messenger, Plaintiff Forman shared highly sensitive information relating to her family's health and safety about her husband's military deployment; his safety depended on the confidentiality of that information.

105. Plaintiff Forman believed that when she shared private content and information with a non-public audience such as Friends, by either restricting access to a non-public audience at the time of posting or through her Privacy Settings, she was preventing third parties from accessing her content and information. Plaintiff Forman was not aware of and did not understand that when she shared content and information with a non-public audience such as Friends, Facebook would disclose such content and information to: (a) Apps used by her Friends; (b) "Business Partners" such as Apple, Amazon, and Samsung; and (c) advertisers. Plaintiff Forman was not aware of and did not understand that Facebook maintained a separate set of Privacy Settings for limiting the disclosure of her content and information to Apps used by her Facebook Friends. Plaintiff Forman was not aware of and did not understand that she could not control, with any settings made available by Facebook, the disclosure of her content and information with Business Partners such as Apple, Amazon, and Samsung. Further, Plaintiff Forman was not aware of and did not understand that Facebook would allow third parties to obtain her content and information and use it to construct a psychographic profile of her for the purpose of attempting to manipulate her voting decisions or other decisions. Plaintiff Forman similarly was not aware of and did not understand that Facebook would allow third parties to access her content and information and combine it with personally identifiable information from other sources, including sources outside of Facebook, to create a unique profile of her (as distinct from the individualized profile that she created for her Facebook account).

106. If Plaintiff Forman had learned what she knows now about Facebook’s data sharing policies before signing up for Facebook, she would not have signed up for Facebook at all. If, after signing up for Facebook, she learned what she knows now, she would have immediately restricted her profile Privacy Settings, limited sharing with Apps used by her Friends, and would have disabled Platform Apps entirely. She also would have altered and reduced her Facebook usage, including being more circumspect regarding sharing personal information.

107. Plaintiff Forman confirmed on Facebook that her content and information may have been “shared” with and “misused” by the This Is Your Digital Life App, because one of Plaintiff Forman’s Facebook Friends downloaded the This Is Your Digital Life App. Plaintiff Forman did not consent to the sharing of her content and information with the This Is Your Digital Life App. Moreover, Plaintiff Forman did not consent to any third-parties accessing her content and information through her Facebook Friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

108. During the 2016 U.S. Presidential election, Plaintiff Forman frequently received political advertisements while using Facebook. On information and belief, Plaintiff Forman was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of her content and information, Plaintiff Forman has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Forman’s private affairs and concerns, as detailed herein. Plaintiff Forman fears that she is at risk of identity theft and fraud, and now spends approximately one to two hours each month monitoring her credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.



109. **Plaintiff Brandon Herman** is a citizen and resident of the State of California. Plaintiff Herman created his Facebook account in 2007 via a personal computer and maintains his Facebook account to the present day. Plaintiff Herman has accessed his Facebook account from a mobile phone and a personal computer. Plaintiff Herman also uses Facebook Messenger and/or instant messaging through Facebook. On or through Facebook, Facebook Messenger, and/or Facebook instant messaging, Plaintiff Herman has watched videos, “liked” videos, “shared” videos, “posted” videos, “liked” pages on Facebook that contain videos, and “shared” pages on Facebook that contain videos.

110. Plaintiff Herman does not recall specific details regarding the account registration process. Plaintiff Herman does not recall being prompted to read the Terms of Service or the Data Policy during the registration process. He does not recall seeing updates to the Terms of Service or the Data Policy since registering for his account. He did not subscribe to, has never visited, and is not aware of the Facebook Site Governance page.

111. On information and belief, Plaintiff Herman’s Privacy Settings for personal information, including birthday, were set to the default setting when he created his account. Plaintiff Herman later changed those settings to Friends Only. On information and belief, Plaintiff Herman’s Privacy Settings for posts, including status updates, photos, and videos, were set to the default setting when he created his account. On information and belief, Plaintiff Herman’s Privacy Settings for Likes, including page likes, interests, and favorites, were set to the default setting when he created his account. Until 2018, post-Cambridge Analytica, Plaintiff Herman did not know that Facebook allowed advertisers to target him directly, using information such as his email address or Facebook ID. Until 2019, Plaintiff Herman did not know that there were separate Privacy Settings to limit the information that Apps used by Friends could obtain.

112. Plaintiff Herman shared private content and information, including personal information, posts, and Likes, with a non-public audience such as Friends Only on Facebook or through Facebook Messenger and/or Facebook instant messaging. Plaintiff Herman expected Facebook to protect and secure that private content and information against access by or disclosure to unauthorized parties. The information included personal family photographs, personal family videos, as well as personal

perspectives regarding politics, religion, relationships, work, and family that he wanted to remain private and non-public. Plaintiff Herman also shared private content and information with Friends through Facebook Messenger and/or Facebook instant messaging. The information included personal perspectives regarding politics, religion, relationships, work and family that he wanted to remain private and non-public.

113. Plaintiff Herman believed that when he shared private content and information with a non-public audience such as Friends Only, by either restricting access to a non-public audience at the time of posting or through his Privacy Settings, he was preventing third parties from accessing his content and information. Plaintiff Herman was not aware of and did not understand that Facebook would disclose content and information when he shared content and information with a non-public audience such as Friends Only to: (a) Apps used by his Friends; (b) “Business Partners” such as Apple, Amazon, and Samsung; and (c) advertisers. Plaintiff Herman was not aware of and did not understand that Facebook maintained a separate set of Privacy Settings for limiting the disclosure of his content and information to Apps used by his Facebook Friends. Plaintiff Herman was not aware of and did not understand that he could not control, with any settings made available by Facebook, the disclosure of his content and information with Business Partners such as Apple, Amazon, and Samsung. Further, Plaintiff Herman was not aware of and did not understand that Facebook would allow third parties to obtain his content and information and use it to construct a psychographic profile of his for the purpose of attempting to manipulate his voting decisions or other decisions. Plaintiff Herman similarly was not aware of and did not understand that Facebook would allow third parties to access his content and information and combine it with personally identifiable information from other sources, including sources outside of Facebook, to create a unique profile of his (as distinct from the individualized profile that he created for his Facebook account).

114. If Plaintiff Herman had learned what he knows now about Facebook’s data sharing policies before signing up for Facebook, he believes that he would not have signed up for Facebook at all. If, after signing up for Facebook, he learned what he knows now, he would have immediately restricted his profile privacy settings, limited sharing with Apps used by his Friends, and would have

disabled Platform Apps entirely. He also would have altered and reduced his Facebook usage, including being more circumspect regarding sharing personal information.

115. On information and belief, Plaintiff Herman believes that his content and information may have been “shared” with and “misused” by the This Is Your Digital Life app, because one of Plaintiff Herman’s Facebook Friends downloaded the This Is Your Digital Life app. Plaintiff Herman was not aware of and did not consent to the sharing of his content and information with the This Is Your Digital Life App or other third parties. Moreover, Plaintiff Herman did not consent to any third parties accessing his content and information through his Facebook Friends and had no knowledge that Facebook had authorized this disclosure of his content and information without his consent.

116. As a result of the release of his content and information, Plaintiff Herman has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using his content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Herman’s private affairs and concerns, as detailed herein. Plaintiff Herman fears that he is at risk of identity theft and fraud, and now spends approximately one and a half hours each month monitoring his credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

117. **Plaintiff Tabielle Holsinger** is a citizen and resident of the State of Idaho. Plaintiff Holsinger created her Facebook account in 2009 via a personal computer and maintains her Facebook account to the present day. Plaintiff Holsinger has accessed her Facebook account from a computer and a mobile phone. She also uses Facebook Messenger and/or Facebook Chat. On or through Facebook, Facebook Messenger, and/or Facebook Chat, Plaintiff Holsinger has obtained and viewed non-public videos, “liked” videos, “shared” videos, “posted” videos, “liked” pages on Facebook that contain videos, and “shared” pages on Facebook that contain videos.” These videos were delivered by Facebook, and included videos that were not posted by Plaintiff Holsinger or her Friends, videos that were selected and delivered by Facebook to Plaintiff Holsinger’s News Feed, and videos that were posted, shared, or liked

to a non-public audience such as Friends. Plaintiff Holsinger has enabled location access while using Facebook, Facebook Messenger, and/or Facebook Chat.

118. Plaintiff Holsinger does not recall specific details regarding the account registration process. Plaintiff Holsinger does not recall being prompted to read or reading the Terms of Service or the Data Policy during the registration process. She does not recall seeing updates to the Terms of Service or the Data Policy since registering for her account. Plaintiff Holsinger does not subscribe to, has never visited, and is not aware of the Facebook Site Governance page.

119. On information and belief, Plaintiff Holsinger's Privacy Settings for personal information, including birthday, were set to the default setting of Friends of Friends when she created her account. On information and belief, Plaintiff Holsinger's Privacy Settings for posts, including status updates, photos, and videos, were set to the default setting of Friends of Friends when she created her account. Plaintiff Holsinger later changed those settings to Friends in approximately 2010 or 2011. On information and belief, Plaintiff Holsinger's Privacy Settings for Likes, including page likes, interests, and favorites, were set to the default setting of Friends of Friends at first. Plaintiff Holsinger later changed those settings to Friends in approximately 2018. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Holsinger did not know that Facebook allowed advertisers to target her directly, using information such as her email address or Facebook User ID. Until 2019, post-Cambridge Analytica Scandal, Plaintiff Holsinger did not know that there were separate Privacy Settings to disable advertisements targeting her on the basis of data from third parties such as data brokers. Until 2019, post-Cambridge Analytica Scandal, Plaintiff Holsinger did not know that there were separate Privacy Settings to limit the information obtained by Apps used by her Friends.

120. Plaintiff Holsinger shared private content and information, including personal information, posts, and Likes, with a non-public audience such as Friends on Facebook. Plaintiff

Holsinger expected Facebook to protect and secure that private content and information against access by or disclosure to unauthorized parties. This information included personal photographs and videos of family and friends, as well as personal perspectives regarding politics, religion, relationships, work, family, and highly personal messages and photos that she wanted to remain private and non-public. Plaintiff Holsinger also shared private content and information with Friends through Facebook Messenger or Facebook Chat. This information included personal photographs and videos of family and friends, as well as personal perspectives regarding politics, religion, relationships, work, family, and highly personal messages and photos that she wanted to remain private and non-public.

121. Plaintiff Holsinger believed that when she shared private content and information with a non-public audience such as Friends, by either restricting access to a non-public audience at the time of posting or through her Privacy Settings, she was preventing third parties from accessing her content and information. Plaintiff Holsinger was not aware of and did not understand that when she shared content and information with a non-public audience such as Friends, Facebook would disclose such content and information to: (a) Apps used by her Friends; (b) “Business Partners” such as Apple, Amazon, and Samsung; and (c) advertisers. Plaintiff Holsinger was not aware of and did not understand that Facebook maintained a separate set of Privacy Settings for limiting the disclosure of her content and information to Apps used by her Facebook Friends. Plaintiff Holsinger was not aware of and did not understand that she could not control, with any settings made available by Facebook, the disclosure of her content and information with Business Partners such as Apple, Amazon, and Samsung. Further, Plaintiff Holsinger was not aware of and did not understand that Facebook would allow third parties to obtain her content and information and use it to construct a psychographic profile of her for the purpose of attempting to manipulate her voting decisions or other decisions. Plaintiff Holsinger similarly was not aware of and did not understand that Facebook would allow third parties to access her content and information and

combine it with personally identifiable information from other sources, including sources outside of Facebook, to create a unique profile of her (as distinct from the individualized profile that she created for her Facebook account).

122. If, after signing up for Facebook, she learned what she knows now, she would have immediately restricted her profile Privacy Settings, limited sharing with Apps used by her Friends, and would have disabled Platform Apps entirely. She also would have altered and reduced her Facebook usage, including being more circumspect regarding sharing personal information.

123. Plaintiff Holsinger confirmed on Facebook that her content and information may have been “shared” with and “misused” by the This Is Your Digital Life App, because one of Plaintiff Holsinger’s Facebook Friends downloaded the This Is Your Digital Life App. Plaintiff Holsinger did not consent to the sharing of her content and information with the This Is Your Digital Life App. Moreover, Plaintiff Holsinger did not consent to any third-parties accessing her content and information through her Facebook Friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

124. During the 2016 U.S. Presidential election, Plaintiff Holsinger frequently received political advertisements while using Facebook. On information and belief, Plaintiff Holsinger was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of her content and information, Plaintiff Holsinger has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Holsinger’s private affairs and concerns, as detailed herein. Plaintiff Holsinger fears that she is at risk of identity theft and fraud, and now spends approximately four hours each month monitoring her

credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

125. **Plaintiff Tyler King** is a citizen and resident of the State of Florida. Plaintiff King created her Facebook account in 2008 via a personal computer and deleted her Facebook account in approximately 2018, after the Cambridge Analytica Scandal became public. Plaintiff King has accessed her Facebook account from a personal computer, a tablet, and a mobile phone. Plaintiff King also used Facebook Messenger and/or Facebook Chat. On or through Facebook, Facebook Messenger, and/or Facebook Chat, Plaintiff King has watched videos, “liked” videos, “shared” videos, “posted” videos, “liked” pages on Facebook that contain videos, and “shared” pages on Facebook that contain videos. These videos were hosted on Facebook’s video streaming services, and included videos that were not posted by Plaintiff King or her Friends, videos that were selected and published by Facebook to Plaintiff King’s News Feed, and videos that were posted, shared, or liked to a non-public audience such as Friends.

126. Plaintiff King recalls that during the account registration process she had to enter her first name, last name, birthday, and email address. Plaintiff King does not recall being prompted to read or reading the Terms of Service or the Data Policy during the registration process. She does not recall seeing updates to the Terms of Service or the Data Policy since registering for her account. She did not subscribe to, has never visited, and is not aware of the Facebook Site Governance page.

127. On information and belief, Plaintiff King’s Privacy Settings for personal information, including birthday, were set to the default setting of Friends of Friends when she created her account. Plaintiff King later changed those settings to Friends in approximately 2010. On information and belief, Plaintiff King’s Privacy Settings for posts, including status updates, photos, and videos, were set to the default setting of Friends of Friends when she created her account. Plaintiff King later changed those

settings to Friends in approximately 2010. On information and belief, Plaintiff King's Privacy Settings for Likes, including page likes, interests, and favorites, were set to the default setting of Friends of Friends at first. Plaintiff King later changed those settings to Friends in approximately 2014. Until 2018, post-Cambridge Analytica Scandal, Plaintiff King did not know that Facebook allowed advertisers to target her directly, using information such as her email address or Facebook User ID. Until 2018, post-Cambridge Analytica Scandal, Plaintiff King did not know that there were separate Privacy Settings to limit the information obtained by Apps used by her Friends. On information and belief, Plaintiff King disabled advertisements targeting her on the basis of data from third parties such as data brokers.

128. Plaintiff King shared private content and information, including personal information, posts, and Likes, with a non-public audience such as Friends on Facebook. Plaintiff King expected Facebook to protect and secure that private content and information against access by or disclosure to unauthorized parties. This information included personal family photographs, personal family videos, as well as personal perspectives regarding politics, religion, relationships, work, and family that she wanted to remain private and non-public. Plaintiff King also shared private content and information with Friends through Facebook Messenger and/or Facebook Chat. This information included personal family photographs, personal family videos, as well as personal perspectives regarding politics, religion, relationships, work, and family that she wanted to remain private and non-public.

129. Plaintiff King believed that when she shared private content and information with a non-public audience such as Friends, by either restricting access to a non-public audience at the time of posting or through her Privacy Settings, she was preventing third parties from accessing her content and information. Plaintiff King was not aware of and did not understand that, when she shared content and information with a non-public audience such as Friends, Facebook would disclose such content and information to: (a) Apps used by her Friends; (b) "Business Partners" such as Apple, Amazon, and



Samsung; and (c) advertisers. Plaintiff King was not aware of and did not understand that Facebook maintained a separate set of Privacy Settings for limiting the disclosure of her content and information to Apps used by her Facebook Friends. Plaintiff King was not aware of and did not understand that she could not control, with any settings made available by Facebook, the disclosure of her content and information with Business Partners such as Apple, Amazon, and Samsung. Further, Plaintiff King was not aware of and did not understand that Facebook would allow third parties to obtain her content and information and use it to construct a psychographic profile of her for the purpose of attempting to manipulate her voting decisions or other decisions. Plaintiff King similarly was not aware of and did not understand that Facebook would allow third parties to access her content and information and combine it with personally identifiable information from other sources, including sources outside of Facebook, to create a unique profile of her (as distinct from the individualized profile that she created for her Facebook account).

130. If Plaintiff King had learned what she knows now about Facebook's data sharing policies before signing up for Facebook, she would not have signed up for Facebook at all. If, after signing up for Facebook, she learned what she knows now, she would have immediately restricted her profile Privacy Settings, limited sharing with Apps used by Friends, and would have disabled Platform Apps entirely. She also would have altered and reduced her Facebook usage, including being more circumspect regarding sharing personal information.

131. Plaintiff King confirmed on Facebook that her content and information may have been "shared" with and "misused" by the This Is Your Digital Life App, because one of Plaintiff King's Facebook Friends downloaded the This Is Your Digital Life App. Plaintiff King did not consent to the sharing of her content and information with the This Is Your Digital Life App. Moreover, Plaintiff King did not consent to any third-parties accessing her content and information through her Facebook Friends

and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

132. During the 2016 U.S. Presidential election, Plaintiff King frequently received political advertisements while using Facebook. On information and belief, Plaintiff King was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of her content and information, Plaintiff King has experienced an increase in phone solicitations, phishing attempts, and compromised credit accounts. Additionally, as a result of the release of her content and information, Plaintiff King has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff King's private affairs and concerns, as detailed herein. Plaintiff King fears that she is at risk of identity theft and fraud, and now spends approximately four hours each month monitoring her credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future. Plaintiff King has access to credit monitoring and identity theft protection services, and because of her heightened risk of identity theft and fraud, anticipates continuing to monitor such services for the foreseeable future.

133. **Plaintiff William Lloyd** is a citizen and resident of the State of New York. Plaintiff Lloyd created his Facebook account in approximately 2014 via a mobile phone and maintains his Facebook account to the present day. Plaintiff Lloyd has accessed his Facebook account from a mobile phone and personal computer. Plaintiff Lloyd also uses Facebook Messenger and/or Facebook Chat. He initially created a Facebook account to promote a book he was writing. On or through Facebook, Facebook Messenger, and/or Facebook Chat, Plaintiff Lloyd has obtained and viewed non-public videos, "liked" videos, "shared" videos, "posted" videos, "liked" pages on Facebook that contain videos,

and “shared” pages on Facebook that contain videos.” These videos were delivered by Facebook, and included videos that were not posted by Plaintiff Lloyd or her Friends, videos that were selected and delivered by Facebook to Plaintiff Lloyd’s News Feed, and videos that were posted, shared, or liked to a non-public audience such as Friends. Plaintiff Lloyd has enabled location access while using Facebook, Facebook Messenger, and/or Facebook Chat. Plaintiff Lloyd has also purchased and attempted to sell items through Facebook Marketplace.

134. Plaintiff Lloyd does not recall specific details regarding the account registration process. Plaintiff Lloyd does not recall being prompted to read or reading the Terms of Service and the Data Policy during the registration process. He does not recall seeing updates to the Terms of Service and the Data Policy since registering for his account. Plaintiff Lloyd does not subscribe to, has never visited, and is not aware of the Facebook Site Governance page.

135. On information and belief, Plaintiff Lloyd’s Privacy Settings for personal information, including birthday, were set to the default setting of Friends when he created his account, though he made certain information, such as his college, was set to Only Me. Plaintiff Lloyd later changed the settings for personal information to Friends in approximately 2015. On information and belief, Plaintiff Lloyd’s Privacy Settings for posts, including status updates, were set to the default setting of Friends when he created his account. Plaintiff Lloyd later changed the settings for anything defaulted to Friends of Friends or Everyone to Friends, in approximately 2015. On information and belief, Plaintiff Lloyd’s Privacy Settings for Likes, including page likes, interests, and favorites, were set to the default setting of Friends of Friends at first. Plaintiff Lloyd later changed those settings to Friends in approximately 2016. He believed that Facebook was limiting the sharing of that information in accordance with his settings. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Lloyd did not know that there were separate Privacy Settings to disable advertisements targeting him on the basis of data from third parties such as

data brokers. Plaintiff Lloyd later became aware of those settings and disabled advertisements targeted on the basis of data from third parties. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Lloyd did not know that there were separate Privacy Settings to limit the information that Apps used by Friends could obtain. Plaintiff Lloyd later became aware of those settings and changed those settings to disable Apps.

136. Plaintiff Lloyd shared private content and information, including personal information, posts, and Likes, with a non-public audience such as Friends on Facebook. He shared this information on his own page, on Friends' pages, and in private groups. Plaintiff Lloyd expected Facebook to protect and secure that private content and information against access by or disclosure to unauthorized parties. This information included personal photographs and videos of friends and family, as well as personal perspectives regarding politics, religion, relationships, work, and family that he wanted to remain private and non-public. Plaintiff Lloyd also shared private content and information with Friends through Facebook Messenger and/or Facebook Chat. This information included personal photographs and videos of friends and family, as well as personal perspectives regarding politics, religion, relationships, work, and family that he wanted to remain private and non-public.

137. Plaintiff Lloyd believed that when he shared private content and information with a non-public audience such as Friends, by either restricting access to a non-public audience at the time of posting or through his Privacy Settings, he was preventing third parties from accessing his content and information. Plaintiff Lloyd was not aware of and did not understand that when he shared content and information with non-public audiences such as Friends, Facebook would disclose such content and information to: (a) Apps used by his Friends; (b) "Business Partners" such as Apple, Amazon, and Samsung; and (c) advertisers. Plaintiff Lloyd was not aware of and did not understand that Facebook maintained a separate set of Privacy Settings for limiting the disclosure of his content and information to

Apps used by his Facebook Friends. Plaintiff Lloyd was not aware of and did not understand that he could not control, with any settings made available by Facebook, the disclosure of his content and information with Business Partners such as Apple, Amazon, and Samsung. Further, Plaintiff Lloyd was not aware of and did not understand that Facebook would allow third parties to obtain his content and information and use it to construct a psychographic profile of him for the purpose of attempting to manipulate his voting decisions or other decisions. Plaintiff Lloyd similarly was not aware of and did not understand that Facebook would allow third parties to access his content and information and combine it with personally identifiable information from other sources, including sources outside of Facebook, to create a unique profile of him (as distinct from the individualized profile that he created for his Facebook account).

138. If Plaintiff Lloyd had learned what he knows now about Facebook's data sharing policies before signing up for Facebook, he would not have signed up for Facebook at all. If, after signing up for Facebook, he learned what he knows now, he would have immediately restricted his profile Privacy Settings, limited sharing with Apps used by his Friends, and would have disabled Platform Apps entirely. He also would have altered and reduced his Facebook usage, including being more circumspect regarding sharing personal information. Plaintiff Lloyd relied on Facebook's promises that "privacy mattered" to the company.

139. Plaintiff Lloyd confirmed on Facebook that his content and information "was likely shared with" and may have been "misused" by the This Is Your Digital Life App, because one of Plaintiff Lloyd's Facebook Friends downloaded the This Is Your Digital Life App. Plaintiff Lloyd was not aware of and did not consent to the sharing of his content and information with the This Is Your Digital Life App. Moreover, Plaintiff Lloyd did not consent to any third-parties accessing his content

and information through his Facebook Friends and had no knowledge that Facebook had authorized this disclosure of his content and information without his consent.

140. During the 2016 U.S. Presidential election, Plaintiff Lloyd frequently received political advertisements while using Facebook. On information and belief, Plaintiff Lloyd was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of his content and information, Plaintiff Lloyd has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using his content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Lloyd's private affairs and concerns, as detailed herein. Plaintiff Lloyd fears that he is at risk of identity theft and fraud, and now spends approximately two hours each month monitoring his credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

141. **Plaintiff Jordan O'Hara** is a citizen and resident of the State of California. Plaintiff O'Hara created his Facebook account in 2007 via a personal computer. Plaintiff O'Hara has accessed his Facebook account from a mobile phone and a personal computer. Plaintiff O'Hara also uses Facebook Messenger and/or Facebook Chat. On or through Facebook, Facebook Messenger, and/or Facebook Chat, Plaintiff O'Hara has obtained and viewed non-public videos, "liked" videos, "shared" videos, "posted" videos, "liked" pages on Facebook that contain videos, and "shared" pages on Facebook that contain videos." These videos were delivered by Facebook, and included videos that were not posted by Plaintiff O'Hara or his Friends, videos that were selected and delivered by Facebook to Plaintiff O'Hara's News Feed, and videos that were posted, shared, or liked to a non-public audience such as Friends.

142. Plaintiff O'Hara does not recall specific details regarding the account registration process. Plaintiff O'Hara does not recall being prompted to read or reading the Terms of Service or the Data Policy during the registration process. He does not recall seeing updates to the Terms of Service or the Data Policy since registering for his account. Plaintiff O'Hara does not subscribe to, has never visited, and is not aware of the Facebook Site Governance page.

143. On information and belief, Plaintiff O'Hara's Privacy Settings for personal information, including birthday, were set to the default setting of Friends of Friends when he created his account. Plaintiff O'Hara later changed these settings to Friends. On information and belief, Plaintiff O'Hara's Privacy Settings for posts, including status updates, photos, and videos, were set to the default setting of Friends of Friends when he created his account. Plaintiff O'Hara later changed these settings to Friends. On information and belief, Plaintiff O'Hara's Privacy Settings for Likes, including page likes, interests, and favorites, were set to the default setting of Friends of Friends at first. Plaintiff O'Hara later changed these settings to Friends. Until 2018, post-Cambridge Analytica Scandal, Plaintiff O'Hara did not know that Facebook allowed advertisers to target him directly, using information such as his email address or Facebook User ID. On information and belief, Plaintiff O'Hara disabled advertisements targeted on the basis of data from third parties such as data brokers. Until 2019, post-Cambridge Analytica Scandal, Plaintiff O'Hara did not know that there were separate Privacy Settings to limit the information that Apps used by Friends could obtain. Plaintiff O'Hara later became aware of those settings and changed those settings to Friends in approximately 2019.

144. Plaintiff O'Hara shared private content and information on Facebook, including personal information, posts, and Likes, with a non-public audience such as Friends on Facebook. Plaintiff O'Hara expected Facebook to protect and secure that private content and information against access by or disclosure to unauthorized parties. This information included personal photographs, personal videos, and

personal perspectives regarding politics, religion, relationships, work, and family that he wanted to remain private and non-public. Plaintiff O'Hara also shared private content and information with Friends through Facebook Messenger and/or Facebook Chat. This information included personal photographs, personal videos, and personal perspectives regarding politics, religion, relationships, work, and family that he wanted to remain private and non-public.

145. Plaintiff O'Hara believed that when he shared private content and information with a non-public audience such as Friends, by either restricting access to a non-public audience at the time of posting or through his Privacy Settings, he was preventing third parties from accessing his content and information. Until 2018, Plaintiff O'Hara was not aware of and did not understand that when he shared content and information with a non-public audience such as Friends, Facebook would disclose such content and information to: (a) Apps used by his Friends; (b) "Business Partners" such as Apple, Amazon, and Samsung; and (c) advertisers. Plaintiff O'Hara was not aware of and did not understand that Facebook maintained a separate set of Privacy Settings for limiting the disclosure of his content and information to Apps used by his Facebook Friends. Plaintiff O'Hara was not aware of and did not understand that he could not control, with any settings made available by Facebook, the disclosure of his content and information with Business Partners such as Apple, Amazon, and Samsung. Further, Plaintiff O'Hara was not aware of and did not understand that Facebook would allow third parties to obtain his content and information and use it to construct a psychographic profile of him to attempt to manipulate his voting decisions or other decisions. Until 2018, Plaintiff O'Hara similarly was not aware of and did not understand that Facebook would allow third parties to access his content and information and combine it with personally identifiable information from other sources, including sources outside of Facebook, to create a unique profile of him (as distinct from the individualized profile that he created for his Facebook account).



146. Plaintiff O'Hara confirmed on Facebook that his content and information may have been "shared" with and "misused" by the This Is Your Digital Life App, because one of Plaintiff O'Hara's Facebook Friends downloaded the This Is Your Digital Life App. Plaintiff O'Hara was not aware of and did not consent to the sharing of his content and information with the This Is Your Digital Life App. Moreover, Plaintiff O'Hara did not consent to any third-parties accessing his content and information through his Facebook Friends and had no knowledge that Facebook had authorized this disclosure of his content and information without his consent.

147. During the 2016 U.S. Presidential election, Plaintiff O'Hara frequently received political advertisements while using Facebook. On information and belief, Plaintiff O'Hara was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of his content and information, Plaintiff O'Hara has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using his content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff O'Hara's private affairs and concerns, as detailed herein. Plaintiff O'Hara fears that he is at risk of identity theft and fraud, and now spends approximately one to two hours each month monitoring his credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future. Because of his heightened risk of identity theft and fraud, Plaintiff O'Hara has obtained credit monitoring and identity theft protection services as a result of his status as a former member of the armed services, and anticipates continuing to use services for the foreseeable future.

148. **Plaintiff Kimberly Robertson** is a citizen and resident of the State of Illinois. Plaintiff Robertson created her Facebook account in 2009 via a personal computer and maintains her Facebook account to the present day. Plaintiff Robertson has accessed her Facebook account from a mobile phone and a personal computer. Plaintiff Robertson also uses Facebook Messenger and/or Facebook Chat. On

or through Facebook, Facebook Messenger, and/or Facebook Chat, Plaintiff Robertson has watched videos, “liked” videos, “shared” videos, “posted” videos, “liked” pages on Facebook that contain videos, and “shared” pages on Facebook that contain videos. These videos were hosted on Facebook’s video streaming services, and included videos that were not posted by Plaintiff Robertson or her Friends, videos that were selected and published by Facebook to Plaintiff Robertson’s News Feed, and videos that were posted, shared, or liked to a non-public audience such as Friends. Plaintiff Robertson has enabled location access while using Facebook, Facebook Messenger, and/or Facebook Chat.

149. Plaintiff Robertson does not recall specific details regarding the account registration process. Plaintiff Robertson does not recall being prompted to read or reading the Terms of Service or the Data Policy during the registration process. She does not recall seeing updates to the Terms of Service or the Data Policy since registering for her account. She did not subscribe to, has never visited, and is not aware of the Facebook Site Governance page.

150. On information and belief, Plaintiff Robertson’s Privacy Settings for personal information, including birthday, were set to the default setting of Friends of Friends when she created her account. Plaintiff Robertson later changed those settings to Friends in approximately 2009. On information and belief, Plaintiff Robertson’s Privacy Settings for posts, including status updates, photos, and videos, were set to the default setting of Friends of Friends when she created her account. Plaintiff Robertson later changed those settings to Friends in approximately 2009. On information and belief, Plaintiff Robertson’s Privacy Settings for Likes, including page likes, interests, and favorites, were set to the default setting of Friends of Friends at first. Plaintiff Robertson later changed those settings to Friends in approximately 2009. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Robertson did not know that Facebook allowed advertisers to target her directly, using information such as her email address or Facebook User ID. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Robertson did

not know that there were separate Privacy Settings to limit the information obtained by Apps used by her Friends. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Robertson did not know that there were separate Privacy Settings to disable advertisements targeting her on the basis of data from third parties such as data brokers.

151. Plaintiff Robertson shared private content and information, including personal information, posts, and Likes, with a non-public audience such as Friends on Facebook. Plaintiff Robertson expected Facebook to protect and secure that private content and information against access by or disclosure to unauthorized parties. This information included personal family photographs, personal family videos, as well as personal perspectives regarding politics, religion, relationships, work and family that she wanted to remain private and non-public. Plaintiff Robertson also shared private content and information with Friends through Facebook Messenger and/or Facebook Chat. This information included personal family photographs, personal family videos, as well as personal perspectives regarding politics, religion, relationships, work, and family that she wanted to remain private and non-public.

152. Plaintiff Robertson believed that when she shared private content and information with a non-public audience such as Friends, by either restricting access to a non-public audience at the time of posting or through her Privacy Settings, she was preventing third parties from accessing her content and information. Plaintiff Robertson was not aware of and did not understand that, when she shared content and information with a non-public audience such as Friends, Facebook would disclose such content and information to: (a) Apps used by her Friends; (b) “Business Partners” such as Apple, Amazon, and Samsung; and (c) advertisers. Plaintiff Robertson was not aware of and did not understand that Facebook maintained a separate set of Privacy Settings for limiting the disclosure of her content and information to Apps used by her Facebook Friends. Plaintiff Robertson was not aware of and did not

understand that she could not control, with any settings made available by Facebook, the disclosure of her content and information with Business Partners such as Apple, Amazon, and Samsung. Further, Plaintiff Robertson was not aware of and did not understand that Facebook would allow third parties to obtain her content and information and use it to construct a psychographic profile of her for the purpose of attempting to manipulate her voting decisions or other decisions. Plaintiff Robertson similarly was not aware of and did not understand that Facebook would allow third parties to access her content and information and combine it with personally identifiable information from other sources, including sources outside of Facebook, to create a unique profile of her (as distinct from the individualized profile that she created for her Facebook account).

153. If Plaintiff Robertson had learned what she knows now about Facebook's data sharing policies before signing up for Facebook, she would not have signed up for Facebook at all. If, after signing up for Facebook, she learned what she knows now, she would have immediately restricted her profile Privacy Settings, limited sharing with Apps used by her Friends, and would have disabled Platform Apps entirely. She also would have altered and reduced her Facebook usage, including being more circumspect regarding sharing personal information.

154. Plaintiff Robertson confirmed on Facebook that her content and information may have been "shared" with and "misused" by the This Is Your Digital Life App, because one of Plaintiff Robertson's Facebook Friends downloaded the This Is Your Digital Life App. Plaintiff Robertson was not aware of and did not consent to the sharing of her content and information with the This Is Your Digital Life App. Moreover, Plaintiff Robertson did not consent to any third-parties accessing her content and information through her Facebook Friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

155. As a result of the release of her content and information, Plaintiff Robertson has experienced an increase in phone solicitations and has had her debit card information stolen. Additionally, as a result of the release of her content and information, Plaintiff Robertson has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Robertson's private affairs and concerns, as detailed herein. Plaintiff Robertson fears that she is at risk of identity theft and fraud, and now spends approximately two hours each month monitoring her credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

156. **Plaintiff Scott Schinder** is a citizen and resident of the State of Texas. Plaintiff Schinder created his Facebook account in 2007 via a computer and maintains his Facebook account to the present day. Plaintiff Schinder has accessed his Facebook account from a computer and mobile phone. Plaintiff Schinder also uses Facebook Messenger and/or Facebook Chat. On or through Facebook, Facebook Messenger, and/or Facebook Chat, Plaintiff Schinder has obtained and viewed non-public videos, "liked" videos, "shared" videos, "posted" videos, "liked" pages on Facebook that contain videos, and "shared" pages on Facebook that contain videos." These videos were delivered by Facebook, and included videos that were not posted by Plaintiff Schinder or his Friends, videos that were selected and delivered by Facebook to Plaintiff Schinder's News Feed, and videos that were posted, shared, or liked to a non-public audience such as Friends.

157. Plaintiff Schinder does not recall specific details regarding the account registration process. Plaintiff Schinder does not recall being prompted to read or reading the Terms of Service during the registration process. He recalls seeing updates to the SRR since registering for his account.

Plaintiff Schinder recalls reading the Data Policy during the registration process. He does not subscribe to, has never visited, and is not aware of the Facebook Site Governance page.

158. On information and belief, Plaintiff Schinder's Privacy Settings for personal information, including birthday, were set to the default setting of Friends of Friends when he created his account. On information and belief, Plaintiff Schinder's Privacy Settings for posts, including status updates, photos, and videos, were set to the default setting of Friends of Friends. On information and belief, Plaintiff Schinder's Privacy Settings for Likes, including page likes, interests, and favorites, were set to the default setting of Friends of Friends at first.

159. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Schinder did not know that Facebook allowed advertisers to target him directly, using information such as his email address or Facebook User ID. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Schinder did not know that there were separate Privacy Settings to disable advertisements targeting him on the basis of data from third parties such as data brokers. Plaintiff Schinder later became aware of those settings and changed those settings to Custom. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Schinder did not know that there were separate Privacy Settings to limit the information that Apps used by Friends could obtain. Plaintiff Schinder later became aware of those settings and changed those settings to Custom.

160. Plaintiff Schinder shared private content and information on Facebook, including personal information, posts, and Likes, with a non-public audience such as Friends. Plaintiff Schinder expected Facebook to protect and secure that private content and information against access by or disclosure to unauthorized parties. This information included personal family and friends photographs and personal perspectives regarding politics, religion, relationships, work, and family that he wanted to remain private and non-public. Plaintiff Schinder also shared private content and information with Friends through Facebook Messenger and/or Facebook Chat. This information included personal family

and friends photographs and personal perspectives regarding politics, religion, relationships, work, and family that he wanted to remain private and non-public.

161. Plaintiff Schinder believed that when he shared private content and information with a non-public audience such as Friends, by either restricting access to a non-public audience at the time of posting or through his Privacy Settings, he was preventing third parties from accessing his content and information. Plaintiff Schinder was not aware of and did not understand that when he shared content and information with non-public audiences such as Friends, Facebook would disclose such content and information to: (a) Apps used by his Friends; (b) “Business Partners” such as Apple, Amazon, and Samsung; and (c) advertisers. Plaintiff Schinder was not aware of and did not understand that Facebook maintained a separate set of Privacy Settings for limiting the disclosure of his content and information to Apps used by his Facebook Friends. Plaintiff Schinder was not aware of and did not understand that he could not control, with any settings made available by Facebook, the disclosure of his content and information with Business Partners such as Apple, Amazon, and Samsung. Further, Plaintiff Schinder was not aware of and did not understand that Facebook would allow third parties to obtain his content and information and use it to construct a psychographic profile of him for the purpose of attempting to manipulate his voting decisions or other decisions. Plaintiff Schinder similarly was not aware of and did not understand that Facebook would allow third parties to access his content and information and combine it with personally identifiable information from other sources, including sources outside of Facebook, to create a unique profile of him (as distinct from the individualized profile that he created for his Facebook account).

162. In approximately April 2018, Plaintiff Schinder received notice from Facebook that his content and information “may have been obtained” by the This Is Your Digital Life App, because one of Plaintiff Schinder’s Facebook Friends downloaded the This Is Your Digital Life App. Plaintiff Schinder

did not consent to the sharing of his content and information with the This Is Your Digital Life App. Moreover, Plaintiff Schinder did not consent to any third-parties accessing his content and information through his Facebook Friends and had no knowledge that Facebook had authorized this disclosure of his content and information without his consent.

163. During the 2016 U.S. Presidential election, Plaintiff Schinder frequently received political advertisements while using Facebook. On information and belief, Plaintiff Schinder was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of his content and information, Plaintiff Schinder has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using his content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Schinder's private affairs and concerns, as detailed herein. Plaintiff Schinder fears that he is at risk of identity theft and fraud, and now spends approximately eight hours each month monitoring his credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

164. **Plaintiff Cheryl Senko** is a citizen and resident of the State of Ohio. Plaintiff Senko created her Facebook account in 2005 via a personal computer. Plaintiff Senko maintains her Facebook account to the present day. Plaintiff Senko has accessed her Facebook account from mobile phones, laptops, personal computers, and a tablet. Plaintiff Senko also uses Facebook Messenger through Facebook. On or through Facebook, Facebook Messenger, and/or Facebook Chat, Plaintiff Senko has watched videos, "liked" videos, "shared" videos, "posted" videos, "liked" pages on Facebook that contain videos, and "shared" pages on Facebook that contain videos. These videos were hosted on Facebook's video streaming services, and included videos that were not posted by Plaintiff Senko or her Friends, videos that were selected and published by Facebook to Plaintiff Senko's News Feed, and



videos that were posted, shared, or liked to a non-public audience such as Friends. Plaintiff Senko has enabled location access while using Facebook, Facebook Messenger, and/or Facebook Chat. Plaintiff Senko has also purchased and/or sold items in the Facebook Marketplace.

165. Plaintiff Senko does not recall specific details regarding the account registration process. Plaintiff Senko does not recall being prompted to read or reading the Terms of Service or the Data Policy during the registration process. She does not recall seeing updates to the Terms of Service or the Data Policy since registering for her account. She did not subscribe to, has never visited, and is not aware of the Facebook Site Governance page.

166. On information and belief, Plaintiff Senko's Privacy Settings for personal information, including birthday, were set to the default setting of Friends when she created her account. Plaintiff Senko later changed those settings to Public in approximately 2011. On information and belief, Plaintiff Senko's Privacy Settings for posts, including status updates, photos, and videos, were set to the default setting of Friends of Friends when she created her account. Plaintiff Senko later changed those settings to Public in approximately 2011. On information and belief, Plaintiff Senko's Privacy Settings for Likes, including page likes, interests, and favorites, were set to the default setting of Friends of Friends at first. Plaintiff Senko later changed those settings to Public in approximately 2011. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Senko did not know that Facebook allowed advertisers to target her directly, using information such as her email address or Facebook User ID. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Senko did not know that there were separate Privacy Settings to limit the information obtained by Apps used by her Friends. On information and belief, Plaintiff Senko disabled advertisements targeting her on the basis of data from third parties such as data brokers.

167. Plaintiff Senko shared private content and information, including personal information, posts, and Likes, with a non-public audience such as Friends on Facebook, particularly between 2005

and 2011. Plaintiff Senko expected Facebook to protect and secure that private content and information against access by or disclosure to unauthorized parties. This information included personal family photographs, personal family videos, as well as personal perspectives regarding politics, religion, and relationships that she wanted to remain private and non-public. Plaintiff Senko also shared private content and information with Friends through Facebook Messenger, during the entire Class Period. This information included personal family photographs, personal family videos, as well as personal perspectives regarding politics, religion, relationships, work, and family that she wanted to remain private and non-public.

168. Plaintiff Senko believed that when she shared private content and information with a non-public audience such as Friends, by either restricting access to a non-public audience at the time of posting or through her Privacy Settings, she was preventing third parties from accessing her content and information. Plaintiff Senko was not aware of and did not understand that, when she shared content and information with a non-public audience such as Friends, Facebook would disclose such content and information to: (a) Apps used by her Friends; (b) “Business Partners” such as Apple, Amazon, and Samsung; and (c) advertisers. Plaintiff Senko was not aware of and did not understand that Facebook maintained a separate set of Privacy Settings for limiting the disclosure of her content and information to Apps used by her Facebook Friends. Plaintiff Senko was not aware of and did not understand that she could not control, with any settings made available by Facebook, the disclosure of her content and information with Business Partners such as Apple, Amazon, and Samsung. Further, Plaintiff Senko was not aware of and did not understand that Facebook would allow third parties to obtain her content and information and use it to construct a psychographic profile of her for the purpose of attempting to manipulate her voting decisions or other decisions. Plaintiff Senko similarly was not aware of and did not understand that Facebook would allow third parties to access her content and information and

combine it with personally identifiable information from other sources, including sources outside of Facebook, to create a unique profile of her (as distinct from the individualized profile that she created for her Facebook account).

169. Plaintiff Senko confirmed on Facebook that her content and information “was likely shared with” the This Is Your Digital Life App, because one of Plaintiff Senko’s Facebook Friends downloaded the This Is Your Digital Life App. Plaintiff Senko was not aware of and did not consent to the sharing of her content and information with the This Is Your Digital Life App. Moreover, Plaintiff Senko did not consent to any third-parties accessing her content and information through her Facebook Friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

170. If, after signing up for Facebook, she learned what she knows now, she would have immediately restricted her profile Privacy Settings, limited sharing with Apps used by her Friends, and would have disabled Platform Apps entirely. She also would have altered and reduced her Facebook usage, including being more circumspect regarding sharing personal information.

171. During the 2016 U.S. Presidential election, Plaintiff Senko frequently received political advertisements while using Facebook. On information and belief, Plaintiff Senko was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of her content and information, Plaintiff Senko has experienced an increase in phishing attempts. Additionally, as a result of the release of her content and information, Plaintiff Senko has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Senko’s private affairs and concerns, as detailed herein. Plaintiff Senko fears that she is at risk of identity theft and fraud, and now spends approximately one hour each month

monitoring her credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future. Because of her heightened risk of identity theft and fraud, Plaintiff Senko enrolled in the credit monitoring service offered by her auto loan company.

172. **Plaintiff Dustin Short** is a citizen and resident of the State of Kansas. Plaintiff Short created his Facebook account in 2005 or 2006 on a personal computer and maintains his Facebook account to the present day. Plaintiff Short has accessed his Facebook account from his personal computer and a mobile phone. He has used mobile phones with Android and Apple operating systems to access Facebook. Plaintiff Short has used Facebook Messenger and/or Facebook Chat. On or through Facebook, Facebook Messenger, and/or Facebook Chat, Plaintiff Short has obtained and viewed non-public videos, “liked” videos, “shared” videos, “posted” videos, “liked” pages on Facebook that contain videos, and “shared” pages on Facebook that contain videos.” These videos were delivered by Facebook, and included videos that were not posted by Plaintiff Short or his Friends, videos that were selected and delivered by Facebook to Plaintiff Short’s News Feed, and videos that were posted, shared, or liked to a non-public audience such as Friends.

173. Plaintiff Short recalls that during the account registration process, he was required to verify his identity through his college email address. Plaintiff Short does not recall being prompted to read or reading Terms of Service or the Data Policy during the registration process. Plaintiff Short does not recall seeing updates to the Terms of Service or the Data Policy since registering for his account. Plaintiff Short does not subscribe to, has never visited, and was not aware of the Facebook Site Governance page until 2019.

174. On information and belief, Plaintiff Short’s Privacy Settings for personal information, including birthday, were set to the default setting of Friends when he created his account. When Plaintiff Short created his account, Facebook membership was limited to college students and Facebook was

closed to non-Facebook members, including search engines. Plaintiff Short later changed those settings to Friends in approximately 2009 for employment-related reasons. On information and belief, Plaintiff Short's Privacy Settings for posts, including status updates, photos, and videos, were set to the default setting of Friends of Friends when he created his account. Plaintiff Short later changed those settings to Friends in approximately 2009. He later changed those settings again to Only Me in 2018. On information and belief, Plaintiff Short's Privacy Settings for Likes, including page likes, interests, and favorites, were set to the default setting of Friends of Friends at first. There were a number of page likes, interests, and favorites that he chose, including sports teams, local businesses, local government, politics, and more. Plaintiff Short later changed those settings to Friends in approximately 2009. He later changed those settings again to Only Me in 2018. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Short did not know that Facebook allowed advertisers to target him directly, using information such as his email address or Facebook User ID. He also did not know that Facebook allowed demographic advertising. On information and belief, Plaintiff Short disabled advertisements targeted on the basis of data from third parties such as data brokers. Plaintiff Short was not aware of and did not understand that Facebook maintained a separate set of Privacy Settings for limiting the disclosure of his content and information to Apps used by his Facebook Friends. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Short did not understand that Facebook was allowing his Friends to release his content and information through apps. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Short did not know that third parties still had access to his content and information and was surprised to learn this. After learning this, Plaintiff Short disabled these settings and immediately restricted his profile Privacy Settings, limited sharing with Apps used by his Friends, and disabled Platform Apps entirely.

175. Plaintiff Short shared private content and information, including personal information, posts, and Likes, with a non-public audience such as Friends on Facebook. Plaintiff Short expected

Facebook to protect and secure that private content and information against access by or disclosure to unauthorized parties. This information included personal family photographs, personal family and friends videos, as well as personal perspectives regarding politics, religion, relationships, and family that he wanted to remain private and non-public. Plaintiff Short also shared private content and information with Friends through Facebook Messenger and/or Facebook Chat. This information included personal photographs, personal videos, and personal perspectives regarding politics, religion, relationships, and family that he wanted to remain private and non-public.

176. Plaintiff Short believed that when he shared private content and information with a non-public audience such as Friends, by either restricting access to a non-public audience at the time of posting or through his Privacy Settings, he was preventing third parties from accessing his content and information. Plaintiff Short was not aware of and did not understand that when he shared content and information with non-public audiences such as Friends, Facebook would disclose such content and information to: (a) Apps used by his Friends; (b) “Business Partners” such as Apple, Amazon, and Samsung; and (c) advertisers. Plaintiff Short was not aware of and did not understand that he could not control, with any settings made available by Facebook, the disclosure of his content and information with Business Partners such as Apple, Amazon, and Samsung. Further, Plaintiff Short was not aware of and did not understand that Facebook would allow third parties to obtain his content and information and use it to construct a psychographic profile of him to attempt to manipulate his voting decisions or other decisions. Plaintiff Short similarly was not aware of and did not understand that Facebook would allow third parties to access his content and information and combine it with personally identifiable information from other sources, including sources outside of Facebook, to create a unique profile of him (as distinct from the individualized profile that he created for his Facebook account).

177. If Plaintiff Short had learned what he knows now about Facebook's data sharing policies before signing up for Facebook, he would not have signed up for Facebook at all. He also would have altered and reduced his Facebook usage, including being more circumspect regarding sharing personal information.

178. Plaintiff Short confirmed on Facebook that his content and information may have been "shared" with and "misused" by the This Is Your Digital Life App, because one of Plaintiff Short's Facebook Friends downloaded the This Is Your Digital Life App. Plaintiff Short did not consent to the sharing of his content and information with the This Is Your Digital Life App. Moreover, Plaintiff Short did not consent to any third-parties accessing his content and information through his Facebook Friends and had no knowledge that Facebook had authorized this disclosure of his content and information without his consent.

179. During the 2016 U.S. Presidential election, Plaintiff Short frequently received political advertisements while using Facebook. On information and belief, Plaintiff Short was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of his content and information, Plaintiff Short has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using his content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Short's private affairs and concerns, as detailed herein. Plaintiff Short fears that he is at risk of identity theft and fraud, and now spends approximately ten hours each week monitoring his credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future. Because of his heightened risk of identity theft and fraud, Plaintiff Short has purchased credit monitoring, identity theft protection services, and legal counsel, and anticipates continuing to pay for such services for the foreseeable future.

180. **Plaintiff Tonya Smith** is a citizen and resident of the State of Alabama. Plaintiff Smith created her Facebook account in 2007 via a personal computer and maintains her Facebook account to the present day. Plaintiff Smith has accessed her Facebook account from a personal computer, a tablet, and a mobile phone. Plaintiff Smith also uses Facebook Messenger and/or Facebook Chat. On or through Facebook, Facebook Messenger, and/or Facebook Chat, Plaintiff Smith has watched videos, “liked” videos, “shared” videos, “posted” videos, “liked” pages on Facebook that contain videos, and “shared” pages on Facebook that contain videos. These videos were hosted on Facebook’s video streaming services, and included videos that were not posted by Plaintiff Smith or her Friends, videos that were selected and published by Facebook to Plaintiff Smith’s News Feed, and videos that were posted, shared, or liked to a non-public audience such as Friends. Plaintiff Smith has enabled location access while using Facebook, Facebook Messenger, and/or Facebook Chat. Plaintiff Smith has also purchased and/or sold items in the Facebook Marketplace.

181. Plaintiff Smith does not recall specific details regarding the account registration process. Plaintiff Smith does not recall being prompted to read or reading the Terms of Service or the Data Policy during the registration process. She did not subscribe to, has never visited, and is not aware of the Facebook Site Governance page.

182. On information and belief, Plaintiff Smith’s Privacy Settings for personal information, including birthday, were set to the default setting of Friends of Friends when she created her account. Plaintiff Smith later changed those settings to Friends in approximately 2007. On information and belief, Plaintiff Smith’s Privacy Settings for posts, including status updates, photos, and videos, were set to the default setting of Friends of Friends when she created her account. Plaintiff Smith later changed those settings to Friends in approximately 2007. On information and belief, Plaintiff Smith’s Privacy Settings for Likes, including page likes, interests, and favorites, were set to the default setting of Friends



of Friends at first. Plaintiff Smith later changed those settings to Friends in approximately 2009. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Smith did not know that Facebook allowed advertisers to target her directly, using information such as her email address or Facebook User ID. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Smith did not know that there were separate Privacy Settings to limit the information obtained by Apps used by her Friends. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Smith did not know that there were separate Privacy Settings to disable advertisements targeting her on the basis of data from third parties such as data brokers.

183. Plaintiff Smith shared private content and information, including personal information, posts, and Likes, with a non-public audience such as Friends on Facebook. Plaintiff Smith expected Facebook to protect and secure that private content and information against access by or disclosure to unauthorized parties. This information included personal family photographs, personal family videos, as well as personal perspectives regarding religion and relationships that she wanted to remain private and non-public. Plaintiff Smith also shared private content and information with Friends through Facebook Messenger and/or Facebook Chat. This information included personal family photographs, personal family videos, as well as personal perspectives that she wanted to remain private and non-public.

184. Plaintiff Smith believed that when she shared private content and information with a non-public audience such as Friends, by either restricting access to a non-public audience at the time of posting or through her Privacy Settings, she was preventing third parties from accessing her content and information. Plaintiff Smith was not aware of and did not understand that, when she shared content and information with a non-public audience such as Friends, Facebook would disclose such content and information to: (a) Apps used by her Friends; (b) “Business Partners” such as Apple, Amazon, and Samsung; and (c) advertisers. Plaintiff Smith was not aware of and did not understand that Facebook maintained a separate set of Privacy Settings for limiting the disclosure of her content and information to

Apps used by her Facebook Friends. Plaintiff Smith was not aware of and did not understand that she could not control, with any settings made available by Facebook, the disclosure of her content and information with Business Partners such as Apple, Amazon, and Samsung. Further, Plaintiff Smith was not aware of and did not understand that Facebook would allow third parties to obtain her content and information and use it to construct a psychographic profile of her for the purpose of attempting to manipulate her voting decisions or other decisions. Plaintiff Smith similarly was not aware of and did not understand that Facebook would allow third parties to access her content and information and combine it with personally identifiable information from other sources, including sources outside of Facebook, to create a unique profile of her (as distinct from the individualized profile that she created for her Facebook account).

185. If Plaintiff Smith had learned what she knows now about Facebook's data sharing policies after signing up for Facebook, she would have immediately restricted her profile Privacy Settings and would have limited sharing with Apps used by her Friends. She also would have altered and reduced her Facebook usage, including being more circumspect regarding sharing personal information.

186. Plaintiff Smith confirmed on Facebook that her content and information may have been "shared" with and "misused" by the This Is Your Digital Life App, because one of Plaintiff Smith's Facebook Friends downloaded the This Is Your Digital Life App. Plaintiff Smith did not consent to the sharing of her content and information with the This Is Your Digital Life App. Moreover, Plaintiff Smith did not consent to any third-parties accessing her content and information through her Facebook Friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

187. During the 2016 U.S. Presidential election, Plaintiff Smith frequently received political advertisements while using Facebook. On information and belief, Plaintiff Smith was targeted by some

or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of her content and information, Plaintiff Smith has experienced an increase in phone solicitations, phishing attempts, and has received an alert that her information was located on the Dark Web. Additionally, as a result of the release of her content and information, Plaintiff Smith has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Smith's private affairs and concerns, as detailed herein. Plaintiff Smith fears that she is at risk of identity theft and fraud, and now spends approximately ten hours each month monitoring her credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future. Because of her heightened risk of identity theft and fraud, Plaintiff Smith has purchased credit monitoring and identity theft protection services, and anticipates continuing to pay for such services for the foreseeable future.

188. **Plaintiff Charnae Tutt** is a citizen and resident of the State of Georgia. Plaintiff Tutt created her Facebook account in 2009 via a personal computer and maintains her Facebook account to the present day. Plaintiff Tutt has accessed her Facebook account from a personal computer, a tablet, and a mobile phone. Plaintiff Tutt also uses Facebook Messenger and/or Facebook Chat. On or through Facebook, Facebook Messenger, and/or Facebook Chat, Plaintiff Tutt has watched videos, "liked" videos, "shared" videos, "posted" videos, "liked" pages on Facebook that contain videos, and "shared" pages on Facebook that contain videos. These videos were hosted on Facebook's video streaming services, and included videos that were not posted by Plaintiff Tutt or her Friends, videos that were selected and published by Facebook to Plaintiff Tutt's News Feed, and videos that were posted, shared, or liked to a non-public audience such as Friends. Plaintiff Tutt has enabled location access while using

Facebook, Facebook Messenger, and/or Facebook Chat. Plaintiff Tutt has also purchased and/or sold items in the Facebook Marketplace.

189. Plaintiff Tutt recalls that during the account registration process she had to provide her first name, last name, birthday, and email address. Plaintiff Tutt does not recall being prompted to read or reading the Terms of Service or the Data Policy during the registration process. She does not recall seeing updates to the Terms of Service or the Data Policy since registering for her account. She did not subscribe to, has never visited, and is not aware of the Facebook Site Governance page.

190. On information and belief, Plaintiff Tutt's Privacy Settings for personal information, including birthday, were set to the default setting of Friends of Friends when she created her account. Plaintiff Tutt later changed those settings to Friends. On information and belief, Plaintiff Tutt's Privacy Settings for posts, including status updates, photos, and videos, were set to the default setting of Friends of Friends when she created her account. On information and belief, Plaintiff Tutt changed those settings to Friends, but also started customizing his privacy on a post-by-post, photo-by-photo, video-by-video basis. On information and belief, Plaintiff Tutt's Privacy Settings for Likes, including page likes, interests, and favorites, were set to the default setting of Friends of Friends at first. Plaintiff Tutt later changed those settings to Only Me. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Tutt did not know that Facebook allowed advertisers to target her directly, using information such as her email address or Facebook User ID. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Tutt did not know that there were separate Privacy Settings to limit the information obtained by Apps used by her Friends. On information and belief, Plaintiff Tutt disabled advertisements targeting her on the basis of data from third parties such as data brokers.

191. Plaintiff Tutt shared private content and information, including personal information, posts, and Likes, with a non-public audience such as Friends on Facebook. Plaintiff Tutt expected

Facebook to protect and secure that private content and information against access by or disclosure to unauthorized parties. This information included personal family photographs, personal family videos, as well as personal perspectives regarding politics, religion, relationships, work, and family that she wanted to remain private and non-public. Plaintiff Tutt also shared private content and information with Friends through Facebook Messenger and/or Facebook Chat. This information included personal family photographs, personal family videos, as well as personal perspectives regarding politics, religion, relationships, work, and family that she wanted to remain private and non-public.

192. Plaintiff Tutt believed that when she shared private content and information with a non-public audience such as Friends, by either restricting access to a non-public audience at the time of posting or through her Privacy Settings, she was preventing third parties from accessing her content and information. Plaintiff Tutt was not aware of and did not understand that, when she shared content and information with a non-public audience such as Friends, Facebook would disclose such content and information to: (a) Apps used by her Friends; (b) “Business Partners” such as Apple, Amazon, and Samsung; and (c) advertisers. Plaintiff Tutt was not aware of and did not understand that Facebook maintained a separate set of Privacy Settings for limiting the disclosure of her content and information to Apps used by her Facebook Friends. Plaintiff Tutt was not aware of and did not understand that she could not control, with any settings made available by Facebook, the disclosure of her content and information with Business Partners such as Apple, Amazon, and Samsung. Further, Plaintiff Tutt was not aware of and did not understand that Facebook would allow third parties to obtain her content and information and use it to construct a psychographic profile of her for the purpose of attempting to manipulate her voting decisions or other decisions. Plaintiff Tutt similarly was not aware of and did not understand that Facebook would allow third parties to access her content and information and combine it with personally identifiable information from other sources, including sources outside of Facebook, to

create a unique profile of her (as distinct from the individualized profile that she created for her Facebook account).

193. If Plaintiff Tutt had learned what she knows now about Facebook's data sharing policies before signing up for Facebook, she would not have signed up for Facebook at all. If, after signing up for Facebook, she learned what she knows now, she would have immediately restricted her profile Privacy Settings, limited sharing with Apps used by Friends, and would have disabled Platform Apps entirely. She also would have altered and reduced her Facebook usage, including being more circumspect regarding sharing personal information.

194. Plaintiff Tutt confirmed on Facebook that her content and information may have been "shared" with and "misused" by the This Is Your Digital Life App, because one of Plaintiff Tutt's Facebook Friends downloaded the This Is Your Digital Life App. Plaintiff Tutt did not consent to the sharing of her content and information with the This Is Your Digital Life App. Moreover, Plaintiff Tutt did not consent to any third-parties accessing her content and information through her Facebook Friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

195. During the 2016 U.S. Presidential election, Plaintiff Tutt frequently received political advertisements while using Facebook. On information and belief, Plaintiff Tutt was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. In particular, Plaintiff Tutt recalls that she received highly offensive advertisements during the 2016 U.S. Presidential election, and believes that she was targeted with such advertisements because of her race and gender. She believes that these advertisements were designed to improperly influence her voting decisions. As a result of the release of her content and information, Plaintiff Tutt has experienced an increase in phone solicitations as well as unauthorized credit inquiries, starting in approximately 2016. Additionally, as a result of the

release of her content and information, Plaintiff Tutt has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Tutt's private affairs and concerns, as detailed herein. Plaintiff Tutt fears that she is at risk of identity theft and fraud, and now spends approximately four to five hours each month monitoring her credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future. Because of her heightened risk of identity theft and fraud, Plaintiff Tutt has obtained credit monitoring and identity theft protection services, and anticipates continuing to use and monitor such services for the foreseeable future.

196. **Plaintiff Juliana Watson** is a citizen and resident of the State of California. Plaintiff Watson created her Facebook account in 2009 via a computer and maintains her Facebook account to the present day. Plaintiff Watson has accessed her Facebook account from a computer and mobile phones using both Apple and Android operating systems. Plaintiff Watson has used Facebook Messenger and/or Facebook Chat. On or through Facebook, Facebook Messenger, and/or Facebook Chat, Plaintiff Watson has obtained and viewed non-public videos, "liked" videos, "shared" videos, "posted" videos, "liked" pages on Facebook that contain videos, and "shared" pages on Facebook that contain videos." These videos were delivered by Facebook, and included videos that were not posted by Plaintiff Watson or her Friends, videos that were selected and delivered by Facebook to Plaintiff Watson's News Feed, and videos that were posted, shared, or liked to a non-public audience such as Friends.

197. Plaintiff Watson does not recall specific details regarding the account registration process. Plaintiff Watson does not recall being prompted to read or reading the Terms of Service or the Data Policy during the registration process. She does not recall seeing updates to the Data Policy since

registering for her account. Plaintiff Watson does not subscribe to, has never visited, and is not aware of the Facebook Site Governance page.

198. On information and belief, Plaintiff Watson's Privacy Settings for personal information, including birthday, were set to the default setting of Friends of Friends when she created her account. Plaintiff Watson later changed those settings to Friends in approximately 2013. On information and belief, Plaintiff Watson's Privacy Settings for posts, including status updates, photos, and videos, were set to the default setting of Friends of Friends when she created her account. Plaintiff Watson later changed those settings to Friends in approximately 2013. On information and belief, Plaintiff Watson's Privacy Settings for Likes, including page likes, interests, and favorites, were set to the default setting of Friends of Friends at first. Plaintiff Watson later changed those settings to Friends in approximately 2013. She believed that Facebook was limiting the sharing of that information in accordance with her settings. Until 2018, post-Cambridge Analytica Scandal, Plaintiff Watson did not know that Facebook allowed advertisers to target her directly, using information such as her email address or Facebook User ID. Plaintiff Watson did not know that Facebook allowed advertisers to target her based on data from third parties such as data brokers. Until 2019, post-Cambridge Analytica Scandal, Plaintiff Watson did not know that there were separate Privacy Settings to limit the information that Apps used by Friends could obtain.

199. Plaintiff Watson shared private content and information on Facebook, including personal information, posts, and Likes, with a non-public audience such as Friends on Facebook. Plaintiff Watson expected Facebook to protect and secure that private content and information against access by or disclosure to unauthorized parties. This information included personal photographs, personal videos recorded by herself or a friend, and personal perspectives regarding politics, religion, relationships, work, and family that she wanted to remain private and non-public. Plaintiff Watson also shared private



content and information with Friends through Facebook Messenger and/or Facebook Chat. This information included personal photographs, personal videos, and personal perspectives regarding politics, religion, relationships, work, and family that she wanted to remain private and non-public.

200. Plaintiff Watson believed that when she shared private content and information with a non-public audience such as Friends, by either restricting access to a non-public audience at the time of posting or through her Privacy Settings, she was preventing third parties from accessing her content and information. Plaintiff Watson was not aware of and did not understand that when she shared content and information with non-public audiences such as Friends, Facebook would disclose such content and information to: (a) Apps used by her Friends; (b) “Business Partners” such as Apple, Amazon, and Samsung; and (c) advertisers. Plaintiff Watson was not aware of and did not understand that Facebook maintained a separate set of Privacy Settings for limiting the disclosure of her content and information to Apps used by her Facebook Friends. Plaintiff Watson was not aware of and did not understand that she could not control, with any settings made available by Facebook, the disclosure of her content and information with Business Partners such as Apple, Amazon, and Samsung. Further, Plaintiff Watson was not aware of and did not understand that Facebook would allow third parties to obtain her content and information and use it to construct a psychographic profile of her for the purpose of attempting to manipulate her voting decisions or other decisions. Plaintiff Watson similarly was not aware of and did not understand that Facebook would allow third parties to access her content and information and combine it with personally identifiable information from other sources, including sources outside of Facebook, to create a unique profile of her (as distinct from the individualized profile that she created for her Facebook account).

201. If Plaintiff Watson had learned what she knows now about Facebook’s data sharing policies before signing up for Facebook, she would have immediately restricted her profile Privacy

Settings and limited sharing with Apps used by her Friends. She also would have altered and reduced her Facebook usage, including being more circumspect regarding sharing personal information.

202. Plaintiff Watson confirmed on Facebook that her content and information “was likely shared with” the This Is Your Digital Life App, because one of Plaintiff Watson’s Facebook Friends downloaded the This Is Your Digital Life App. Plaintiff Watson did not consent to the sharing of her content and information with the This Is Your Digital Life App. Moreover, Plaintiff Watson did not consent to any third-parties accessing her content and information through her Facebook Friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

203. During the 2016 U.S. Presidential election, Plaintiff Watson frequently received political advertisements while using Facebook. On information and belief, Plaintiff Watson was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of her content and information, Plaintiff Watson has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Watson’s private affairs and concerns, as detailed herein. Plaintiff Watson fears that she is at risk of identity theft and fraud.

204. **Plaintiff Annie Wenz** is a citizen and resident of the State of Florida. Plaintiff Wenz created her Facebook account in 2009 via a personal computer and maintains her Facebook account to the present day. Plaintiff Wenz has accessed her Facebook account from a mobile phone and a personal computer. Plaintiff Wenz also uses Facebook Messenger and/or instant messaging through Facebook. On or through Facebook, Facebook Messenger, and/or Facebook instant messaging, Plaintiff Wenz has watched videos, “liked” videos, “shared” videos, “posted” videos, “liked” pages on Facebook that contain videos, and “shared” pages on Facebook that contain videos.

205. Plaintiff Wenz does not recall specific details regarding the account registration process. Plaintiff Wenz does not recall being prompted to read the Terms of Service or the Data Policy during the registration process. She does not recall seeing updates to the Terms of Service or the Data Policy since registering for her account. She did not subscribe to, has never visited, and is not aware of the Facebook Site Governance page.

206. On information and belief, Plaintiff Wenz's Privacy Settings for personal information, including birthday, were set to the default setting when she created her account. Plaintiff Wenz later changed those settings to Friends of Friends. On information and belief, Plaintiff Wenz's Privacy Settings for posts, including status updates, photos, and videos, were set to the default setting when she created her account. On information and belief, Plaintiff Wenz's Privacy Settings for Likes, including page likes, interests, and favorites, were set to the default setting when she created her account. Until 2018, post-Cambridge Analytica Scandal Plaintiff Wenz did not know that Facebook allowed advertisers to target her directly, using information such as her email address or Facebook ID. Until 2019, Plaintiff Wenz did not know that there were separate Privacy Settings to limit the information that Apps used by Friends could obtain.

207. Plaintiff Wenz shared private content and information, including personal information, posts, and Likes, with a non-public audience including Friends Only and Friends of Friends on Facebook or through Facebook Messenger and/or Facebook instant messaging. Plaintiff Wenz expected Facebook to protect and secure that private content and information against access by or disclosure to unauthorized parties. The information included personal family photographs, videos of family and friends, as well as personal perspectives regarding politics, religion, relationships, work, and family that she wanted to remain private and non-public. Plaintiff Wenz also shared private content and information with Friends through Facebook Messenger and/or Facebook instant messaging. The information included personal photographs, videos of family and friends, personal perspectives regarding politics, religion, relationships, work, and family that she wanted to remain private and non-public.

208. Plaintiff Wenz believed that when she shared private content and information with a non-

public audience such as Friends Only, by either restricting access to a non-public audience at the time of posting or through her Privacy Settings, she was preventing third parties from accessing her content and information. Plaintiff Wenz was not aware of and did not understand that Facebook would disclose content and information when she shared content and information with a non-public audience such as Friends Only to: (a) Apps used by her Friends; (b) “Business Partners” such as Apple, Amazon, and Samsung; and (c) advertisers. Plaintiff Wenz was not aware of and did not understand that Facebook maintained a separate set of Privacy Settings for limiting the disclosure of her content and information to Apps used by her Facebook Friends. Plaintiff Wenz was not aware of and did not understand that she could not control, with any settings made available by Facebook, the disclosure of her content and information with Business Partners such as Apple, Amazon, and Samsung. Further, Plaintiff Wenz was not aware of and did not understand that Facebook would allow third parties to obtain her content and information and use it to construct a psychographic profile of her for the purpose of attempting to manipulate her voting decisions or other decisions. Plaintiff Wenz similarly was not aware of and did not understand that Facebook would allow third parties to access her content and information and combine it with personally identifiable information from other sources, including sources outside of Facebook, to create a unique profile of her (as distinct from the individualized profile that she created for her Facebook account).

209. If Plaintiff Wenz had learned what she knows now about Facebook’s data sharing policies before signing up for Facebook, she believes that she would not have signed up for Facebook at all. If, after signing up for Facebook, she learned what she knows now, she would have immediately restricted her profile privacy settings, limited sharing with Apps used by her Friends, and would have disabled Platform Apps entirely. She also would have altered and reduced her Facebook usage, including being more circumspect regarding sharing personal information.

210. Plaintiff Wenz confirmed on Facebook that her content and information may have been “shared” with and “misused” by the This Is Your Digital Life app, because one of Plaintiff Wenz’s Facebook Friends downloaded the This Is Your Digital Life app. Plaintiff Wenz did not consent to the sharing of her content and information with the This Is Your Digital Life app. Moreover, Plaintiff

Wenz did not consent to any third-parties accessing her content and information through her Facebook Friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

211. During the 2016 U.S. Presidential election, Plaintiff Wenz frequently received political advertisements while using Facebook. On information and belief, Plaintiff Wenz was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of her content and information, Plaintiff Wenz has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Wenz's private affairs and concerns, as detailed therein.

## **B. Defendants and Co-Conspirators**

### **1. Prioritized Defendant and Doe Defendants:**

212. **Facebook, Inc.** ("Facebook"), a publicly traded company, is incorporated in the State of Delaware, with its executive offices located at 1601 Willow Road, Menlo Park, California 94025 and its headquarters located at 1 Hacker Way, Menlo Park, California 94025. Facebook is an online social media and social networking service company founded in 2004. In 2004 Facebook started as a social networking website enabling users to connect, share, and communicate with each other through text, photographs, and videos as well as to interact with third party Apps such as games and quizzes on mobile devices and personal computers. Over time, Facebook has evolved into its own platform that allows users to connect with each other while also acting as a data broker, harvesting user content and information and selling access to the data via targeted messaging to third parties such as advertisers, political action groups and others. Facebook's market value is currently estimated at more than \$473 billion, with annual revenues of \$40 billion from advertising.

213. **Doe Defendants 1-100:** Plaintiffs do not know the true names of Doe Defendants 1-100, inclusive, and therefore sue them by those fictitious names. Plaintiffs are informed and believe, and on the basis of that information and belief, allege that each of those defendants were proximately responsible for the events and happenings alleged in this Complaint and for Plaintiffs' injuries and

damages.

**2. Non-Prioritized Defendants (Individual Defendants Named in Actions Consolidated in this MDL as to Whom Co-Lead Counsel Seek a Stay)**

214. **Stephen Kevin Bannon** is a resident of the District of Columbia. At all relevant times, Bannon was a part owner, Vice President, and Secretary of Cambridge Analytica until he resigned from those positions to act as the chief executive of Donald Trump’s presidential campaign. At all relevant times, Bannon had decision-making authority at Cambridge Analytica and directed and approved the actions taken by Cambridge Analytica alleged herein.

215. **Aleksandr Kogan**, a/k/a Aleksandr Spectre, is a resident of the state of California and Cambridge, England. Dr. Kogan was a founder of GSR. At all relevant times, Dr. Kogan had decision-making authority at GSR and directed, approved, or otherwise ratified the actions taken by GSR as alleged herein.

**C. Interested Parties**

216. **Sheryl Kara Sandberg** is an individual residing in Menlo Park, California. Ms. Sandberg is the chief operating officer (“COO”) of Facebook. Ms. Sandberg has served as Facebook’s COO since 2008, and has been a member of Facebook’s Board since 2012. As Facebook’s COO, Ms. Sandberg is responsible for Facebook’s day-to-day operations and reports directly to Mr. Zuckerberg. Ms. Sandberg oversees Facebook’s business operations, including sales, marketing, business development, human resources, public policy, and communications. Ms. Sandberg was instrumental in developing Facebook’s online advertising programs, and was the “architect” of Facebook’s transformation “into a global advertising juggernaut.”

217. **Mark Elliot Zuckerberg** is an individual residing in Palo Alto, California. Mr. Zuckerberg is the founder of Facebook and has served as Facebook’s CEO and as a member of the Board since July 2004, and as Chairman of the Board since January 2012. Mr. Zuckerberg is responsible for Facebook’s day-to-day operations, as well as the overall direction and product strategy of Facebook. He is also Facebook’s controlling stockholder with ownership of stock and proxies for stock representing more than 53.3% of Facebook’s voting power as of April 13, 2018, though he owns

only 16% of Facebook's total equity.

**D. Unnamed Co-Conspirators: Cambridge-Analytica-Related Entities<sup>11</sup>**

218. **Cambridge Analytica LLC** ("Cambridge Analytica") is a privately held limited liability company organized under the laws of the State of Delaware, incorporated on December 31, 2013, with its principal offices located at 597 5th Avenue, 7th Floor, New York, New York 10017. Cambridge Analytica does business throughout the United States, including in this District. Cambridge Analytica maintains offices in London, New York, and Washington, D.C. Its registered agent for service of summons is The Corporation Trust Company, 1209 Orange Street, Corporation Trust Center, Wilmington, Delaware 19801. Cambridge Analytica is a political consulting and "behavioral microtargeting" firm that combines data mining, data brokerage, and data analysis with strategic communication for the electoral process. It was founded in 2013 as a subsidiary of its parent company SCL Group, to participate in American politics. In 2014, Cambridge Analytica was involved in 44 U.S. political races. Cambridge Analytica was also active in the Brexit campaign. According to the *Business Insider*, Defendant Stephen Bannon was Vice President of Cambridge Analytica from June 2014 until August 2016.

219. **Cambridge Analytica Commercial LLC** ("CA Commercial") is a privately held limited liability company organized under the laws of the State of Delaware, incorporated on January 21, 2015, and is a division of Cambridge Analytica. CA Commercial's registered agent for service of summons is The Corporation Trust Company, 1209 Orange Street, Corporation Trust Center, Wilmington, Delaware 19801. Cambridge Analytica is owned in part (19%) by SCL Elections Ltd, a British company owned by SCL Analytics Limited, which is owned in part by SCL Group. During the relevant time, Alexander Nix was CEO of both SCL Elections Ltd and Cambridge Analytica UK.

220. **Cambridge Analytica Holdings LLC** is a privately held limited liability company

---

<sup>11</sup> These entities were named in prior complaints consolidated into this docket. These entities are not named here pursuant to Title 11, § 362 of the United States Bankruptcy Code in addition to this court's order staying claims. *See* Pretrial Order No. 5: Scheduling at 1, ECF No. 103 ("The case is stayed as to the Cambridge Analytica defendants pending the outcome of the parties' request of the bankruptcy court for relief from the automatic stay.").



organized under the laws of the State of Delaware, incorporated on May 9, 2014. Cambridge Analytica Holdings, LLC's registered agent for service of summons is The Corporation Trust Company, 1209 Orange Street, Corporation Trust Center, Wilmington, Delaware 19801. According to the *Guardian*, hedge fund billionaire Robert Mercer funded CA Holdings, which created and initially ran Cambridge Analytica.<sup>12</sup>

221. **Cambridge Analytica Limited** is a British-registered company headquartered in London, England with U.S. offices located in New York, New York and Washington, D.C.

222. **Cambridge Analytica (UK) Limited** is a British-registered company headquartered in London, England with U.S. offices located in New York, New York and Washington, D.C. Prior to changing its name, Cambridge Analytica (UK) Limited was formerly registered as SCL USA Limited.

223. **Cambridge Analytica Political LLC** ("CA Political") is a privately held limited liability company organized under the laws of the State of Delaware, incorporated on January 21, 2015, and is a division of Cambridge Analytica. CA Political's registered agent for service of summons is The Corporation Trust Company, 1209 Orange Street, Corporation Trust Center, Wilmington, Delaware 19801.

224. Cambridge Analytica, CA Political and CA Commercial all share the same website: <https://cambridgeanalytica.org>. According to Cambridge Analytica's website, CA Political and CA Commercial are Divisions of Cambridge Analytica LLC. Upon information and belief, CA Holdings is a shell holding company for shares of Cambridge Analytica, CA Political and CA Commercial.

225. **SCL Elections Limited** is a British company incorporated on October 17, 2012. Its address is listed as c/o PFK Littlejohn, chartered accountants located at 1 Westferry Circus, Canary Wharf, London, E14 4HD, United Kingdom. Alexander Nix is listed as a director of SCL Elections and the ultimate controlling party as of the end of 2015.

226. **SCL Group Limited**, formerly known as Strategic Communications Laboratories Ltd, is a British company registered with the UK Companies House in 2005. Its headquarters are located at 55

---

<sup>12</sup> Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, *Guardian* (Mar. 17, 2018), <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.



New Oxford Street, London, WC1A 1BS. SCL Group Limited also has multiple U.S. affiliates, including SCL Group Inc. with offices in New York located at 597 5th Avenue, 7th Floor, New York, New York, 10036, and SCL USA Inc. with offices in Washington, D.C. located at 1901 Pennsylvania Avenue, N.W., Washington, D.C. 20006.

227. **SCL USA Inc.** is a privately held company incorporated under the laws of the State of Delaware, incorporated on April 22, 2104, and is a wholly owned subsidiary of SCL Elections. Its address is 597 5th Avenue, 7th Floor, New York, New York 10017 and its registered agent for service of summons is Erisedentagent, Inc., 1013 Centre Road, Suite 403S, Wilmington, Delaware 19805. Alexander Nix is SCL USA Inc.’s CEO. SCL USA is the alter ego of SCL Group.

**E. Other Non-Defendant Co-Conspirator**

228. **Global Science Research Limited** was a United Kingdom company that harvested and sold the private information of social media users for profit. On information and belief, Global Science Research Limited (“GSR”) did significant business in California, but has since dissolved. Its successors in interest are unknown at this time.

#### **IV. FACTUAL BACKGROUND**

**A. Facebook’s Transition from Social Media Company to Data Broker**

229. Facebook started as a user-driven experience. Users were comfortable sharing information about themselves on the social media platform in part because they believed they were sharing their content and information with the connections they selected, and that they controlled how their content and information was shared.

230. Indeed, millions of Facebook users joined Facebook before 2007, when Facebook launched the Facebook Platform—which allowed Apps on the user interface—and opened the website to search-engine indexing. Even after Facebook began allowing Apps to access user information and search engines to index user profiles, Facebook promoted the site as a place where users could connect with friends and family. Facebook recognizes this in its mission statement: “People use Facebook to stay connected with friends and family, to discover what’s going on in the world, and to share and

express what matters to them.”<sup>13</sup>

231. Since its inception, Facebook has faced a profound conflict of interest. In order to generate revenue, the Company has opted to monetize its platform and incorporate advertising. Facebook’s revenue thus comes principally from entities wishing to target Facebook’s users. To better target users, advertisers want access to as much information about users as Facebook will provide them.

232. Yet it is clear that users would not engage on the platform without protection of their privacy. For this reason, Facebook represents to users that they control their content and information, and that it will not give advertisers access to users’ content and information without users’ consent. Facebook expressly promises users they possess “the power to control exactly who can see the information and content they share.”<sup>14</sup>

233. At the same time, Facebook continually tested the limits of what user content and information can be shared publicly in order to attract advertisers who will pay to target users. On many occasions over the years, when Facebook unilaterally instituted changes which diminished user privacy, users and privacy watchdogs resisted. For example, in 2006, Facebook introduced a feature called “News Feed” without notice or consent to users. That feature revealed some of users’ information in a daily feed to Friends. In reaction more than a million users joined protest groups. Others protested outside Facebook’s Silicon Valley headquarters. “We did a bad job of explaining what the new features were and an even worse job of giving you control over them,” Zuckerberg conceded at the time.<sup>15</sup> Thus Facebook searched for a way to make user content and information available to advertisers without letting users see how it was happening.

---

<sup>13</sup> *Mission Statement*, Facebook Newsroom, <https://newsroom.fb.com/company-info/> (last visited Feb. 19, 2019).

<sup>14</sup> *E.g., Facebook Redesigns Privacy*, Facebook Newsroom (May, 26, 2010) <https://newsroom.fb.com/news/2010/05/facebook-redesigns-privacy/>; see Ryan Nakashima, *Promises, promises: Facebook's history with privacy*, Phys.Org (Mar. 30, 2018), <https://phys.org/news/2018-03-facebook-history-privacy.html>.

<sup>15</sup> Jessica Guynn, *Facebook's Mark Zuckerberg has promised to protect user privacy before. Will this time be different?*, USA Today (April 10, 2018), <https://www.usatoday.com/story/tech/2018/04/10/facebook-mark-zuckerberg-has-promised-protect-user-privacy-before-time-different/502603002/>.

# 1. Facebook Encouraged User Engagement to Drive Advertising Revenues.

234. User engagement is a key financial metric for Facebook. User presence alone is not the compelling driver of revenue; it is also how actively users engage on the Facebook user platform, and in what forums. “Engagement” or “user engagement” on Facebook is calculated by counting users’ actions relating to content posted on Facebook’s platform. For example, users may “Like” a Post, click on a link or comment on an image. Analysts predict Facebook’s future revenues based on user engagement rates and other key metrics, and this drives Facebook’s share price.<sup>16</sup>

235. Because of its importance to Facebook’s financial performance, Facebook precisely tracks user engagement both on and off Facebook’s platform, reporting monthly active users (“MAUs”),<sup>17</sup> daily active users (“DAUs”)<sup>18</sup> and mobile MAUs (“Mobile MAUs”).<sup>19</sup> Facebook’s efforts to increase user engagement have been remarkably successful.<sup>20</sup> In 2012, ahead of its public offering, Facebook stated that it had 901 million MAUs, 526 million DAUs, and 500 million Mobile MAUs.<sup>21</sup>

---

<sup>16</sup> See Paige Cooper, *41 Facebook Stats That Matter to Marketers in 2019*, Hootsuite (Nov. 13, 2018), <https://blog.hootsuite.com/facebook-statistics/> (“Facebook’s focus on meaningful connection has driven rising user engagement, which in turn drives monetization for the platform.”); Adam Levy, *The 4 Pillars of Facebook’s Growing Ad Revenue*, The Motley Fool (May 9, 2017), <https://www.fool.com/investing/2017/05/09/the-4-pillars-of-facebooks-growing-ad-revenue.aspx> (noting that “growing engagement is a sign Facebook will continue to see ad revenue growth even as it faces ad load saturation.”).

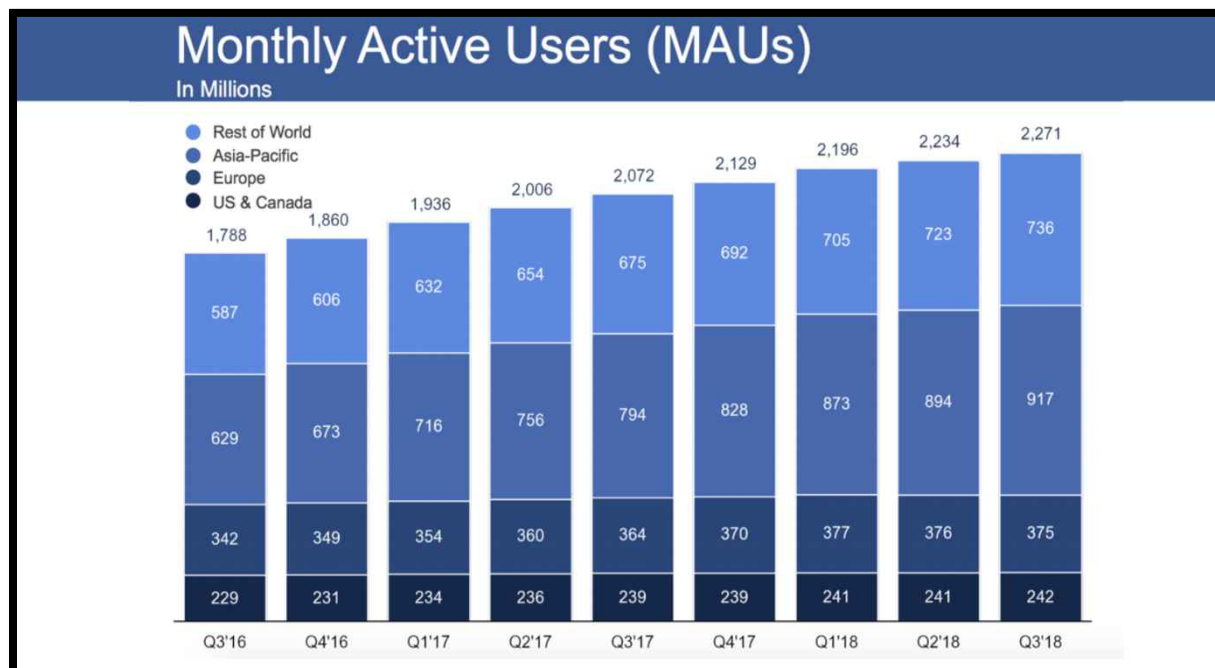
<sup>17</sup> Facebook Inc., Amended Registration Statement (Form S-1/A), at 88 (May 16, 2012), <https://www.sec.gov/Archives/edgar/data/1326801/000119312512235588/d287954ds1a.htm> [hereinafter *Facebook Form S-1/A*] (defining a MAU as “a registered Facebook user who logged in and visited Facebook through our website or a mobile device, or took an action to share content or activity with his or her Facebook friends or connections via a third-party website that is integrated with Facebook, in the last 30 days as of the date of measurement.”).

<sup>18</sup> *Id.* at 49 (defining DAU as “a registered Facebook user who logged in and visited Facebook through our website or a mobile device, or took an action to share content or activity with his or her Facebook friends or connections via a third-party website that is integrated with Facebook, on a given day.”)

<sup>19</sup> *Id.* at 50 (defining a Mobile MAU as “a user who accessed Facebook via a mobile app or via mobile-optimized versions of our website such as m.facebook.com, whether on a mobile phone or tablet such as the iPad, during the period of measurement.”).

<sup>20</sup> Phil Simon, *Facebook: The New King of Data Brokers*, Wired, <https://www.wired.com/insights/2014/10/facebook-king-data-brokers/> (last visited Feb. 20, 2019).

<sup>21</sup> Facebook Form S-1/A, *supra* note 17, at 88.



236. Facebook also tracks user engagement more minutely and reports it to investors. For example, in the first quarter of 2012, ahead of its Initial Public Offering (“IPO”), Facebook tracked 3.2 billion Likes and Comments by users each day, reporting that users were uploading 300 million photos each day.<sup>22</sup> These numbers have greatly increased over time.<sup>23</sup> To calculate these numbers, Facebook engages in extensive analysis of user activity on its user platform, reporting it to advertisers in market analytic reports.<sup>24</sup> Facebook even provides “real-time analytics” which allows advertisers to view live users engagement with advertisements.<sup>25</sup> These real-time analytics are marketed by Facebook as tools

<sup>22</sup> *Id.*

<sup>23</sup> Brittany Darwell, *Facebook platform supports more than 42 million pages and 9 million apps*, Adweek (Apr. 27, 2012), <https://www.adweek.com/digital/facebook-platform-supports-more-than-42-million-pages-and-9-million-apps>.

<sup>24</sup> *Marketing Analytics - Success Through Analysis*, WordStream, <https://www.wordstream.com/marketing-analytics> (last visited Feb. 20, 2019).

<sup>25</sup> Matthew Creamer, *Facebook Explains Its New Real-Time Insights*, AdAge (Mar. 15, 2012), <https://adage.com/article/digital/facebook-explains-real-time-insights/233320/>; Greg Finn, *PageLever Now’ Launches Real-time Facebook Post Analytics & Management Tool*, Marketing Land (Nov. 1, 2012), <https://marketingland.com/pagelever-now-launches-real-time-facebook-post-analytics-management-tool-25576>.

for advertisers to increase sales.

237. In May 2015, Facebook stated to investors: “Our financial performance has been and will continue to be significantly determined by our success in adding, retaining, and engaging active users. . . . If people do not perceive our products to be useful, reliable, and trustworthy, we may not be able to attract or retain users or otherwise maintain or increase the frequency and duration of their engagement.”<sup>26</sup>

## **2. User Engagement Increased When Facebook Gave App Developers Users’ Content and Information**

238. A key driver of user engagement for Facebook was the addition of Apps to its platform. Starting in 2007, Facebook gave App Developers access to user content and information, encouraging them to build Apps to stimulate user engagement.<sup>27</sup>

239. To incentivize App Developers to develop Apps, Facebook paid App Developers not with cash, but in kind. This payment came in the form of users’ content and data, including content that was marked private. As the U.K. House of Commons Digital, Culture, Media and Sport Committee (“DCMS Committee”) explained in its Final Report, dated February 14, 2019 (“DCMS Report”):

“Data reciprocity” is the exchange of data between Facebook and apps, and then allowing the apps’ users to share their data with Facebook. As Ashkan Soltani told us, Facebook’s business model is “to monetise data” which evolved into Facebook paying app developers to build apps, using the personal information of Facebook’s users. To Mr Soltani, Facebook was and is still making the following invitation: “Developers, please come and spend your engineering hours and time in exchange for access to user data.”<sup>28</sup>

240. Facebook users’ content and information, including associated metadata, is highly valuable to both Facebook and the third parties—including Apps, Whitelisted Apps, Business Partners, and advertisers—with whom Facebook unlawfully shared this content and information. As Cambridge

---

<sup>26</sup> Facebook Form S-1/A, *supra* note 17, at 12.

<sup>27</sup> *Platform is here*, Facebook (Jun 1, 2007), <https://www.facebook.com/notes/facebook/platform-is-here/2437282130/>.

<sup>28</sup> U.K. House of Commons, Digital, Culture, Media and Sport Committee, *Disinformation and ‘Fake News’: Final Report*, 2017-19, HC 1791, (“DCMS Report”) (Feb. 14, 2019), at ¶ 103, <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf>.

Analytica whistleblower Brittany Kaiser stated, “[c]orporations like Google, Facebook, Amazon, all of these large companies, are making tens or hundreds of billions of dollars off of monetising people’s data.”<sup>29</sup> Kaiser noted that because “data is probably your most valuable asset,” “[i]ndividuals should be able to monetise their own data—that’s their human value—not to be exploited.”<sup>30</sup>

241. The value of such data, including Facebook users’ content and information, is not hypothetical. Facebook itself demonstrated that with its “Facebook Research” App, through which “Facebook secretly paid users, aged between 13 and 25, up to \$20 in gift cards per month to sell their phone and website activity.”<sup>31</sup>

242. In an internal Facebook email, Mark Zuckerberg roughly calculated the value of allowing Apps to read user content at ten cents per user per year.<sup>32</sup>

243. Moreover, sharing user content and information with third parties was enormously valuable to Facebook. In fact, “sharing private user data with third parties was one of the core tactics that contributed to Facebook’s success.”<sup>33</sup> In 2009—notably, one year after Sandberg was hired as COO and the first year in which Facebook turned a profit—Facebook introduced third-party games such as Zynga’s FarmVille, and enabled the games to “leverag[e] friends lists to boost the population of players.”<sup>34</sup> This was highly profitable to Facebook, in that “30 percent of Zynga’s in-game advertising and purchase revenues went to Facebook” and, in the year before its IPO, “Zynga alone accounted for twelve percent of Facebook’s revenue.”<sup>35</sup> Consequently, “Zynga’s ability to leverage friends lists contributed to an insight: giving third-party developers access to friends lists would be a huge positive for Facebook’s business.”<sup>36</sup>

---

<sup>29</sup> McNamee, *supra* note 302, at 197.

<sup>30</sup> *Id.*

<sup>31</sup> DCMS Report, *supra* note 28, ¶ 115.

<sup>32</sup> *Id.* ¶ 97.

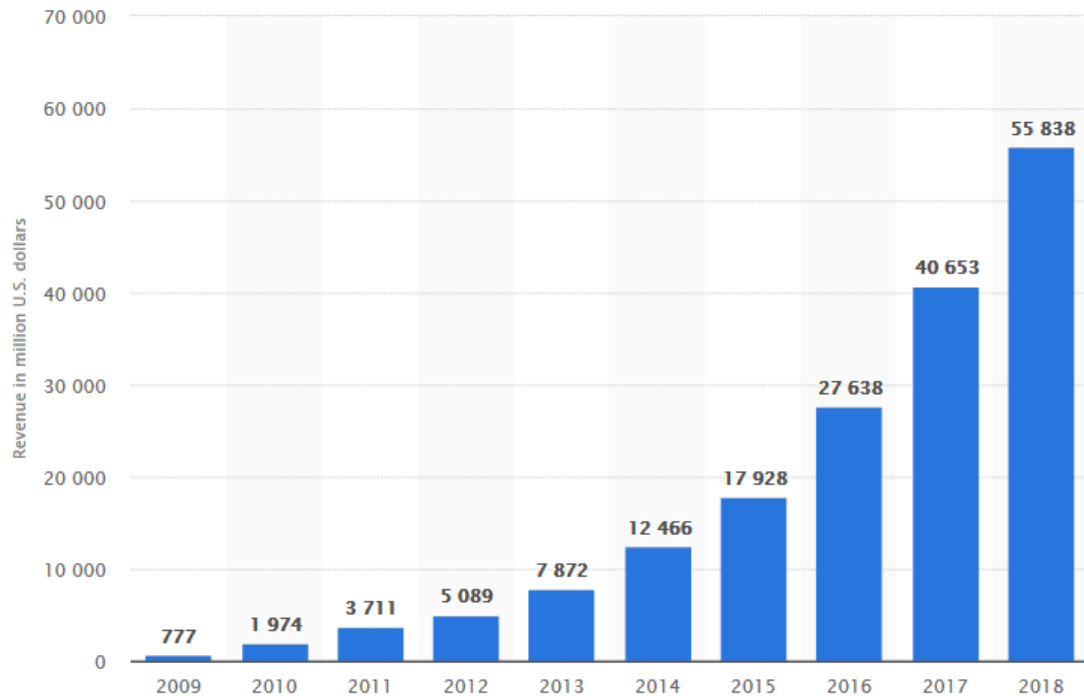
<sup>33</sup> McNamee, *supra* note 302 at 184.

<sup>34</sup> *Id.*

<sup>35</sup> *Id.*

<sup>36</sup> *Id.*

244. Facebook’s sharing of user content and information with third parties—including Apps, Business Partners, Whitelisted Apps, and advertisers—has resulted in “explosive revenue growth,” as shown in the chart below.<sup>37</sup>



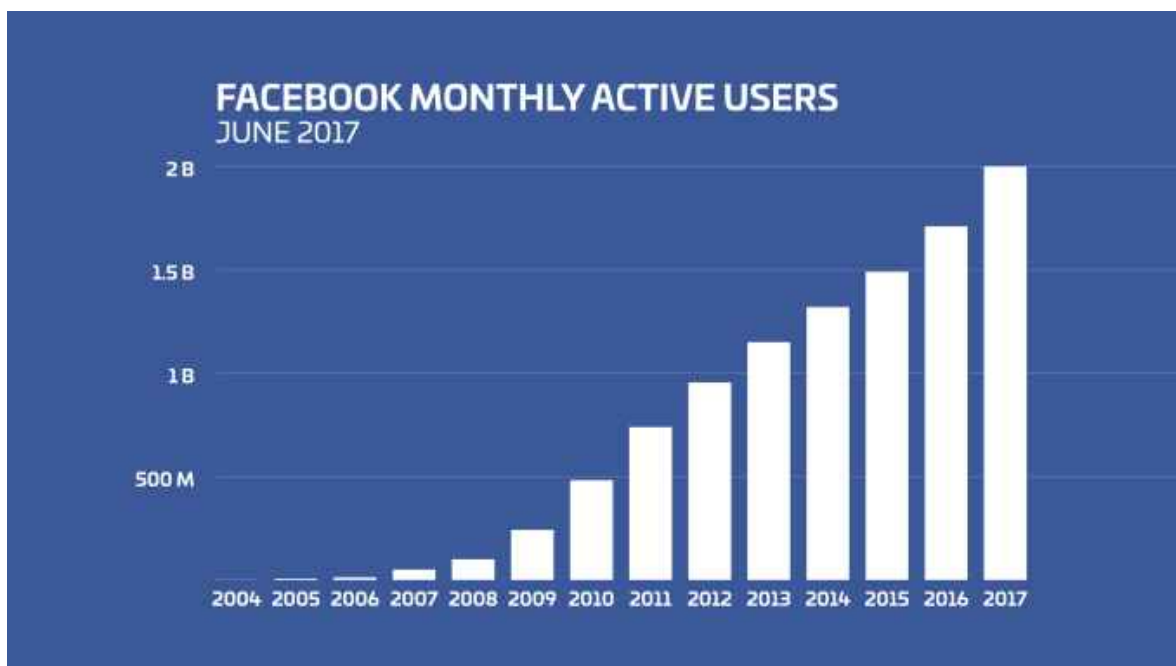
© Statista 2019

245. Facebook’s sharing of user content and information has resulted in explosive user growth as well. As demonstrated in the below diagram, Facebook’s user growth was relatively flat until 2007, when Facebook launched its platform and started secretly sharing user content and information with its Business Partners. User growth then skyrocketed.<sup>38</sup>

<sup>37</sup> Facebook’s annual revenue from 2009 to 2018 (in million U.S. dollars), Statista, <https://www.statista.com/statistics/268604/annual-revenue-of-facebook/> (last visited Feb. 22, 2019).

<sup>38</sup> Josh Constance, *Facebook now has 2 billion monthly users ... and responsibility*, TechCrunch, <https://techcrunch.com/2017/06/27/facebook-2-billion-users/> (last visited Feb. 22, 2019); Gabriel J.X. Dance, Nicholas Confessore, and Michael LaForgia, *Facebook Gave Device Makers Deep Access to Data on Users and Friends*, N.Y. Times (June 3, 2018), <https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html>.





246. Facebook’s partnership with Apps was effective in building the platform at minimal out-of-pocket cost to Facebook. With a more developed User Platform, Facebook’s active user numbers steadily increased, as did users’ activity on Facebook. “I would expect that next year, people will share twice as much information as they share this year, and next year, they will be sharing twice as much as they did the year before,” Zuckerberg predicted in 2008.<sup>39</sup>

247. Apps like the wildly popular FarmVille were remarkably successful and attracted millions of users. At its peak in March 2010, FarmVille had 83.76 million monthly active users.<sup>40</sup> Daily active users of the App alone peaked at 34.5 million a year later.<sup>41</sup>

248. By April 2012, there were more than 9 million Apps on Facebook and 42 million

<sup>39</sup> Anita Balakrishnan, Sara Salinas, & Matt Hunter, *Mark Zuckerberg has been talking about privacy for 15 years — here's almost everything he's said*, Cnbc (Mar. 21, 2018), <https://www.cnbc.com/2018/03/21/facebook-ceo-mark-zuckerbergs-statements-on-privacy-2003-2018.html>.

<sup>40</sup> Dean Takahashi, *Zynga’s CityVille becomes the biggest-ever app on Facebook*, VentureBeat (Jan. 3, 2011), <https://venturebeat.com/2011/01/03/zyngas-cityville-becomes-the-biggest-ever-app-on-facebook/>.

<sup>41</sup> *Id.*



“Pages.”<sup>42</sup> Facebook publicly reported that between January 1 and March 31, 2012, more than 300 million photos were uploaded to the site each day. Users also generated an average 3.2 billion Likes<sup>43</sup> and comments each day in the first quarter of 2012—up from 2.7 billion per day in Q4 2011. By this time, Facebook boasted more than 125 billion Friend connections between its 901 million monthly active users.<sup>44</sup> However, Facebook still was not capturing revenue at a level that satisfied investors.

249. In 2012, Facebook took the company public.<sup>45</sup> Following its IPO which, at the time, was the biggest Internet- based technology IPO in history, Facebook’s share price plummeted. While there were some technical difficulties on the day of the IPO, most analysts viewed Facebook’s anemic average revenue per user (“ARPU”) as the problem.<sup>46</sup> This disastrous experience encouraged Facebook to accelerate changes to its business model to further favor advertisers, not its users. Facebook concluded that its initial “social networking” business model needed to change, and quickly, if the Company were to survive.

250. Zuckerberg decided it was time to choose between users’ privacy and the Company’s revenues. In an internal email written by Zuckerberg to his senior executive team in 2012, Zuckerberg debated this conflict of interest, and firmly picked a winner – Facebook. As Zuckerberg wrote in the email:

We’re trying to enable people to share everything they want, and to do it on Facebook. Sometimes the best way to enable people to share something is to have a developer build a special purpose app or network for that type of content and to make that app social by having Facebook plug into it. ***However, that may be good for the world but it’s not good***

---

<sup>42</sup> A “Page” is a Facebook profile, often public, that anyone, including artists, fan-generated community pages, public figures, businesses, and entertainers can set up, and which other users can Like. A Page is distinct from a user profile. Brittany Darwell, *Facebook platform supports more than 42 million pages and 9 million apps*, Adweek (Apr. 27, 2012), <https://www.adweek.com/digital/facebook-platform-supports-more-than-42-million-pages-and-9-million-apps/>.

<sup>43</sup> Facebook Form S-1/A, *supra* note 17, at 97 (discussing “Likes” as electronic indications that a user approved, or at least reacted to, a post, photo, experience, article or other content on Facebook).

<sup>44</sup> *Id.* at 1.

<sup>45</sup> Emil Protalinski, *Facebook’s IPO by the numbers*, ZDNet (Feb. 1, 2010), <https://www.zdnet.com/article/facebook-ipo-by-the-numbers/>.

<sup>46</sup> See, e.g., Paul La Monica, *5 reasons to not 'like' Facebook's IPO*, CNN Money (May 4, 2012), <https://money.cnn.com/2012/05/04/markets/thebuzz/index.htm?iid=EL>.

*for us unless people also share back to Facebook and that content increases the value of our network. So ultimately, I think the purpose of platform—even the read side—is to increase sharing back into Facebook.*<sup>47</sup>

251. Facebook launched an all-out offensive to monetize user engagement by sharing what users shared with third parties. The problem with these initiatives is that Facebook did not clearly explain to users the changes it was making to its platform and how users' content and information would be funneled to third parties paying Facebook for access to it.

252. What Zuckerberg refers to in this email as the "read side" is actually the part of the platform accessible to Facebook's Business Partners and App Developers. This was different than the platform users experienced. The fact that he refers to "read side" as differing from the user platform reflects the two sides of the Facebook experience. One side was the platform on which users engaged (the "User Platform"); the back end of the platform, the "read side," funneled users' content to Facebook's Business Partners and App Developers.

253. First, the Company turned Likes into product endorsements; next, it launched a marketplace for content and information about the people on its platform.<sup>48</sup> Users may have still believed that Facebook was a social network where they could connect with people they knew, but Facebook's true focus was to sell the information Facebook was collecting about its users. These initiatives greatly increased users' deanonymization and violated their privacy settings.

254. For example, starting in 2012, Facebook released its "Custom Audiences" feature to advertisers, which allows advertisers to directly target specific Facebook users with advertisements.<sup>49</sup> Using this feature, advertisers could upload a spreadsheet with user identifying information, including email, phone number, Mobile Advertiser ID, first name, last name, zip/postal code, city, state/province, country, date of birth, year of birth, gender, age, Facebook App User ID, and Facebook Page User IDs.

---

<sup>47</sup> DCMS Report, *supra* note 28, ¶ 105.

<sup>48</sup> Rebecca Greenfield, *2012: The Year Facebook Finally Tried to Make Some Money*, The Atlantic (Dec. 14, 2012), <https://www.theatlantic.com/technology/archive/2012/12/2012-year-facebook-finally-tried-make-some-money/320493/>.

<sup>49</sup> Brittany Darwell, *The Year in Facebook Advertising 2012*, Adweek (Dec. 31, 2012), <https://www.adweek.com/digital/the-year-in-facebook-advertising-2012/>.

255. Another key initiative of value to advertisers was the ability to surveil users' reactions in real time to content. For example, Facebook promotes an auto-play video function for all mobile and desktop users. This function causes videos to play automatically as users scroll through their News Feeds. Thus, as videos play automatically, Facebook increases users' engagement with video advertisements, which Facebook then reports to advertisers.<sup>50</sup>

256. In May 2014, Facebook announced new video marketing analytics that allowed advertisers to see "video views, unique video views, the average duration of the video view and audience retention."<sup>51</sup> "Average Duration of Video Viewed [w]as the total time spent watching a video divided by the total number of people who have played the video."<sup>52</sup> As recent reporting has shown, Facebook has the ability to see precisely how long each user is watching each video, and can report it to third parties in real time.<sup>53</sup>

257. Video views data provide rich information to advertisers about users, including what they like, dislike, and how long content can hold their interest. Videos are also wildly popular with Facebook users. In November 2015, Zuckerberg boasted on an earnings call with investors that Facebook users watched 8 billion videos per day.<sup>54</sup>

---

<sup>50</sup> Justin Lafferty, *Facebook announces international launch of auto-play video ads*, Adweek (May 20, 2014), <https://www.adweek.com/digital/facebook-announces-international-launch-of-auto-play-video-ads/>.

<sup>51</sup> Facebook Business, *Introducing Video Metrics*, Facebook (May 5, 2014), <https://www.facebook.com/business/news/Coming-Soon-Video-Metrics>.

<sup>52</sup> *How is the "Average Duration of Video Viewed" calculated?*, Facebook, <https://web.archive.org/web/20161001014809/https://www.facebook.com/business/help/community/question/?id=10104227902985423> (last visited Feb. 21, 2019).

<sup>53</sup> Suzanne Vranica, *Advertisers Allege Facebook Failed to Disclose Key Metric Error for More Than a Year*, Wall St. J. (Oct. 16, 2018), <https://www.wsj.com/articles/advertisers-allege-facebook-failed-to-disclose-key-metric-error-for-more-than-a-year-1539720524?mod=e2tw>; see also, *Letizia et al. v. Facebook, Inc.*, No. 16-cv-06232-JSW, Dkt. 165 at 10 (N.D. Cal. Filed Oct. 27, 2016) (Order denying in part Facebook's motion to dismiss and discussing allegations that Facebook inflated average time spent watching videos between 60-80 percent).

<sup>54</sup> Josh Constine, *Facebook Hits 8 Billion Daily Video Views, Doubling From 4 Billion In April*, TechCrunch (Nov. 4, 2015), [https://techcrunch.com/2015/11/04/facebook-video-views/?\\_ga=2.184710381.511973801.1549821477-1625503738.1539793011](https://techcrunch.com/2015/11/04/facebook-video-views/?_ga=2.184710381.511973801.1549821477-1625503738.1539793011) (last visited Feb. 21, 2019).

258. These are not the only tools Facebook employs to surveil users with the goal of monetizing that information. Facebook also tracks users through Social Plugins, such as the Facebook “like” or “Share” buttons. Only following the Cambridge Analytica scandal have users begun to learn the extent of this surveillance: “If those buttons are on the page, regardless of whether you touch them or not, Facebook is collecting data.”<sup>55</sup>

259. In addition to the Plugins, Facebook also uses Facebook Analytics such as Facebook Pixel (“Pixel”) in order “better understand how people use their services.” Pixel is a transparent image embedded into the webpage that collects data and transmits it to Facebook.<sup>56</sup> Facebook has promoted Pixel as an “analytics tool that allows you to measure the effectiveness of your advertising by understanding the actions people take on your website.”<sup>57</sup> Facebook reported that from April 9–16, 2018, “the Facebook Like button appeared on 8.4 million websites, the Share button appeared on 931k websites, and there were 2.2 million Facebook Pixels installed on websites.”<sup>58</sup>

260. Facebook also collects sensitive information on many App users regardless of whether App users log in through their Facebook accounts or whether they have a Facebook account. Facebook gathers this information through its Software Development Kits (“SDK”), which are available for mobile operating systems, including Apple and Android.<sup>59</sup> SDK is a software development tool that

---

<sup>55</sup> Allen St. John, *How Facebook Tracks You, Even When You're Not on Facebook*, Consumer Reports (Apr. 11, 2018), <https://www.consumerreports.org/privacy/how-facebook-tracks-you-even-when-youre-not-on-facebook/>.

<sup>56</sup> *Id.*

<sup>57</sup> *About Facebook Pixel*, Facebook Business, <https://www.facebook.com/business/help/553691765029382> (last visited Feb. 21, 2019).

<sup>58</sup> DCMS Report, *supra* note 28, ¶ 185.

<sup>59</sup> *See, e.g.*, with respect to Android, “Facebook’s SDK for Android allows app developers to integrate their apps with Facebook’s platform and contains a number of core components: Analytics, Ads, Login, Account Kit, Share, Graph API, App Events and App Links. . . . Facebook’s SDK also offers Analytics (data, trends, and aggregated audience insights about the people interacting with the app), as well as Ads and reading and writing to Facebook’s Graph API.” *How Apps on Android Share Data with Facebook (even if you don’t have a Facebook account)*, Privacy International (Dec. 2018), <https://privacyinternational.org/sites/default/files/2018-12/How%20Apps%20on%20Android%20Share%20Data%20with%20Facebook%20-%20Privacy%20International%202018.pdf>.

helps App Developers build Apps for specific operating systems.<sup>60</sup> Facebook collects this information the moment App Users begin sharing information with the App.

261. A study conducted between August and December 2018 by Privacy International found that 61 percent of the Apps it tested shared App users' information with Facebook. The Wall Street Journal has since found "11 popular Apps" available on both Apple and Google phones "have also been sharing sensitive data entered by users."<sup>61</sup> This includes six of the top 15 health and fitness Apps available in Apple's iOS store. For example, "Flo Health Inc.'s Flo Period & Ovulation Tracker, which claims 25 million active users, told Facebook when a user was having her period or informed the App of an intention to get pregnant, the tests showed."<sup>62</sup> In the case of Flo Health, the sensitive information sent to Facebook included a "unique advertising identifier" that can be matched to a device or profile.<sup>63</sup>

262. Facebook uses information collected through its SDKs to target users with Facebook ads. Facebook does not provide users with the option to stop the company from collecting their information through SDKs.

### **3. Facebook's Partnerships with Data Brokers Resulted in Aggregated, Deanonimized User Information**

263. At the same time that Facebook was working with App Developers to expand the Facebook platform, Facebook instituted a more sophisticated method for third parties to target users. By combining users' content and information on Facebook with data Facebook acquired from data brokers, Facebook was able to offer its advertisers and Business Partners a way to pinpoint their user audience. This significantly exposed users to deanonymization.

264. For example, in April 2013, Facebook partnered with data brokerage firm Datalogix to assess the impact of Facebook advertisements on users' purchases outside of Facebook. Datalogix provided Facebook with datasets that it ultimately associated with specific Facebook users. By

---

<sup>60</sup> *Id.*

<sup>61</sup> Sam Schechner, *You Give Apps Sensitive Personal Information. Then They Tell Facebook*, The Wall Street Journal (Feb. 22, 2019) <https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook>.

<sup>62</sup> *Id.*

<sup>63</sup> *Id.*

matching the information provided by data brokers with the content and information that Facebook curates on its platforms, Facebook was able to create digital dossiers containing information about millions of individuals—users and nonusers alike. These dossiers include names, addresses, health information, information about your neighbors, inclinations and proclivities. All of these are used to predict future behavior, as described below. Facebook did not tell users about these dossiers.

265. As Facebook has continued to build its digital dossiers, it has forged relationships with the many data brokers who provide data about individuals from across the world, including:

- Acxiom (data from Australia, France, Germany, the U.K. and the U.S.);
- Acxiom Japan;
- CCC Marketing (data from Japan);
- Epsilon (data from the U.S.);
- Experian (data from Australia, Brazil, U.K. and U.S.);
- Oracle Data Cloud (formerly Datalogix) (data from U.K. and U.S.); and
- Quantum (data from Australia)

266. Facebook has worked with these data brokers to collect information about consumers through public records, loyalty card programs, surveys, and independent data providers to be incorporated into its digital dossiers.

267. Facebook has then used these dossiers as filters through which advertisers could more precisely target users.<sup>64</sup>

268. As of 2016, Facebook was collecting more than 52,000 unique data points to classify users and providing at least 29,000 targeted categories for advertisers to choose from. Nearly 600 of these categories were provided by third-party data brokers.<sup>65</sup> This “data” is not only clinical information like date of birth; it is rich in personal information that taken together describes individuals and provides support for Facebook and advertisers to draw inferences about future behavior. It is this supposedly predictive quality of the aggregated data that is so valuable to Facebook’s advertisers.

---

<sup>64</sup> Tim Peterson, *Facebook Will Remove Advertisers’ Other Third-Party Data Option, But Loopholes, Questions Remain*, DigiDay (Apr. 6, 2018), <https://digiday.com/marketing/facebook-will-remove-advertisers-third-party-data-option-loopholes-questions-remain/>.

<sup>65</sup> Julia Angwin, Surya Mattu, & Terry Parris Jr., *Facebook Doesn’t Tell Users Everything It Really Knows About Them*, ProPublica (Dec. 27, 2016), <https://www.propublica.org/article/facebook-doesnt-tell-users-everything-it-really-knows-about-them>.

Through App partnerships, it now includes information like users' ovulation.

269. Facebook does not disclose to users that it matches content and information users reveal on the Facebook platform with information provided through data brokers collected from a myriad of sources to build digital profiles of them. Indeed, a March 2018 study shows 74% of Facebook users did not think their data was being collected when they were not logged into Facebook.<sup>66</sup>

#### **4. The Wealth of Data About Users Enabled Highly Invasive Forms of Psychographic Marketing**

270. The availability of thousands of highly personal data points about individuals has facilitated invasive and targeted marketing called "psychographic marketing." Psychographic marketing exploits a user's fears, feelings, and values by appealing to a person's motives and instincts in order to influence a person's emotions, mood, and behavior.

271. To be effective, psychographic marketing requires a de-anonymized target audience through which the marketer can pinpoint personality traits for manipulation, exploiting deeply ingrained values and beliefs gleaned from an information-rich dossier such as those compiled by Facebook.

272. And although Facebook promised its users it would not allow advertisers to target them personally, Facebook's financial motivations prevailed. By granting access to user data to third parties and permitting those third parties to analyze and plug in the results of their analysis, Facebook exposed its users to a level of manipulation far beyond mere targeted marketing.

273. Recognizing the importance of anonymity for the privacy and security of users who trusted Facebook with an unprecedented amount of personal content and information, Facebook expressly promised users that it would remove identifying information from content delivered to advertisers:

When we deliver ads, we do not share your information (information that personally identifies you, such as your name or contact information) with advertisers unless you give us permission. We may provide advertisers with information when we have removed

---

<sup>66</sup> Paul Hitlin & Lee Rainie, *Facebook Algorithms and Personal Data*, Pew Research Center (Jan. 16, 2019), <http://www.pewinternet.org/2019/01/16/facebook-algorithms-and-personal-data/>.



your name and other personally identifiable information, or combined it with other information so that it no longer personally identifies you.”<sup>67</sup>

274. To the contrary, Facebook collection of users’ content and information combined with other data sources enabled personalized psychographic marketing. Facebook’s drive to increase user engagement and the lure of psychographic marketing campaigns collide with the Cambridge Analytical Scandal in which Kogan’s App administered a test which was designed to determine users’ OCEAN scores.

275. OCEAN refers to a measure of five basic personality traits: Openness, Conscientiousness, Extroversion, Agreeableness, and Neuroticism.<sup>68</sup> From the data Kogan collected about these traits, Cambridge Analytica was able to extrapolate tendencies, interests and vulnerabilities that drove manipulative messaging of a much more invasive and private sort than typical commercial targeting seeking to drive consumer behavior through, for example, an interest in shoes.

276. Investigations triggered by the Cambridge Analytica Scandal have revealed that it was not just Kogan and Cambridge Analytica that purchased Facebook user content and information with the goal of using these manipulative marketing tactics. The DCMS Report revealed that thousands of other Apps mined Facebook for such user information.<sup>69</sup> Politicians, advertisers and even foreign nations all engaged in psychographic marketing on Facebook using Facebook user content and information that had been disclosed to third parties without users’ authorization.

277. As *Wired* stated: “One minute you’re filling out an App survey; the next, your answers are informing the psychographically targeted ads of a political campaign. No one signed up for that.”<sup>70</sup>

278. These changes in Facebook’s business model have turned the Company into one of the

---

<sup>67</sup> *Data Use Policy*, Facebook, , <https://www.facebook.com/about/privacy> (last updated Nov. 15, 2013) [<https://web.archive.org/web/20131113201958/https://www.facebook.com/about/privacy>].

<sup>68</sup> Erin Brodwin, *Here’s the personality test Cambridge Analytica had Facebook users take*, Business Insider (Mar. 19, 2018), <https://www.businessinsider.com/facebook-personality-test-cambridge-analytica-data-trump-election-2018-3>.

<sup>69</sup> DCMS Report, *supra* note 28, ¶ 123.

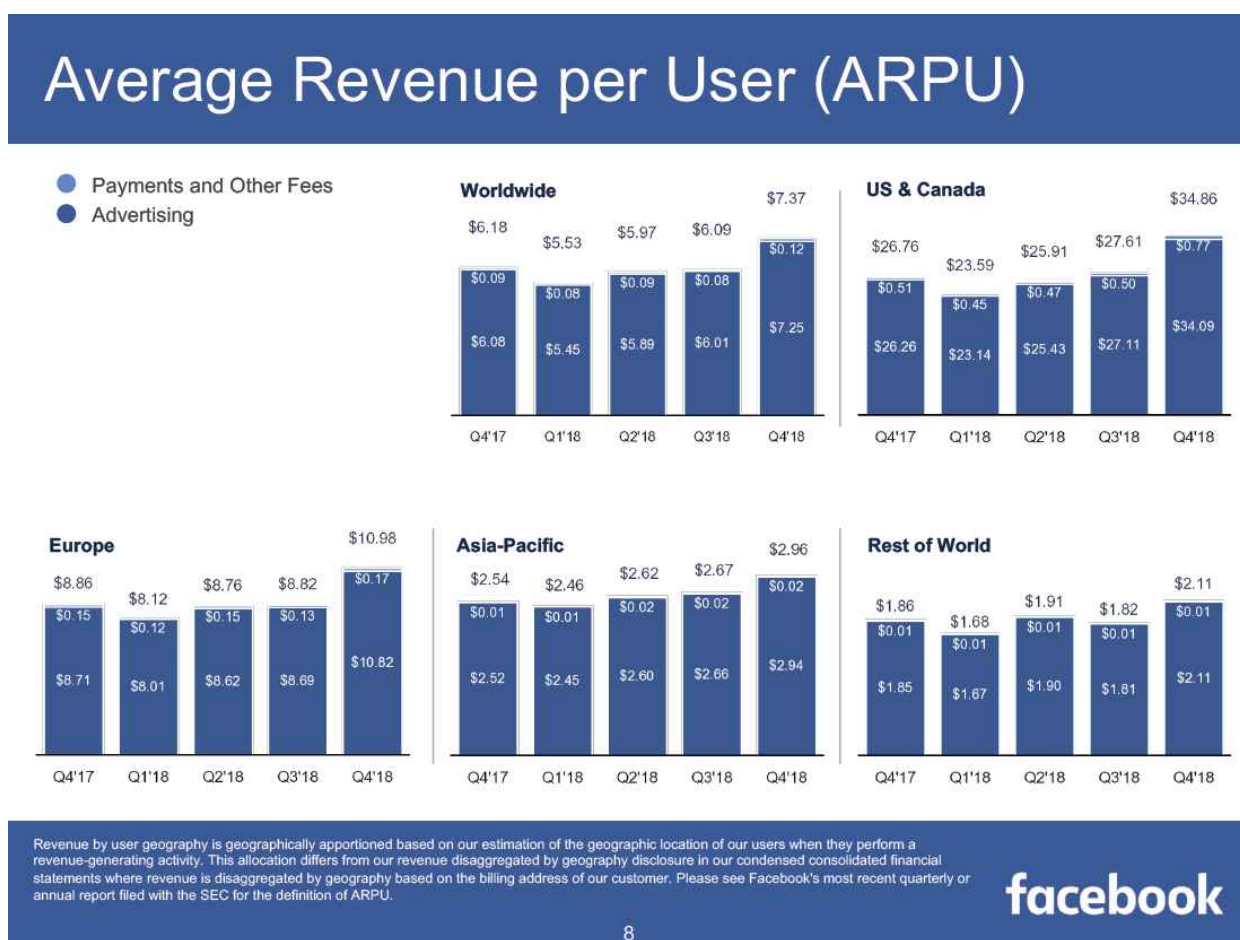
<sup>70</sup> Brian Barrett, *Facebook Owes You More Than This*, *Wired* (Mar. 19, 2018), <https://www.wired.com/story/facebook-privacy-transparency-cambridge-analytica/>.



most powerful entities in the world. Facebook reported 2.32 billion MAUs and 1.52 billion DAUs in the fourth quarter of 2018. Although Facebook's revenues were over \$16.9 billion for that quarter.<sup>71</sup>

279. These numbers are broken down by Facebook in metrics called Average Revenue Per User, or ARPU. ARPU is calculated in part by an assessment of the "quality" of those users. More engaged users are more valuable to Facebook and higher quality than less engaged ones, because of the amount of information they provide and make available to advertisers.

280. In 2018, ARPU for users in Canada and the United States was \$34 per user.<sup>72</sup>

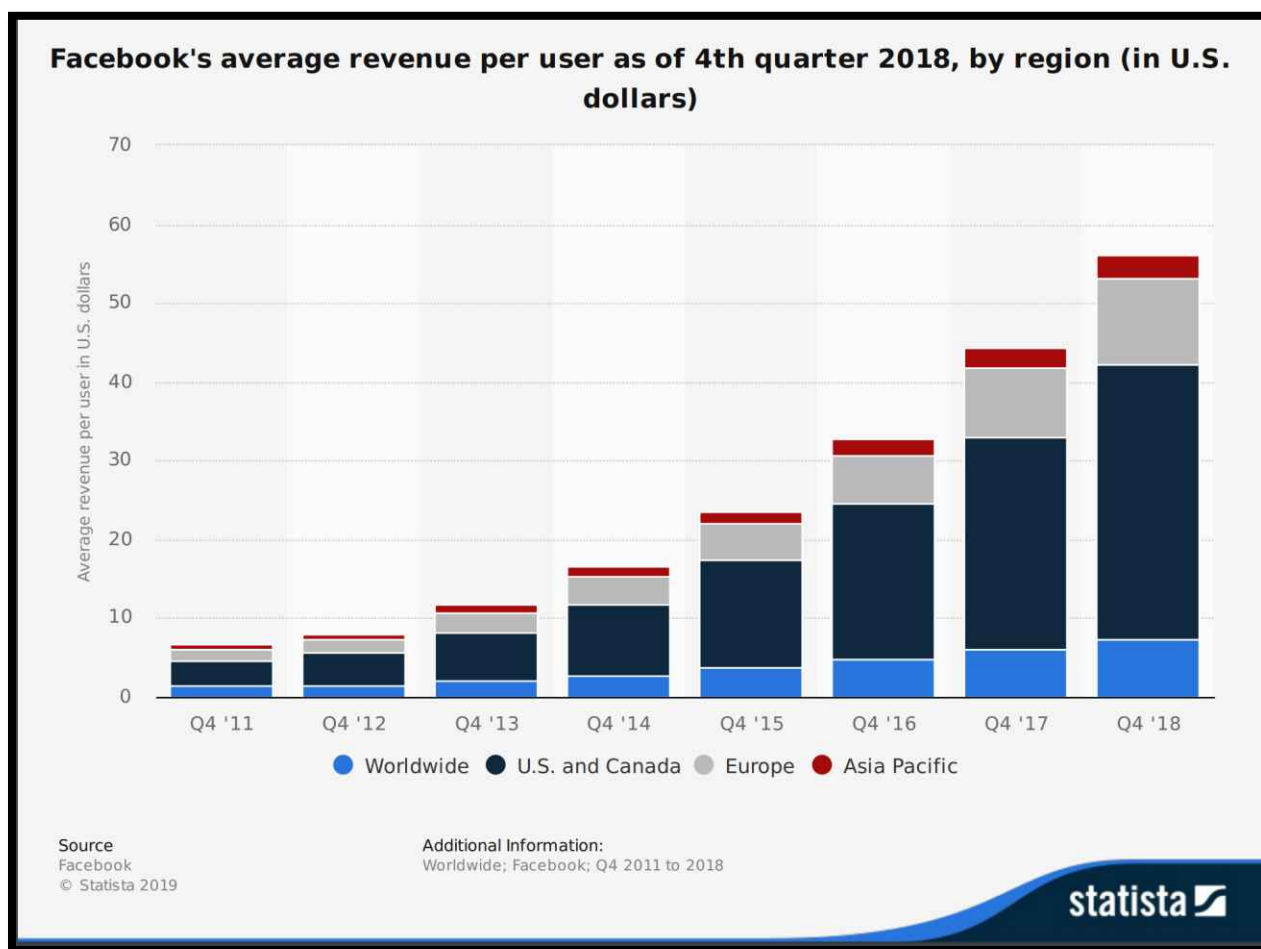


281. This extraordinary growth rests upon Facebook's annual revenues of \$55 billion year.<sup>73</sup>

<sup>71</sup> *Facebook Q4 2018 Results*, Facebook (Jan. 30, 2019), [https://s21.q4cdn.com/399680738/files/doc\\_financials/2018/Q4/Q4-2018-Earnings-Presentation.pdf](https://s21.q4cdn.com/399680738/files/doc_financials/2018/Q4/Q4-2018-Earnings-Presentation.pdf).

<sup>72</sup> *Id.*

<sup>73</sup> *Facebook - Statistics & Facts*, Statista, <https://www.statista.com/topics/751/facebook/> (last visited Feb. 21, 2019) (containing metrics relating to Facebook's astronomical growth).



282. Corresponding with Facebook's increased ARPU, Facebook's share prices also grew exponentially.<sup>74</sup> Before the Cambridge Analytica Scandal, increasing revenues drove the stock to a share price as high as \$242:

<sup>74</sup> Benjamin Rains, *User Growth, ARPU & Other Key Q3 Facebook (FB) Estimates*, Nasdaq (Oct. 29, 2018), <https://www.nasdaq.com/article/user-growth-arpu-other-key-q3-facebook-fb-estimates-cm1045438>.



**B. Facebook Made It Difficult and Sometimes Impossible for Users to Prevent Facebook from Publishing Their Content and Information to Third-Party Applications.**

**1. Overview of the Facebook User Platform**

283. As discussed above, Facebook began as a user-driven experience. To induce users to feel comfortable sharing on its platform, Facebook created a series of tools to create the illusion that users, not Facebook, controlled what content was shared with third parties.

284. Users could interact on the Facebook user platform in a myriad of ways. After a user registered for Facebook, she would create a profile, which included the information Facebook required a user to submit at registration (Name, Gender, Email Address, and Birthday). If users wished, they could augment their profile with other optional information, such as Profile Picture; Hometown; Interested in (i.e., dating partners' gender or sex); Looking for (i.e., friends, dating, networking); Relationships (e.g., relationship status or family relationships); Political and Religious Views; Likes and Interests (e.g., music, sports, hobbies); and Education and Work (e.g., high school, college, employer).<sup>75</sup>

285. After creating a profile, users could reach out to people to seek mutual status as

<sup>75</sup> FTC Complaint, *In the Matter of Facebook, Inc.*, No. C-4365 (F.T.C. July 2012), <https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf>.

“Friends,” and could see other users to connect with through their networks or through their Friends’ connections on Facebook. By featuring connections with Friends as an organizing principle of the User Platform, users developed the sense that Facebook was a place of safety and familiar people. Users could “Post” content on their Facebook homepage, and interact with content posted by other users. Postings could be set to public or a variety of private settings, as described below. Finally, users could privately message each other using Facebook Chat (which became “Facebook Messenger”), a private messaging system between the user and other Facebook members. The record of a user’s interactions with the Facebook User Platform become a part of a user’s Profile, and was accessible to other Facebook users as described elsewhere in this Complaint.

**2. Facebook Falsely Promised Users That Their Privacy Controls Limited Sharing of Their Content and Information to the Audiences They Selected**

286. Throughout the Class Period, Facebook told users they could limit who viewed their content through three different types of privacy-related tools (“Privacy Controls”). The Privacy Controls applied to individual posting of content and overrode any Default Privacy Settings which Facebook unilaterally established (as discussed elsewhere in this Complaint).

287. Describing the Privacy Controls in a general sense is somewhat challenging because the Privacy Controls changed in material ways over time at Facebook’s prerogative. However, in every iteration, the Privacy Controls limited sharing of content and information to the limited audiences users selected. Users who engaged in setting these restrictions did so because they believed those restrictions would be honored.

288. The three types of Privacy Controls were:

**A. Profile Privacy Settings**, which limited who could see the content displayed on a user’s profile or shared by a user. There were at least 12 separate Profile Privacy Settings, each applying to different kinds of content.

**B. Profile Privacy Controls**, which allowed a user to control who could see information about the user himself or herself, including the types of Pages they liked or followed, the user’s photos, hometown, etc., information designated as publicly available information (“PAI”),

however was not controlled by Profile Privacy Control Tools.<sup>76</sup>

**C. Publisher Privacy Control**, which allowed users to define who can see the content they were posting, but allowed users to change the audience for individual posts.<sup>77</sup> It overrides any other default settings. This tool appears next to or as part of the Publisher Window, which is the portion of the User Platform where a user posts content.

289. Each of these Privacy Controls was located in a different section of the Facebook User Platform. Each of these Privacy Controls promised users they could make affirmative privacy choices for the categories of user content and information displayed on the user's profile or shared by the user for which users had Privacy Controls.

### **3. Facebook's "Privacy Controls" Misled Users About How to Control the Information and Content That They Shared with Applications.**

290. Critically, Facebook's Privacy Controls purported to give users control over who could see their content and information on the Facebook user platform. That is, they controlled the content and information that other *users* could see.

291. The revelation of the Cambridge Analytica scandal was that these "Privacy Controls" did not control what third-party applications or Business Partners could see. For that, users had to go to another part of Facebook, to a fourth tool, the "**App Settings**" page. What's more, it is apparent only now that even the App Settings did not control the information available to 5,200 "Whitelisted Apps," and *no* setting prevented Facebook sharing users' content and information with Business Partners.<sup>78</sup> That is, thousands of Apps had access to all user content and information, regardless of users' Privacy Controls or App Settings.

---

<sup>76</sup> Facebook, *Facebook Redesigns Privacy*, *supra* note 14 (introducing privacy controls for pages); *Making it Easier to Share With Who You Want*, Facebook (Aug. 23, 2011), <https://www.facebook.com/notes/facebook/making-it-easier-to-share-with-who-you-want/10150251867797131> (introducing inline privacy controls for profile information and posts).

<sup>77</sup> See, e.g., *Facebook Asks More Than 350 Million Users Around the World To Personalize Their Privacy*, Facebook Newsroom (Dec. 9, 2009), <https://newsroom.fb.com/news/2009/12/facebook-asks-more-than-350-million-users-around-the-world-to-personalize-their-privacy/> (introducing Publisher Privacy Control); Facebook, *Making it Easier to Share*, *supra* note 76.

<sup>78</sup> DCMS Report, *supra* note 28, ¶ 81.

292. Facebook shared information with Whitelisted Apps and Business Partners secretly and at its own discretion, driven by its business interests, not users' privacy interests.<sup>79</sup> Thus, the Privacy Controls described herein were a fig leaf insofar as sharing with Facebook's Whitelisted Apps and Business Partners were concerned.

293. However, the Privacy Controls, along with Facebook's other statements regarding users' control of their content and information, created an expectation of privacy for reasonable users who believed that the Privacy Controls actually operated as Facebook said they did. The Privacy Controls are described below. Users who understood they needed to do more to protect their privacy spent significant time adjusting these controls. *See* ¶¶ 29, 38, 45, 52, 63, 71, 81, 88, 96, 107, 115, 123, 131, 144, 163, 171, 191, 213, 220.

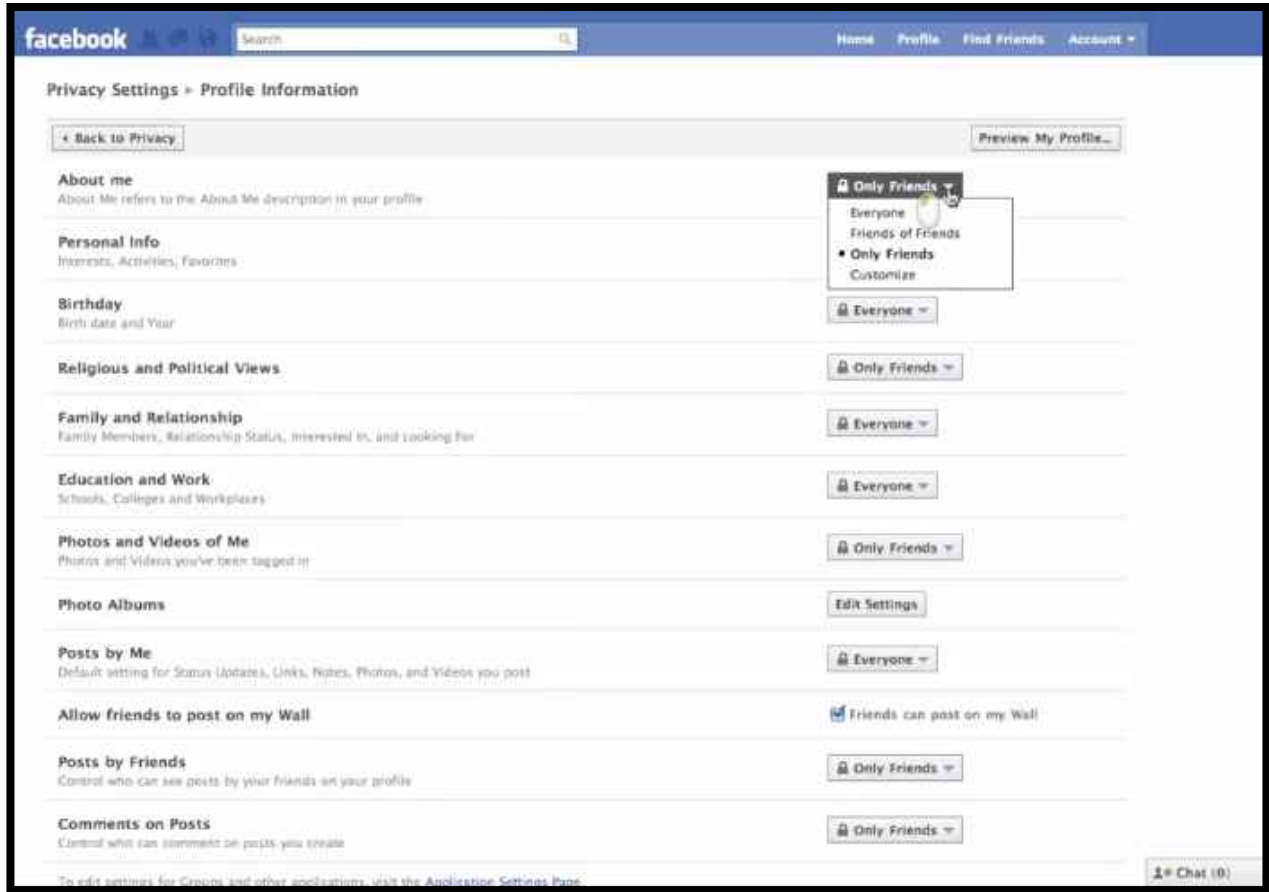
294. The **Profile Privacy Settings** tool was available during the entire Class Period through the Profile Privacy Settings screen. Though the Profile Privacy Settings screen changed throughout the Class Period, at all relevant times the Profile Privacy Settings purported to give Facebook users the ability to control who could see their content and information. To access the Profile Privacy Settings from the Facebook home page, a user clicked on Account and selected Privacy Settings to access the Privacy Page. From there, a user selected a privacy hyperlink and then Profile, which would take the user to a Profile Privacy Settings screen. The Profile Privacy Settings screen allowed users to set her own default audience for the content and information the user shared with other Facebook users. Users could accept Facebook's default Profile Privacy settings (which changed throughout the Class Period) or could modify them. Users who changed their profile Privacy Settings to limit the audience for their profile or posts relied on Facebook's assertions of choice and control over who could view the content they posted.

295. For example, the below screenshot of this "Privacy Settings" screen from 2010 offered a list of the categories of information. From this menu, the user could seemingly choose a specific audience to share this information with. Clicking the dropdown arrow next to each category allowed users to specify whether the information is shared with "Everyone," "Friends," "Friends of Friends," or

---

<sup>79</sup> *Id.*

to choose their own customized audience list.<sup>80</sup>



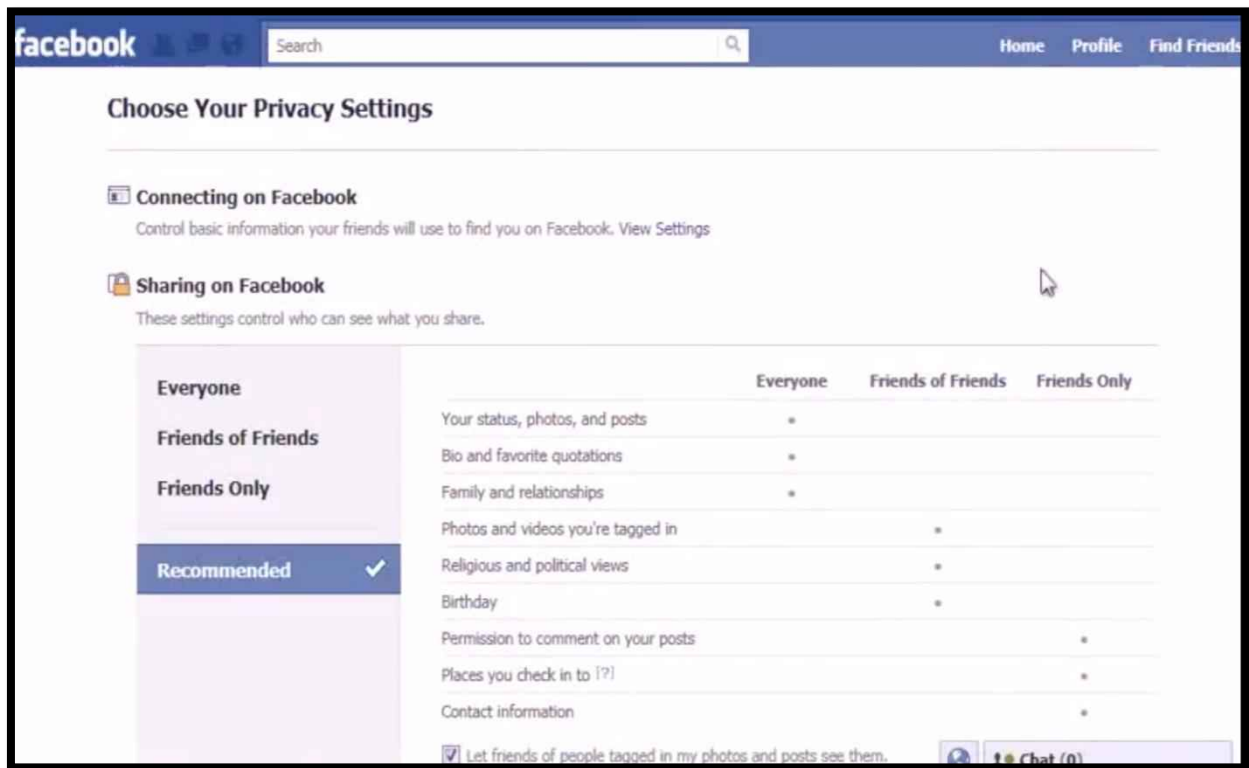
296. This screen changed slightly, to the display below, around 2010 to 2011.<sup>81</sup> Like the previous screen, this webpage seemingly allowed users to choose who can see their content and information.

<sup>80</sup> Aarpwi, *FB Privacy Settings*, YouTube (Apr. 6, 2010), <https://www.youtube.com/watch?v=HRhB3R9DTNo> (last visited Feb. 22, 2019).

<sup>81</sup> Kvchosting, *How to Manage Your Privacy Settings on Facebook*, YouTube (Mar. 25, 2013), <https://www.youtube.com/watch?v=O378rrYcjlC> (last visited Feb. 22, 2019).

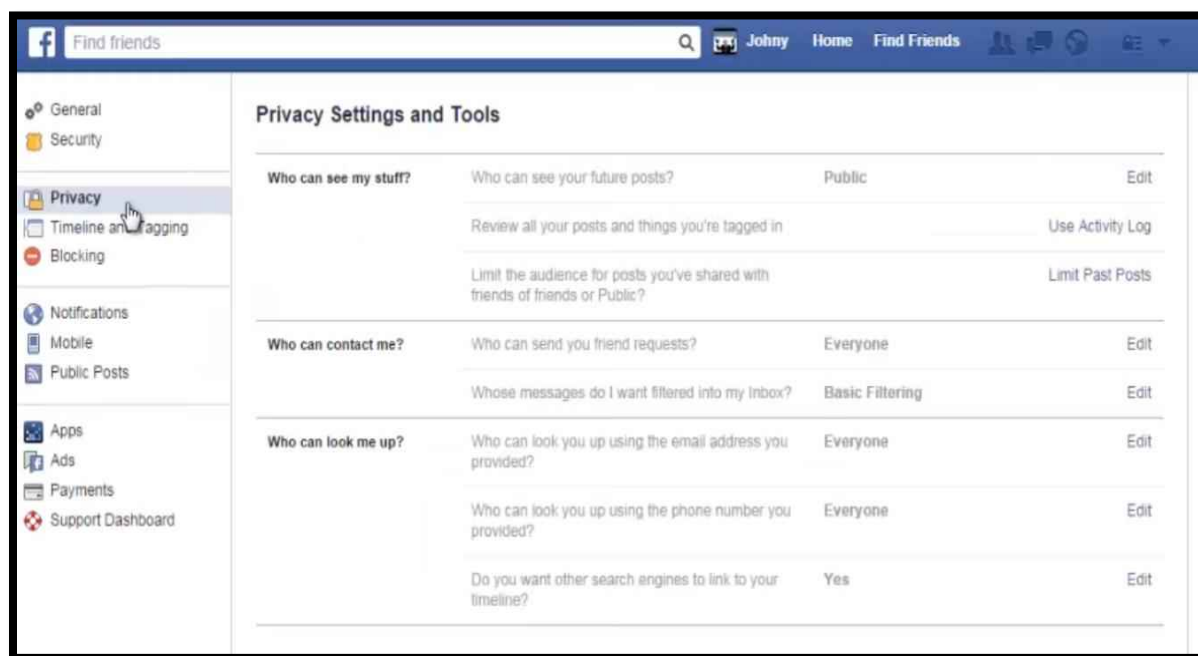


297. At some time in 2012 to 2013, the display changed again to the display below. This



screen stayed substantially the same until April 2018.





298. As with the prior iterations of the Profile Privacy Control screens, during the period leading up to 2018, users could select the edit button next to each category of information. This would then allow the user to choose the exact audience that could view the user's posts. For each "Privacy Setting" depicted above, users could click a dropdown menu and restrict access to specified users, e.g., "Only Friends," or "Friends of Friends."

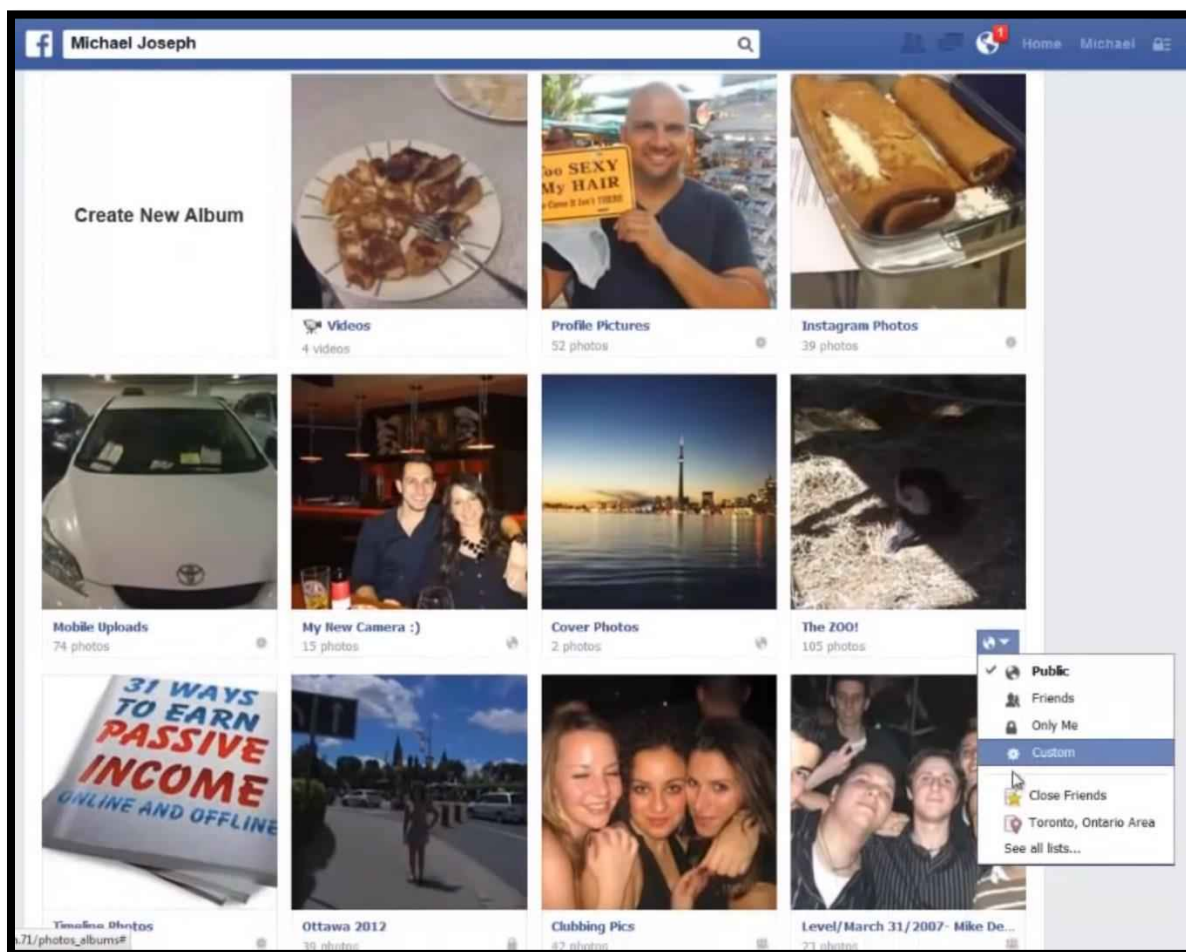
299. **Second**, the **Profile Privacy Controls**, introduced for Pages on May 26, 2010, and for other profile content on August 23, 2011, controlled the audience for the categories of information displayed on a user's Profile, e.g., the Pages they interacted with on Facebook, their photo albums, or other basic information such as hometown.<sup>82</sup> Users could control who could see the books, movies, or sports teams they liked by locating the "Favorites" section of their Profile Page, and selecting the audience for each category of Page Likes from a drop-down menu. Similarly, a user could select the audience for her hometown, or photo albums.

300. Users also had Profile Privacy Controls that could limit the audience for each individual category of information displayed on their Facebook profile (e.g., books and movies). For example, a

<sup>82</sup> Facebook, *Making it Easier to Share*, *supra* note 76.

user who wanted to hide her likes could locate the “likes” category on their public profile and select an audience dropdown menu next to each “likes” category.<sup>83</sup> This menu gave users the following options for whom the information could be shared with: “Public,” “Friends,” “Only Me,” and “Custom.”

301. Facebook also seemingly offered users’ Profile Privacy Controls over their photos. Users could set entire photo albums as well as individual photos to a specific audience. An example is shown



below:

<sup>83</sup> *Id.*



302. Just like the Profile Privacy Settings page, each of these Profile Privacy Controls purported to give a user control over who could see her content and information. In actuality, only the “Only Me” selection would have limited third-party applications from accessing the user’s information through her Friends. This was not clear in the controls.

303. *Third*, after December 9, 2009, users could use the **Publisher Privacy Control Tool** to control the audience for specific content shared by a user, called a “Post.” Posts are some of the most commonly created user content on Facebook.<sup>84</sup> Posts include videos, media, photos, and other content accompanied by anything a user wishes to express on the platform. Photos and other content users post also contain geolocation data, relationship data, information about people’s moods and proclivities. Posts are the heart of the user experience on Facebook. The privacy settings for them are the backbone of users’ expectations of privacy on the platform.

<sup>84</sup> Facebook, *Facebook Asks More*, *supra* note 77.

304. Regardless of any profile Privacy Setting a user might have in place, a user could select an audience for any content he wished to post. That is, the Publisher Privacy Control overrode any default settings for that particular Post. Put differently, even if the default settings were public, users could—and frequently did—select limited audiences for the content they shared.<sup>85</sup> Users invested time and effort in making those selections and reasonably expected that they would limit audiences for the content

305. As the below example from 2011 shows, a user could set the audience for a specific status update, photo, or video at the time that the user shared the content. Users could also retroactively restrict audiences by category (such as photo album) or content on the user's Profile Page.<sup>86</sup>

306. The Profile Privacy Control and Publisher Privacy Control tools were the primary



controls available to Facebook users as they navigated the Facebook user platform, meaning that users could interact with them to choose the audience for their content in the process of sharing content, rather than having to go to a separate part of Facebook like the Profile Privacy Settings screen. Given the relative accessibility and prominence of the Profile Privacy Control and Publisher Privacy Control tools, users expected that the audiences they selected to view content they shared would actually be limited to their designated audiences.

<sup>85</sup> Facebook, *Making It Easier to Share*, *supra* note 76; see also Facebook, *Improving User Control on Facebook* (Dec. 9. 2009), [https://www.eff.org/files/press\\_presentation\\_wednesday.pdf](https://www.eff.org/files/press_presentation_wednesday.pdf).

<sup>86</sup> Facebook, *Making It Easier to Share*, *supra* note 76.

307. Most of Facebook’s Privacy Settings, including the default privacy settings Facebook selected for new users, appeared to users only if they visited the Profile Privacy Settings screen, or sought out specific parts of the user’s Profile. Because the Publisher Privacy Control tool in particular was available in real time as a user shared information, interacted with Friends, or otherwise used the Platform, it was the Publisher Privacy Control tool that shaped a user’s expectations for how one’s content would be shared. Even new users whose Profile Privacy Settings were defaulted by Facebook to public for much of their content and information during that 2010-2014 time period had the ability to designate specific posts, photos, and videos as private, and to send private content and information to specific recipients via Facebook Messenger. Many Plaintiffs used the Publisher Privacy Control to set the privacy for specific posts, limiting their audiences during this time. Individual decisions to limit audiences were not overridden by default settings. But Facebook gave third parties access to this private content regardless.

308. Facebook repeatedly promised users that its Privacy Controls would allow users “choice” of audience and “control” over who viewed their content and information on Facebook. Users who changed their Privacy Settings to limit the audience for their profile or Posts reasonably relied on Facebook’s assertions as to users’ choice and control.

**4. To Control Sharing with Applications, Facebook Required Users to Hunt for, Find, and Change the Default Preferences of Their App Settings.**

309. To prevent their information from being shared with applications through their Friends, users needed to access their App Settings, not their Privacy Controls.

310. **App Settings.** In 2010, Facebook created a completely separate set of privacy settings to control what content and information *applications* could access. App Settings were buried within Facebook’s website so effectively that all but the most sophisticated or intrepid users would know they existed and controlled users’ privacy. The App Settings were set by default to *share* all content with third-party applications, not to prevent sharing. By hiding the App Settings and establishing sharing by

default, Facebook published users' content and information without their knowing consent.<sup>87</sup>

311. To access App Settings, a user would first need to access the Settings webpage. On that webpage, a user would need to click a hyperlink to "Apps" (during the Class Period, this link has also been labeled "Applications" and "Applications and Websites").

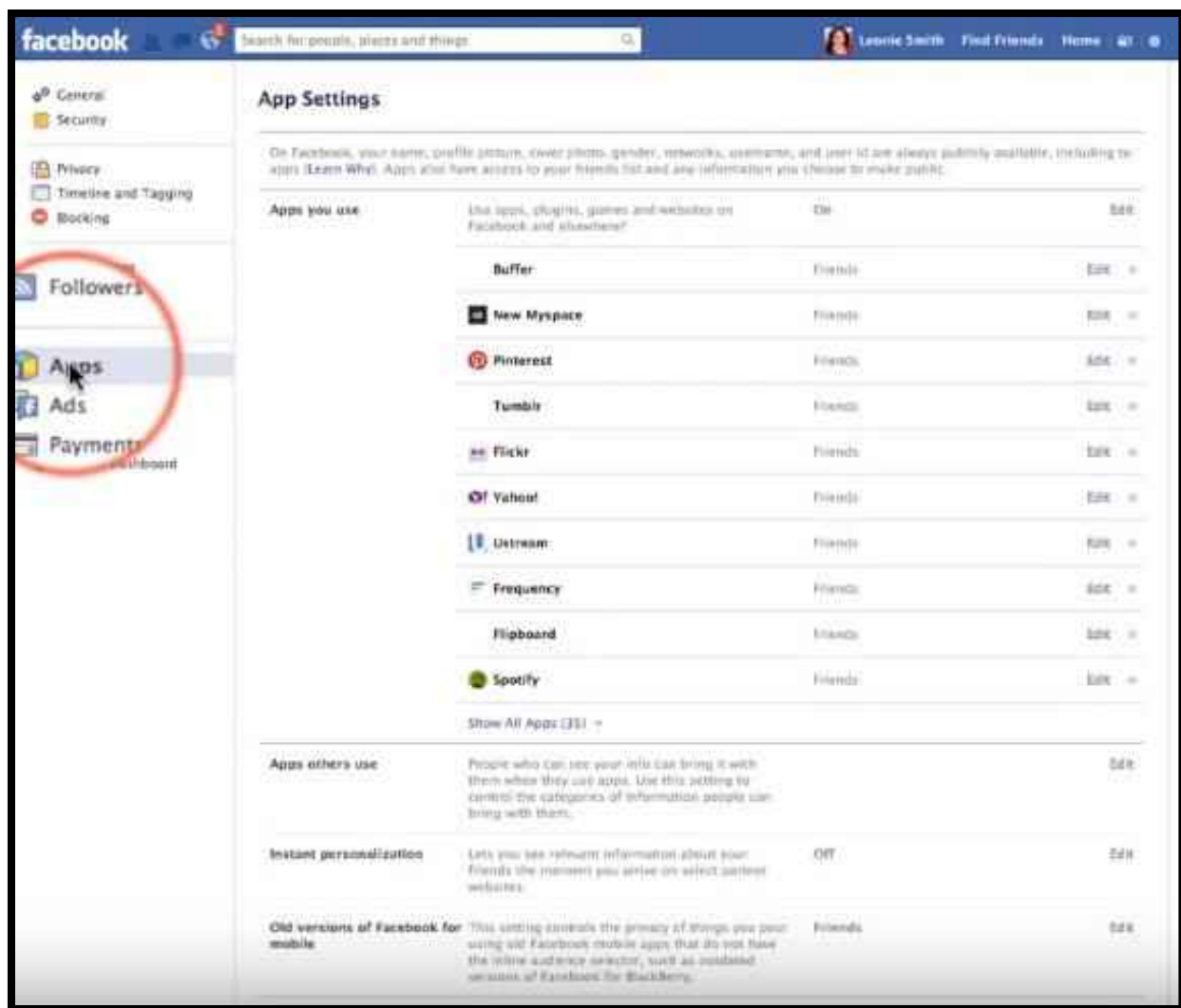
312. After accessing the App Settings webpage, a user would then need to click the "Edit Settings" link next to the subheading "Apps others use."<sup>88</sup> This subheading is described with these words: "People who can see your info can bring it with them when they use Apps. Use this setting to control the categories of information people can bring with them."<sup>89</sup>

---

<sup>87</sup> See Brief for Appellants at 42-43, *Six4Three, LLC v. Facebook, Inc., et al.*, No. A154890/155334 (Cal. Ct. App. Feb. 6, 2019) (noting that counsel for Facebook has recently taken the legal position that Facebook "depublished" users' content and information by turning off access to certain Apps). The conclusion then is that Facebook must have been publishing users' content before it made the decision to depublish it.

<sup>88</sup> See Leonie Smith, *Advanced Privacy Settings for Facebook 2013-2014*, YouTube (Jan. 17, 2013), <https://www.youtube.com/watch?v=OPRFQyGq-yM> (last visited Feb. 22, 2019).

<sup>89</sup> *Id.*




313. A user would be able to alter their application-related privacy settings only after clicking the “edit” link.

314. In December 2009, Facebook changed the “Apps others use” control. Under original settings, users had a one-click option to prevent the disclosure of personal information to third party App Developers through the Facebook Application Programming Interface (“API”)<sup>90</sup>, as the screenshot below indicates<sup>91</sup>:

<sup>90</sup> “Application Programming Interface” or “API” is a collection of commands that an application can run on Facebook, including authorization commands, data retrieval commands, and data publishing commands.

<sup>91</sup> Kevin Bankston, *Facebook's New Privacy Changes: The Good, The Bad, and The Ugly*, Electronic Frontier Foundation (Dec. 9, 2009), <https://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly>.





☐ Do not share any information about me through the Facebook API

315. Facebook changed this control in December 2009, to eliminate the universal one-click option and replace it with a complex control panel. This further prevented users from being able to limit their information from being shared.

316. After December 2009, default “Apps others use” controls allowed the sharing of over fifteen categories of information. The default settings for every user allowed third parties access to the following categories of information: Bio; Birthday; Family and relationships; My website; If I’m online; My status updates; My photos; My videos; My links; My notes; Hometown; Current city; Education and work; Activities, interests, things I like; and My app activity. These default settings are shown below:



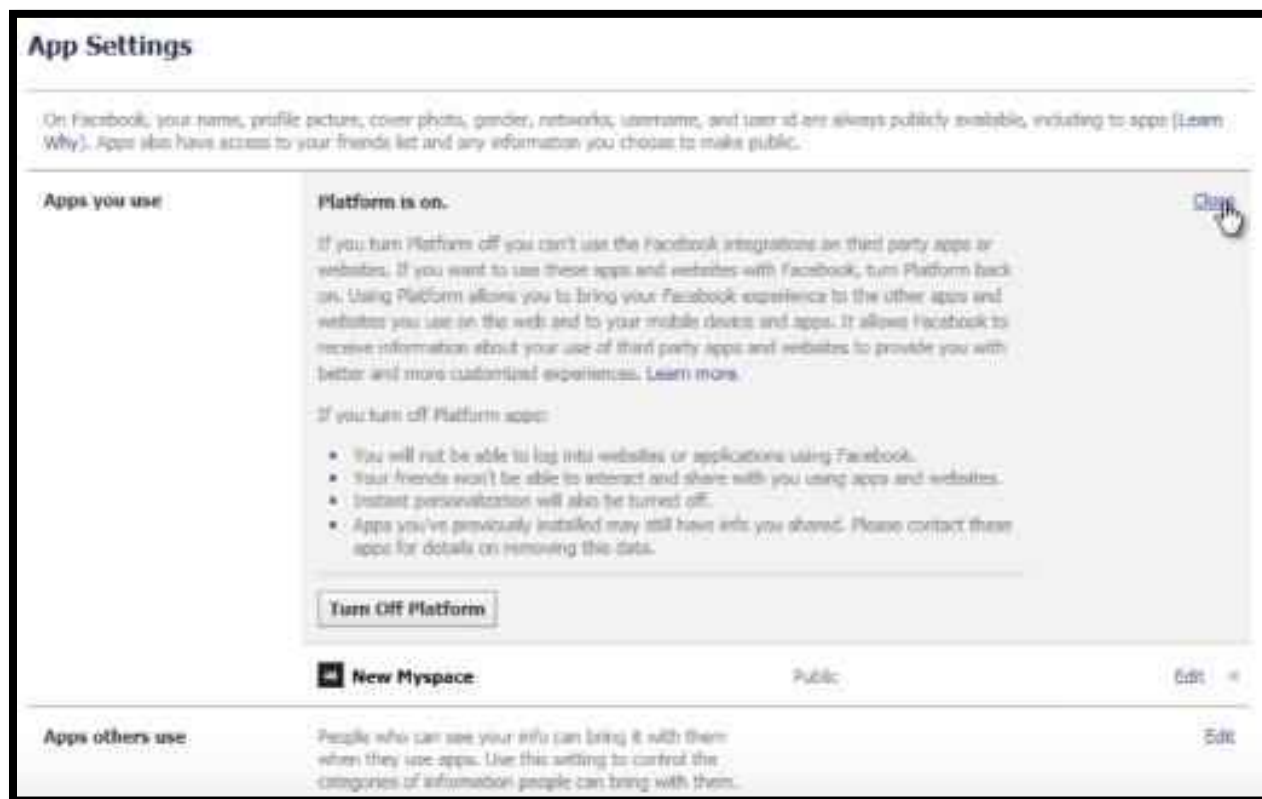


317. Each of these controls corresponds to a category of content and information that App Developers could access using Graph API v1.0.

318. To change her settings, a user would have to click each individual box and click “Save Changes.” In total, the user would have had to make twenty separate clicks to prevent Facebook from sharing these categories of content and information with third parties.

319. Even if a user un-checked each of these boxes, Facebook would still share that user’s friend list, gender, and other information that the user had made public. The only way to turn access off to third parties entirely was to turn off access to all applications. Yet, by default, applications were turned on. Thus, a user who had never accessed or signed up for an application still would have shared over fifteen categories of their information to third parties.

320. To turn off applications entirely, a user would need to go to the App Settings page, go to the “Apps you use” subheading, and click the “edit” link next to that subheading. This would bring up the following disclosure:



321. Only by clicking “Turn Off Platform” could the user prevent all access to her information by third-party App Developers. This would have taken five affirmative clicks from the user.

322. Moreover, if a user set her profile privacy settings to “public” but set her App Settings to prevent sharing with third-party Apps, Facebook would override users’ App Settings. Rather than abiding by a user’s express desire to prevent Apps from accessing her content and information, Facebook allowed Friends to authorize third-party access to a user’s content and information. However, the reverse was not true. If users set their profile privacy settings for information to a non-public setting like Friends or Friends of Friends, Facebook would not limit the information third parties could access through Friends’ App usage.

323. The “Apps others use” control panel no longer was effective after Graph API v1.0 was deprecated in May 2015. Regarding this control panel, Facebook stated: “This feature is a legacy control. It does not reflect the information apps can get on the version of our platform implemented

from 2014.”<sup>92</sup> Yet, even after this control panel was deprecated, Facebook continued to give users’ content and information to Whitelisted Apps Developers and Business Partners.

324. Overall, this process defies the reasonable expectations of a user. Users who chose to limit their Privacy Settings to “Friends,” “Friends of Friends,” and “Public” would still have potentially shared their information with their Friends’ Apps Developers.

325. Notably, App Developers had access to more information they were collecting about users than users had options to control. The App control panel facing users did not identify the same categories of content that App Developers could access.

326. The disconnect meant that App Developers could download information that users had not had the option of excluding from availability to them. For example, even if a user deselected all content displayed in this panel, App Developers could still gain access to user’s information, such as messages and posts on the App User’s timeline.

327. Moreover, when an App User granted permission to App Developers, the user’s Friends were not given any contemporaneous notice identifying the categories of their information being shared to the App Developer. Thus, users had no way to view what content and information Apps were accessing through users’ Friends.

328. What’s more, while Facebook provided App Users with a list of Apps users themselves authorized, Friends received no notice of all of the Apps downloading their content. That meant that Friends had no way to modulate their behavior or remove that access. A real time example is that the App Pikinis, developed by App Developer Six4Three, collected photos of women in bikinis, curating them for users to rate and review. If a woman sent a photo attached to a private message to just one person, that photo was still published to Six4Three by Facebook when that “Friend” downloaded its App. Women in those photos had no notice that their content was downloaded and no way to retrieve it.

329. Indeed, an FTC complaint from 2011 (“FTC Complaint”) filed against Facebook outlines many of the same issues that persisted:

---

<sup>92</sup> James Titcomb, *A Facebook privacy setting to manage what data you share does not do anything*, The Telegraph (Mar. 22, 2018), <https://www.telegraph.co.uk/technology/2018/03/22/facebook-privacy-setting-manage-data-share-does-not-do-anything/>.

14. None of the pages . . . have disclosed that a user's choice to restrict profile information to "Only Friends" or "Friends of Friends" would be ineffective as to certain third parties. Despite this fact, in many instances, Facebook has made profile information that a user chose to restrict to "Only Friends" or "Friends of Friends" accessible to any Platform Applications that the user's Friends have used (hereinafter "Friends' Apps"). Information shared with such Friends' Apps has included, among other things, a user's birthday, hometown, activities, interests, status updates, marital status, education (*e.g.*, schools attended), place of employment, photos, and videos.

15. Facebook's Central Privacy Page and Profile Privacy Page have included links to "Applications," "Apps," or "Applications and Websites" that, when clicked, have taken users to a page containing "Friends' App Settings," which would allow users to restrict the information that their Friends' Apps could access.

16. *However, in many instances, the links to "Applications," "Apps," or "Applications and Websites" have failed to disclose that a user's choices made through profile privacy settings have been ineffective against Friends' Apps.* For example, the language alongside the Applications link . . . has stated, "[c]ontrol what information is available to applications **you use** on Facebook." (Emphasis added). *Thus, users who did not themselves use applications would have had no reason to click on this link, and would have concluded that their choices to restrict profile information through their Profile Privacy Settings were complete and effective.*<sup>93</sup>

330. Moreover, this process required users to navigate through multiple webpages and privacy setting controls. By hiding the controls and establishing privacy settings that allowed sharing, Facebook sought to manufacture users' consent.

331. Perhaps most egregiously, Facebook provided users with no tools to control whether and how their content and information could be accessed by Business Partners. Neither the Privacy nor the App Settings had any effect on Business Partners' access to their content and information.

## **5. Facebook Changed the Default Privacy Settings from 2010-2014 to Make More Content Public, Prompting FTC Action.**

332. Users who signed up before November 2009 were assured that in general their content was nonpublic because Facebook's default Privacy Settings made most user content available only to Friends and Networks.<sup>94</sup> For example, Friends had access to a user's Contact Information, Birthday, and other Profile Information, while Friends and Networks had access to Wall Posts, Photos, and

---

<sup>93</sup> FTC Complaint, *supra* note 75 (emphasis added).

<sup>94</sup> *Id.* at ¶ 19.

Friends Lists. Only a user's name and network were designated as public information by Facebook. Users could control access to other content and information including Name, Profile Picture, Gender, Friend List, Pages, Networks, and Posts through Privacy Controls, as described in more detail elsewhere in this Complaint.<sup>95</sup>

333. In December 2009, however, Facebook changed its Privacy Policy to designate additional items of user information as public.<sup>96</sup> With these changes, Facebook unilaterally made users' name, profile picture, gender, current city, Friend List and Page Likes public, regardless of a users' prior Privacy Settings.<sup>97</sup> This meant that users could not prevent other users or third-party Apps from seeing this content, including content that they had designated private. For users who had signed up and built a community on Facebook, their only choice was to leave Facebook or surrender their preferred privacy restrictions on some of their content and information. This was a breach of Facebook's promise to users that they controlled their content and information.

334. At the same time, Facebook changed the default Privacy Settings for most other types of information, including for "About Me" information, Family and Relationships, Work and Education, and Posts, to "Everyone," changing the default of Photos and Videos, Birthday, and Religious and Political Views to Friends of Friends, and keeping access to user Contact Information to Friends Only.<sup>98</sup>

335. However, even during this time period, users could privately message one another, reasonably expecting that content shared through Facebook Messenger would remain between those limited audiences. Users could also post and designate their post content private.

---

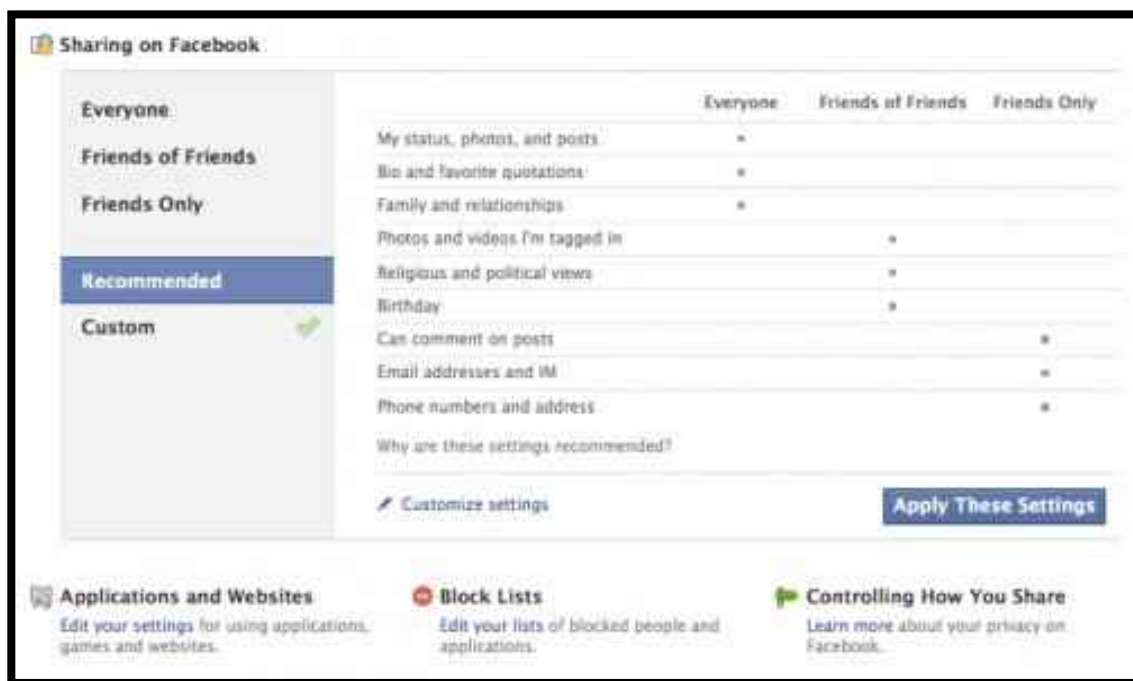
<sup>95</sup> *Id.* at ¶ 20-22; Opsahl, Kurt, *Facebook's Eroding Privacy Policy: A Timeline*, Electronic Frontier Foundation (Apr. 28, 2010), <https://www.eff.org/deeplinks/2010/04/facebook-timeline>.

<sup>96</sup> FTC Complaint, *supra* note 75, ¶20-22.

<sup>97</sup> Facebook, *Facebook Asks More*, *supra* note 77.

336. While the 2009 default Privacy Setting remained in place for new users until 2014, Facebook responded to the public outcry about the unilateral changes to public in May 2010, by designating less user information as public. After May 26, 2010, a user's name, profile picture (should a user choose to have one), gender (though this could be hidden on the profile), and networks (should the user join any) were designated as PAI, and while current city, Friend List and Page Likes were defaulted to public, they could be changed by a user to a more private setting.<sup>99</sup>

337. In May 2014, after years of controversy, Facebook restored the default Privacy Setting of



“Friends Only” for Posts for new users, but did not change settings for existing users.<sup>100</sup> Rather, Facebook offered existing users “Privacy Check-ups” that continued to recommend public disclosure of nearly all user content and information.<sup>101</sup> Facebook also made the setting for posts “sticky,” meaning that new posts defaulted to whatever setting was selected for the previous post. These user-content default settings have largely remained in place since 2014, though Facebook has made adjustments to

<sup>99</sup> Facebook, *Facebook Redesigns Privacy*, *supra* note 14.

<sup>100</sup> Josh Constine, *Facebook Stops Irresponsibly Defaulting Privacy of New Users' Posts to "Public," Changes to "Friends,"* TechCrunch (May 22, 2014), <https://techcrunch.com/2014/05/22/sometimes-less-open-is-more>.

<sup>101</sup> *Id.*

the location and availability of privacy settings and controls.<sup>102</sup>

**C. Facebook Allowed Third Parties to Access Facebook Users’ Content and Information Without or Beyond the Scope of Users’ Consent.**

338. Through its use of various API technology, Facebook allowed App Developers, device makers, and other Business Partners to access its platform and interact with Facebook users.

339. For example, Facebook used an “Events API” to allow users to grant an App permission to get information about events the user is hosting or attending, including private events. Additionally, Facebook used a “Groups API” to make it easier for users to post and respond to content in their groups. Likewise, Facebook offered a “Pages API” to help App Developers create tools for Page owners to schedule posts and reply to comments or messages.

340. In April 2018, following the Cambridge Analytica Scandal and resulting inquiries, Facebook acknowledged that all three of these APIs could provide access to a great deal of user content and information and, thus, Facebook opted to impose more requirements for App Developers before they could gain access to user data through any of these APIs.

341. Facebook’s Graph API, is the “primary way to get data into and out of the Facebook platform.”<sup>103</sup> The first version of Graph API, Graph API v1.0, available from April 2010 to May 2015, was very permissive.<sup>104</sup> It was ultimately through this platform that Cambridge Analytica purchased the data of as many as 87 million Facebook users.

**1. Facebook Developed an Interface That Allowed App Developers to Access a Facebook User’s Content and Information Via That User’s Friend.**

342. Facebook announced its Graph API v1.0 in April 2010 at Facebook’s annual App Developer conference. In unveiling Graph API v1.0, Mr. Zuckerberg laid out his plan to turn the Web

---

<sup>102</sup> Daniel Terdiman, *Facebook Just Announced These Changes To Try To Ease Your Mind On Privacy And Data*, Fast Company (Mar. 28, 2018) <https://www.fastcompany.com/40550689/how-facebook-is-striving-to-ease-users-minds-on-privacy-and-data>.

<sup>103</sup> *Overview—Graph API*, Facebook for Developers, <https://developers.facebook.com/docs/graph-api/overview> (last visited Feb. 20, 2019).

<sup>104</sup> *Changelog—Graph API*, Facebook for Developers, <https://web.archive.org/web/20141208030452/https://developers.facebook.com/docs/apps/changelog#> (last visited on Feb. 20, 2019).



into what he called “instantly social experiences.”<sup>105</sup>

343. Graph API v1.0 enabled App Developers to access and store the App User’s name, gender, birthdate, location, photos, and Page likes. App Developers could also collect this information from the App User’s Friends. Device makers and Business Partners had similar access.

344. Facebook organizes users’ content and information on Graph API as “objects”<sup>106</sup> (e.g., people, photos, events, and pages), “connections”<sup>107</sup> between users (e.g., Friend relationships, shared content, and photo tags), and fields which is the metadata associated with an object.<sup>108</sup>

345. Metadata, or “data about data,” are additional pieces of data associated with each Post, message, or other content. Metadata provide context to data. For example, the metadata of a video includes the timestamp of when the video was created, the profile of the user who created the video, and the title and description of the video. Facebook metadata also include users’ privacy restrictions. When Facebook made certain user content, such as photos and videos, available on Graph API v1.0, the metadata reflecting user’s privacy designations associated with this content was not provided to third parties, although other metadata was.

346. In order to read, publish, and delete non-public content and information on Graph API v1.0, App Developers needed to request permission from the user that downloaded and logged into the application.

347. For every permission that is granted, Facebook grants a corresponding “access token,” that the App Developer can then use to query information through the Graph API.

---

<sup>105</sup> Erick Schonfeld, *Zuckerberg: “We are Building a Web Where the Default is Social”*, TechCrunch (Apr. 21, 2010), <https://techcrunch.com/2010/04/21/zuckerbergs-buildin-web-default-social/>.

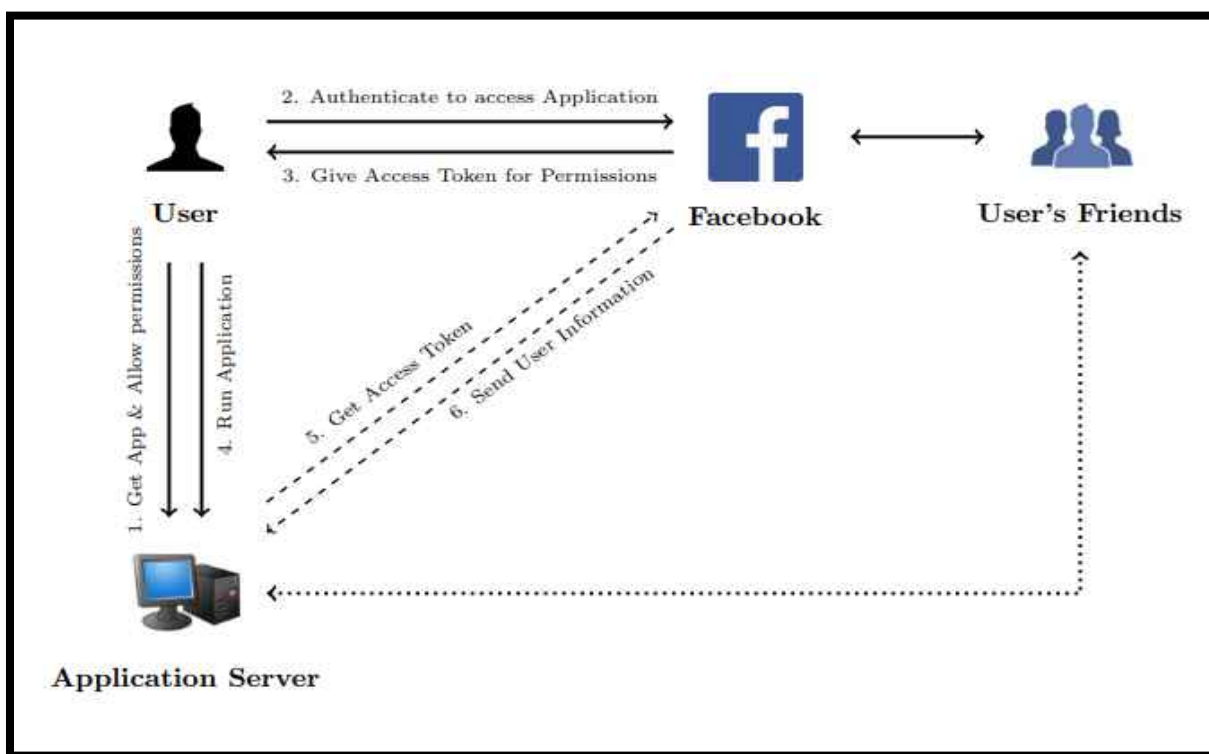
<sup>106</sup> Also referred to as “nodes.” *Overview—Graph API*, *supra* note 103.

<sup>107</sup> Also referred to as “edges.” *Id.*

<sup>108</sup> *Id.*



348. After the App Developer submits the query, Graph API returns that object as well as a set of metadata and connections associated for that object.



349. Third parties using the Graph API v1.0 could access user-data in two ways: server-based and browser-based.

350. Through the server-based method, a user installs the App, which then allows the App to get an “access token” from Facebook. Once the App receives an access token, it may use it to issue a request for certain user data (or Friend data) to Facebook’s server. Facebook will respond by transmitting the requested data to the App server. The data contained in Facebook’s response is then received and stored by the App server.

351. The browser-based method is slightly different. A user installs the App, which then resides in the user’s web browser. After installation, the App obtains an “access token” and, using the access token, may issue a request for certain user data (or Friend data) to Facebook’s server. Facebook will respond by transmitting the requested data to the user’s browser. The App sends this data from the user’s browser to the App server, which stores it.

352. In the browser-based method, Facebook's server sends data to the user's browser. Unknown to Facebook or the user, the App code, which resides in the user's browser, captures this data before it reaches the user and sends it to the App's own server. Thus, it is plausible to consider it an interception. In the server-based method, on the other hand, Facebook's server sends data to the App's server, so that an App residing in the user's browser cannot intercept it.

353. In both server-based and browser-based methods, third parties were able to store users' content and information.

354. Under Graph API v1.0, App Developers could access different categories of users' content and information. The graph below displays all categories of information available under Graph API v1.0:

Basic Info (default)	Extended Profile Properties (xpP)		Extended Permissions (xP)
	User Data	Friends Data	
uid	user_about.me	friends_about.me	ads_management
name	user_actions.books	friends_actions.books	ads_read
first_name	user_actions.music	friends_actions.music	create_event
last_name	user_actions.news	friends_actions.news	create_note
link	user_actions.video	friends_actions.video	email
username	user_activities	friends_activities	export_stream
gender	user_birthday	friends_birthday	manage_friendlists
locale	user_checkins	friends_checkins	manage_notifications
age_range	user_education_history	friends_education_history	manage_pages
	user_events	friends_events	photo_upload
	user_friends	friends_games_activity	publish_actions
	user_games_activity	friends_groups	publish_checkins
	user_groups	friends_hometown	publish_stream
	user_hometown	friends_interests	read_friendlists
	user_interests	friends_likes	read_insights
	user_likes	friends_location	read_mailbox
	user_location	friends_notes	read_page_mailboxes
	user_notes	friends_online_presence	read_requests
	user_online_presence	friends_photo_video_tags	read_stream
	user_photo_video_tags	friends_photos	rspv.event
	user_photos	friends_questions	share_item
	user_questions	friends_relationship_details	sms
	user_relationship_details	friends_relationships	status_update
	user_relationships	friends_religion_politics	video_upload
	user_religion_politics	friends_status	xmpp_login
	user_status	friends_subscriptions	
	user_videos	friends_website	
	user_website	friends_work_history	
	user_work_history		

355. Under Graph API v1.0, App Developers, by default gained access to users' "Basic Info," which included their User ID, name, gender, their current city, age, Friend lists, and any other

information that the App User had made publicly available.<sup>109</sup>

356. In order to gain access to nonpublic content and information, App Developers needed to request permission from the App User. Through this process, App Developers gained access to the App User's content and information and the user's Friends' content and information.

357. Under Graph API v1.0, App Developers could request three types of permissions: User permission, Friends permission, and Extended Permissions.<sup>110</sup>

358. Graph API v1.0 categorized both the User and Friends permissions as "Extended Profile Properties." Extended Profile Properties included: about me; activities; birthdays; check ins; education history; events; groups; hometown; interests; likes; location; notice; photos; questions; relationships; relationship details; religion and politics; status; subscriptions; videos; websites; and work history. A chart from Facebook's App Developer page defining these permissions follows below<sup>111</sup>:

---

<sup>109</sup> *Permissions Reference*, Facebook Developers, (Sept. 23, 2012), <https://web.archive.org/web/20120923065901/https://developers.facebook.com/docs/authentication/permissions/> (last visited Feb. 20, 2019).

<sup>110</sup> *Id.*

<sup>111</sup> *Extended Profile Properties*, Facebook Developers (Sept. 11, 2013), <https://developers.facebook.com/docs/reference/login/extended-profile-properties/> [<https://web.archive.org/web/20130911191323/https://developers.facebook.com/docs/reference/login/extended-profile-properties/>].

User permission	Friends permission	Description
<code>user_about_me</code>	<code>friends_about_me</code>	Provides access to the "About Me" section of the profile in the <code>about</code> property
<code>user_activities</code>	<code>friends_activities</code>	Provides access to the user's list of activities as the <code>activities</code> connection
<code>user_birthday</code>	<code>friends_birthday</code>	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
<code>user_checkins</code>	<code>friends_checkins</code>	Provides read access to the authorized 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, 2012.
<code>user_education_history</code>	<code>friends_education_history</code>	Provides access to education history as the <code>education</code> property
<code>user_events</code>	<code>friends_events</code>	Provides access to the list of events the user is attending as the <code>events</code> connection
<code>user_groups</code>	<code>friends_groups</code>	Provides access to the list of groups the user is a member of as the <code>groups</code> connection
<code>user_hometown</code>	<code>friends_hometown</code>	Provides access to the user's hometown in the <code>hometown</code> property
<code>user_interests</code>	<code>friends_interests</code>	Provides access to the user's list of interests as the <code>interests</code> connection
<code>user_likes</code>	<code>friends_likes</code>	Provides access to the list of all of the pages the user has liked as the <code>likes</code> connection
<code>user_location</code>	<code>friends_location</code>	Provides access to the user's current city as the <code>location</code> property
<code>user_notes</code>	<code>friends_notes</code>	Provides access to the user's notes as the <code>notes</code> connection
<code>user_photos</code>	<code>friends_photos</code>	Provides access to the photos the user has uploaded, and photos the user has been tagged in
<code>user_questions</code>	<code>friends_questions</code>	Provides access to the questions the user or friend has asked
<code>user_relationships</code>	<code>friends_relationships</code>	Provides access to the user's family and personal relationships and relationship status
<code>user_relationship_details</code>	<code>friends_relationship_details</code>	Provides access to the user's relationship preferences
<code>user_religion_politics</code>	<code>friends_religion_politics</code>	Provides access to the user's religious and political affiliations
<code>user_status</code>	<code>friends_status</code>	Provides access to the user's status messages and checkins. Please see the documentation for the <code>location_post</code> table for information on how this permission may affect retrieval of information about the locations associated with posts.
<code>user_subscriptions</code>	<code>friends_subscriptions</code>	Provides access to the user's subscribers and subscribers
<code>user_videos</code>	<code>friends_videos</code>	Provides access to the videos the user has uploaded, and videos the user has been tagged in
<code>user_website</code>	<code>friends_website</code>	Provides access to the user's web site URL
<code>user_work_history</code>	<code>friends_work_history</code>	Provides access to work history as the <code>work</code> property

359. In addition, App Developers could request “Extended Permissions” from the App User. These permissions gave access to the content and information of both the App Users and the users’

Read Permissions	
Permission	Description
<code>read_friendlists</code>	Provides access to any friend lists the user created. All user's friends are provided as part of basic data, this extended permission grants access to the lists of friends a user has created, and should only be requested if your application utilizes lists of friends.
<code>read_insights</code>	Provides read access to the Insights data for pages, applications, and domains the user owns.
<code>read_mailbox</code>	Provides the ability to read from a user's Facebook Inbox.
<code>read_requests</code>	Provides read access to the user's friend requests
<code>read_stream</code>	Provides access to all the posts in the user's News Feed and enables your application to perform searches against the user's News Feed
<code>xmpp_login</code>	Provides applications that integrate with Facebook Chat the ability to log in users.
<code>user_online_presence</code>	Provides access to the user's online/offline presence
<code>friends_online_presence</code>	Provides access to the user's friend's online/offline presence
Publish Permissions	
Permission	Description
<code>ads_management</code>	Provides the ability to manage ads and call the Facebook Ads API on behalf of a user.
<code>create_event</code>	Enables your application to create and modify events on the user's behalf
<code>manage_friendlists</code>	Enables your app to create and edit the user's friend lists.
<code>manage_notifications</code>	Enables your app to read notifications and mark them as read. <b>Intended usage:</b> This permission should be used to let users read and act on their notifications; it should not be used to for the purposes of modeling user behavior or data mining. Apps that misuse this permission may be banned from requesting it.
<code>publish_actions</code>	Enables your app to post content, comments and likes to a user's stream and requires extra permissions from a person using your app. Because this permission lets you publish on behalf of a user please read the Platform Policies to ensure you understand how to properly use this permission. Note, you do <b>not</b> need to request the <code>publish_actions</code> permission in order to use the Feed Dialog, the Requests Dialog or the Send Dialog. Facebook used to have a permission called <code>publish_stream</code> , <code>publish_actions</code> replaces it in most cases, for users. For pages, <code>publish_stream</code> is still required to publish to a page's timeline.
<code>publish_stream</code>	The <code>publish_stream</code> permission is required to post to a Facebook Page's timeline. For a Facebook User use <code>publish_actions</code> .
<code>rsvp_event</code>	Enables your application to RSVP to events on the user's behalf



Friends. These permissions are defined below:<sup>112</sup>

360. Through these permissions, App Developers gained access to the content and information about the App User's Friends. For example, "Read\_mailbox" permission allowed the App Developer to read the *private* messages of users. This access would include messages sent to and from the App User's Friends.

361. Also, read\_stream allowed the App Developer to read the nonpublic posts on the App User's timeline. This access would include content posted by the App User's Friends on the user's timeline even if that content was meant only for Friends. It also included any content that the App User's Friends had been tagged in. Tagging is a metadata field that refers to the process by which users can link other users to objects on Facebook.

362. App Developers sought all permissions, including the permissions that gave access to Friends' content and information, from the App User when she downloaded or logged into the App. Facebook did not send any notification to Friends when third party App developers gained these permissions.

363. Regarding Facebook's sharing of content and information with App Developers, Ashkan Soltani, independent researcher and consultant and former Chief Technologist at the Federal Trade Commission, stated that he "found that time and time again Facebook allows App Developers to access personal information of users and their Friends, in contrast to their privacy settings and their policy statements," and consequently "there is very little the user can do to prevent their information from being accessed."<sup>113</sup>

## **2. Graph API Allows App Developers to Access Users' Video Information.**

364. A key element of Apps, for users, was the ability to watch and share video content on Facebook's platform. Facebook has developed considerable resources into collecting, curating and

---

<sup>112</sup> *Extended Permissions*, Facebook Developers (Sept. 11, 2013), <https://developers.facebook.com/docs/reference/login/extended-permissions/> [<https://web.archive.org/web/20130911191422/https://developers.facebook.com/docs/reference/login/extended-permissions/>].

<sup>113</sup> DCMS Report, *supra* note 28 ¶ 89, <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf>.

enabling users to watch videos on its platform.

365. To provide this functionality, Facebook stores video information in its data centers, and further stores copies of videos in secondary distribution centers known as "edge caches" located throughout the World. There are ten such distribution centers in the United States alone. When a user attempts to access videos on the Platform, Facebook sends out the copy of the video from the nearest distribution center. The viewer is then able to watch the video on Facebook.

366. Facebook has successfully encouraged users to watch videos on the platform and video viewing is a substantial component of user activity on Facebook. For example, in 2007, Facebook announced a partnership with Ziddio.com that would “allow Facebook users to create and share user-generated videos and give them the chance to become part of a new television series titled ‘Facebook Diaries.’”<sup>114</sup> As part of that partnership, Facebook “encouraged [users] to upload, view, share and rate videos.”<sup>115</sup> In 2013, Facebook announced that it was “starting to test an easier way to watch videos on Facebook.”<sup>116</sup> A 2016 Facebook Newsroom post stated, “[w]e’re focused on creating video experiences that people want, and we’ve heard that people want different options for how and where they watch videos that they discover on Facebook.”<sup>117</sup> Facebook Watch, a feature released in 2017, touted Facebook’s expanded video platform for “[o]riginal shows and popular videos.”<sup>118</sup>

367. Facebook, in turn, passed information about how users watched video content onto third parties. For example, video information was available to App Developers through at least seven different categories of data. These categories included: “users\_videos”, “friends\_video”; “users\_subscriptions”; “friends\_subscriptions”; “users\_likes”; “friends\_likes”; and “read\_stream.”

---

<sup>114</sup> *Facebook and Comcast’s Ziddio Partner to Create User-Generated TV*, Facebook Newsroom (Feb. 7, 2007), <https://newsroom.fb.com/news/2007/02/facebook-and-comcasts-ziddio-partner-to-create-user-generated-tv/>.

<sup>115</sup> *Id.*

<sup>116</sup> Kelly Mayes, *An Easier Way to Watch Video*, Facebook Newsroom (Sept. 12, 2013), <https://newsroom.fb.com/news/2013/09/an-easier-way-to-watch-video/>.

<sup>117</sup> Brent Ayrey, *A New Way to Watch Videos from Facebook on Your TV*, Facebook Newsroom (Oct. 13, 2016), <https://newsroom.fb.com/news/2016/10/a-new-way-to-watch-videos-from-facebook-on-your-tv/>.

<sup>118</sup> Facebook Newsroom, *Introducing Watch, a New Platform for Shows on Facebook* (Aug. 9, 2017), <https://newsroom.fb.com/news/2017/08/introducing-watch-a-new-platform-for-shows-on-facebook>.

Facebook set users' default App settings to allow sharing of six out of the seven of these categories.

368. According to Facebook's definition, the data queries "users\_videos" and "friends\_video" permissions allowed App Developers to obtain "the videos the user has uploaded, and videos the user has been tagged in." Facebook set users' default "App settings" to allow all of this information to be shared with App Developers through a user's Friend. Thus, any App Developer who requested these permissions could have received video information from all users who had not changed the default settings.

369. The "users\_likes" and "friends\_likes" data categories allowed access "to the list of all of the pages the user [had] liked." Facebook defines "Facebook Pages" as "a public profile that allows anyone including artists, public figures, businesses, brands, organizations, and charities to create a presence on Facebook and engage with the Facebook community."

370. According to Facebook's S-1 filing in April 2012, "Examples of popular Pages on Facebook include Lady Gaga, Disney, and Manchester United, each of which has more than 20 million Likes." By March 31, 2012, "there were more than 42 million Pages with ten or more likes." Accordingly, users' likes would have included the Facebook pages for any movies, television shows, actors, production studios, etc., that the user had liked. Facebook set users' default "App settings" to allow this information to be shared to App Developers through a users' Friend.

371. Facebook allowed App Developers access to video information through the "read\_stream" query. Facebook's Developer webpage defined this category as providing "access to all the posts in the user's News Feed and enables your application to perform searches against the user's News Feed." This information would include any videos uploaded by the user as well as any videos or video hyperlinks shared with a user. It would also include any and all posts by that user and any and all posts shared with that user about videos. For instance, an App Developer using this permission setting could see a user's posted critique of a specific movie.

372. Facebook also allowed access through "read\_mailbox" category of information, which allowed Developers were able to read the private messages between the App User and her Friends. Thus, if users shared videos through messenger, the App Developer would gain access to users' video



information. This permission was removed from Facebook's APIs in October 2015.<sup>119</sup>

373. Information made available to Apps and third parties about what video users viewed and what they posted about the videos, is a rich source of content and information for Facebook with tremendous value.

**3. To Allow Third Parties Unfettered Access to Users' Content and Information, Facebook Stripped Users' Privacy Designations for Certain Content Available on Graph API.**

374. The investigations following the Cambridge Analytica scandal have revealed that Facebook's platform actually removed user privacy designations from some of the content provided to third parties. This is significant in light of Facebook's strenuous representations, in this court and around the world, that users' privacy settings were honored. Investigation of counsel in this action has further revealed violations of users' privacy settings not previously publicly described as a finding of any other investigation.

375. Facebook provided users tools to limit the audiences who could view the content they shared on a per-post basis. These post-based privacy selections were available regardless of default settings. For example, a user with "public" default settings could still elect to post something and limit the audience to something more private such as "Friends." Alternatively, that user might send a photo in a private message via Facebook Messenger. Facebook promised users unequivocally that those settings would be honored.

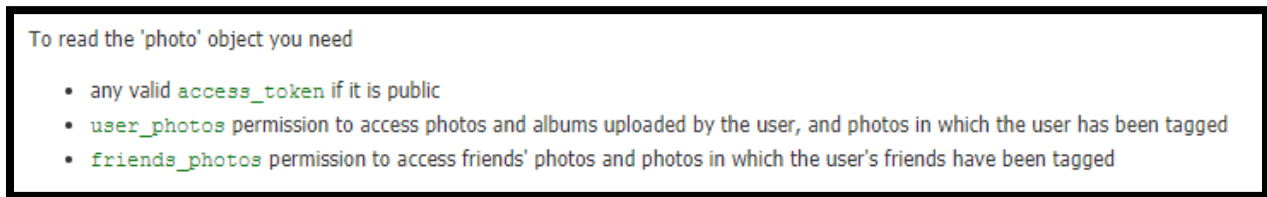
376. Both the default and per-post-based privacy designations are metadata associated with content on Facebook. For example, when a video is posted, the video metadata includes the timestamp of when the video was created, the profile of who created the video, and any comment associated with that video. However, during at least part of the Class Period, when Facebook made certain content – including Photos, Videos, Checkins, and Status –available on Graph API v1.0, the metadata reflecting user's privacy designations associated with this content was not provided to third parties, even though other metadata was.

---

<sup>119</sup> *Id.*; *Changelog*, Facebook for Developers, <https://developers.facebook.com/docs/graph-api/changelog/archive> (last visited Feb. 21, 2019).

377. Because Facebook stripped privacy designation metadata from the associated content, third parties were unable to verify that a user's privacy settings allowed for this content to be shared and, therefore, could not confirm that they were adhering to users' privacy designations as required by Facebook's SRR.<sup>120</sup>

378. From at least 2010 to present, Facebook has maintained a Developer Webpage that provides an overview of Graph API. The Developer Webpage includes the permission required to access an object, the metadata fields of that object, and the connections associated with that object. For example, in 2012, the top of the Photo webpage demonstrated the following permissions that may be required to view the photo:<sup>121</sup>



379. As shown above, certain permissions were required when App Developers sought access to non-public information on Graph API.

380. The Webpage also displays the metadata fields associated with each object. In 2012, for example, the fields for photographs included: ID, From, Tags, Name, Name\_tags, Icon, Picture, Source, Height, Width images, Link, Place, Created\_time, Updated\_time, Position.<sup>122</sup>

381. However, from at least 2010 to 2013, Facebook did not include the privacy restriction metadata in the fields listed for certain objects, such as photos and videos.

<sup>120</sup> *Statement of Rights and Responsibilities*, Facebook (June 8, 2012), [www.facebook.com/legal/terms](http://www.facebook.com/legal/terms), [<https://web.archive.org/web/20121205191915/https://www.facebook.com/legal/terms>]

<sup>121</sup> *Photo*, Facebook Developers (Oct. 18, 2012), <http://developers.facebook.com/docs/reference/api/photo/> [<https://web.archive.org/web/20121018125458/http://developers.facebook.com/docs/reference/api/photo/>].

<sup>122</sup> *Id.*

382. Yet, conspicuously, Facebook included privacy restriction metadata for other objects, such as Events, Groups, and Posts. For example, the Facebook webpage for Posts includes the privacy restriction metadata under fields. A screenshot follows below:<sup>123</sup>



<code>privacy</code>	The privacy settings of the <code>Post</code> .	<code>read_stream</code>	A JSON object with fields described <a href="#">here</a> .
----------------------	---	--------------------------	--

383. Notably, Facebook included the privacy metadata on some objects following the shift to Graph API v2.0 in May 2015. For example, Videos did not include the privacy restriction metadata in 2010 to 2013; however, in 2015, Facebook's Developer Webpage began including the privacy metadata for Videos.

384. From September 18, 2013, the Developer Webpage displayed the following fields available for Video objects, which does not include privacy restriction metadata:<sup>124</sup>

<sup>123</sup> *Post*, Facebook Developers (Nov. 9, 2013), <https://developers.facebook.com/docs/reference/api/post/> [<https://web.archive.org/web/20131109050811/https://developers.facebook.com/docs/reference/api/post/>].

<sup>124</sup> *Video*, Facebook Developers (May 29, 2013), <http://developers.facebook.com/docs/reference/api/video/> [<https://web.archive.org/web/20130529165931/http://developers.facebook.com/docs/reference/api/video/>].

## Fields

The `Video` object has the following fields.

Name	Description	Permissions	Returns
<code>id</code>	The video ID	<code>user_videos</code>	<code>string</code>
<code>from</code>	The profile (user or page) that created the video	<code>user_videos</code>	object containing <code>id</code> and <code>name</code> fields
<code>tags</code>	The users who are tagged in this video	<code>user_videos</code>	array of objects containing <code>id</code> and <code>name</code> fields
<code>name</code>	The video title or caption	<code>user_videos</code>	<code>string</code>
<code>description</code>	The description of the video	<code>user_videos</code>	<code>string</code>
<code>picture</code>	The URL for the thumbnail picture for the video	<code>user_videos</code>	<code>string</code>
<code>embed_html</code>	The html element that may be embedded in an Web page to play the video	<code>user_videos</code>	<code>string</code> containing a valid URL
<code>icon</code>	The icon that Facebook displays when video are published to the Feed	<code>user_videos</code>	<code>string</code> containing a valid URL
<code>source</code>	A URL to the raw, playable video file	<code>user_videos</code>	<code>string</code> containing a valid URL
<code>created_time</code>	The time the video was initially published	<code>user_videos</code>	<code>string</code> containing ISO-8601 date-time
<code>updated_time</code>	The last time the video or its caption were updated	<code>user_videos</code>	<code>string</code> containing ISO-8601 date-time
<code>comments</code>	All of the comments on this video	<code>user_videos</code>	array of objects containing <code>id</code> , <code>from</code> , <code>message</code> , <code>created_time</code> , and <code>likes</code> fields

385. Yet, by November 5, 2015, the Developer Webpage included Privacy setting in its list of fields associated with Video objects:<sup>125</sup>

<code>privacy</code> Privacy	Privacy setting for the video.
---------------------------------	--------------------------------

386. Because Facebook stripped privacy restrictions metadata from the associated content, third parties were unable to verify that a user's privacy settings allowed for this content to be shared

<sup>125</sup> *Video*, Facebook Developers (Nov. 5, 2015), <http://developers.facebook.com/docs/reference/api/video/> [<https://web.archive.org/web/20151105092521/https://developers.facebook.com/docs/graph-api/reference/video>].

and, therefore, could not confirm that they were adhering to users' privacy settings as required by Facebook's Platform Policy.

387. Upon information and belief, Facebook alone was responsible for determining what content was loaded into Graph API v1.0. The removal of users' privacy metadata from certain content including photos and videos, persisted from at least 2010-2013.

388. Facebook's stripping of the privacy metadata was a deliberate act that thwarted users' affirmative privacy designations as to photos and videos by allowing third parties to access users' content without providing users' corresponding privacy settings. Thus, Facebook failed to provide third parties with the crucial information that would have allowed third-party Apps to verify that they were accessing users' photos in compliance with users' privacy settings.

389. With regard to Apps, these actions violated Facebook's agreement with users. Namely, "[w]e require applications to respect your privacy...."<sup>126</sup> Upon information and belief, Facebook was notified by at least one App Developer, of the missing metadata associated with photos and the subsequent inability of the App Developer to verify that it was adhering to users' privacy designations as early as 2012.

390. Upon information and belief, Facebook deliberately allowed App Developers to access users' photos and videos, without regard to their privacy settings, in order to maximize the amount of user content and information available to third parties. Indeed, if the metadata containing privacy designations had been made available through Graph API v1.0, it would have greatly diminished App Developers' ability to use this content. The failure to provide this metadata served Facebook's plan for growth-at-all-costs. That is, here as elsewhere, Facebook's actual practice undermined the policy to which it paid lip service, egregiously harming users and greatly benefiting Facebook.

#### **4. Cambridge Analytica Used Facebook's Graph API Interface to Take Users' Content and Information.**

391. In 2007, psychologists Michal Kosinski and David Stillwell from Cambridge University's Psychometrics Centre began using a Facebook quiz they developed called

---

<sup>126</sup> *Statement of Rights and Responsibilities*, Facebook (June 8, 2012), <https://www.facebook.com/legal/terms> [<https://web.archive.org/web/20121205191915/https://www.facebook.com/legal/terms>].

“myPersonality” to study personality traits of consenting users. The App determined gender, age and sex, opening doors for psychologists to consider different ways to connect “likes” with personality traits. Their research received notice from the U.S. Defense Advanced Research Projects Agency ( “DARPA”). Kosinski and Stillwell published their findings in the Proceedings of the National Academy of Sciences in 2013.<sup>127</sup>

392. Researchers from Cambridge University used the myPersonality quiz to create a database “with profile information for over six million Facebook users. It has those users’ psychological profiles, their likes, their music listening, their religious and political views, and their locations, among other information. It says it can predict users’ leadership potential, personality, and ‘satisfaction with life.’”<sup>128</sup>

393. In 2013, Cambridge Analytica approached the myPersonality App team to get access to the App’s data but was turned down because of its political ambitions.<sup>129</sup>

394. In 2013, Aleksandr Kogan and his company Global Science Research (“GSR”) created an application called “MyDigitalLife” (also known as “thisisyourdigitallife”). Facebook had begun collaborating with Kogan concerning Facebook data in 2012. The agreement that Kogan struck with Facebook in 2013 allowed Kogan to launch the MyDigitalLife App on the Facebook platform.<sup>130</sup>

395. Facebook’s ties with GSR run deep. One of GSR’s two co-founders, Joseph Chancellor, is an employee at Facebook, but was placed on administrative leave after the Cambridge Analytica

---

<sup>127</sup> Eric Killelea, *Cambridge Analytica: What We Know About the Facebook Data Scandal*, Rolling Stone (Mar. 20, 2018) <https://www.rollingstone.com/culture/culture-news/cambridge-analytica-what-we-know-about-the-facebook-data-scandal-202308/>.

<sup>128</sup> Kashmir Hill, *The Other Cambridge Personality Test Has Its Own Database with Millions of Facebook Profiles*, Gizmodo (Mar. 22, 2018), <https://gizmodo.com/the-other-cambridge-personality-test-has-its-own-databa-1823997062>.

<sup>129</sup> Only after the Cambridge Analytica Scandal did Facebook reveal that data from myPersonality had been publicly available for years. Phee Waterfield & Timothy Revell, *Huge new Facebook data leak exposed intimate details of 3M users*, New Scientist (May 15, 2018), <https://www.newscientist.com/article/2168713-huge-new-facebook-data-leak-exposed-intimate-details-of-3m-users/>.

<sup>130</sup> On August 22, 2018, Facebook notified four million users that their data was misused when myPersonality refused Facebook’s request for an audit. Ime Archibong, *An Update on Our App Investigation*, Facebook Newsroom (Aug. 22, 2018), <https://newsroom.fb.com/news/2018/08/update-on-app-investigation/>.

Scandal was publicized in 2018.

396. MyDigitalLife marketed itself to Facebook users as a tool that would help them have a better understanding of their own personalities, and that would supply data for use by academic psychologists. The App prompted users to answer questions for a psychological profile. Questions focused on the so-called “Big Five” personality traits: extraversion, agreeableness, openness, conscientiousness, and neuroticism.

397. Through MyDigitalLife, Kogan gained access to the personal data of the approximately 300,000 Facebook users that downloaded the App. In spring 2014, Kogan was approached by an SCL-affiliated contractor and was asked to provide consulting services. Kogan set up GSR to carry out the work. The project was intended to deliver to SCL personality scores matched to the voter registration file for several million people. Kogan authorized GSR’s Facebook App to collect data from App users about not just the user, but also the user’s Friends. This data was then used to predict personality and then provided back to SCL.

398. GSR made no secret of the blatantly commercial nature of its use of Facebook data. It states in its “End User Terms and Conditions” that it intended to “sell” and “license (by whatever means and on whatever terms)” the personal content it obtained through the YDL App. Facebook was provided with GSR’s terms of service and thus was given constructive if not actual notice that GSR was selling user content and information. Kogan has stated that he “never heard a word” from Facebook concerning his intent to “sell” data even though he had publicly posted his intention for a year and a half.

399. Kogan and GSR actively began their relationship with Cambridge Analytica in 2014 and 2015. During this time, Kogan and GSR provided Cambridge Analytica with much more than the personal content and information of the Facebook users who had downloaded the MyDigitalLife App. Graph API v1.0, which Facebook was still using, allowed the App to access the data that users’ *Friends* had shared with them. Through this platform, Facebook gave Kogan and GSR, and thus Cambridge Analytica and other third parties like the University of Toronto and the University of British Columbia, the content and information of more than 50 million additional people who, according to Facebook,



“had their privacy settings set to allow it.”

400. Facebook now estimates that of the up to 87 million Facebook users affected by this scheme, only approximately 300,000 of them had downloaded the MyDigitalLife App—and those users had agreed to share only their own content and information for the limited purposes associated with the App. Facebook admits, however, that historical logs of users’ privacy settings are scant. Upon information and belief, at least the photos shared with Cambridge Analytica were stripped of identifying information that would have communicated the privacy restrictions of users’ Friends. About 1,500 people also gave the App access to their private messages, and people who sent or received messages with those people potentially had their private messages accessed as well.

401. In addition to supplying Cambridge Analytica with fresh Facebook user data on an ongoing basis, Kogan and GSR, at Cambridge Analytica’s request, also performed modelling work on the data. Communications disclosed by Cambridge Analytica personnel demonstrate Kogan’s active role in this modeling.

402. CEO Zuckerberg has admitted that Facebook became aware that Kogan and GSR had misused data in 2015 and conducted an investigation.<sup>131</sup> Defendant Facebook states that it contacted Kogan following the publication of the *Guardian* article in 2015. In its “End User Terms and Conditions,” GSR informed users that UK law governed the rights concerning the MyDigitalLife App:

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.<sup>132</sup>

---

<sup>131</sup> *Facebook’s Use and Protection of User Data: Hearing Before the H. Energy and Commerce Comm.*, 2018 WL 1757479, at 22-23 (Apr. 11, 2018) (Statement of Mark Zuckerberg).

<sup>132</sup> At least part of the personal content stored by GSR was located in the U.K. and administered by Facebook Ireland, Inc. GSR represented to Facebook users that it was a “research organization” with a “registered office based at Magdalene College, Cambridge.” Publicized emails between Kogan and researchers at Cambridge demonstrate that Kogan used Cambridge’s U.K.-based servers for GSR.



The 2015 report from the *Guardian* was thus focused on U.K. citizens and did not receive any meaningful attention in the United States.

403. At minimum, Facebook became aware that GSR sold Facebook data containing personal content by March 2016, when, while negotiating a settlement of claims with Kogan, Facebook was informed that Kogan had made roughly \$800,000 re-selling Facebook user data. Facebook failed to determine at that time the scope and extent of the content and information GSR had obtained. Indeed, Facebook waited over two years to make any type of public disclosure.

404. Kogan initially used the Facebook data that he had obtained in 2012 and subsequently to co-author a number of papers that had obvious commercial purposes and applications. Kogan co-authored papers entitled “*Tracing Cultural Similarities and Differences in Emotional Expression through Digital Records of Emotions*,” “*Happiness Predicts Larger Online Social Networks for Nations and Individuals Low, but not High, in Consumeristic Attitudes and Behaviors*,” “*Silk Road to Friendships: Economic Cooperation is Associated with International Friendships around the World*,” “*Big Data Public Health: Online Friendships can Identify Populations At-Risk of Physical Health Problems and All-Causes Morbidity*,” and “*Donations Predict Social Capital Gains for Low SES, But Not High SES Individuals and Countries*.”<sup>133</sup>

405. Christopher Wylie, a former Cambridge Analytica contractor, has recently revealed how the data mining process at Cambridge Analytica worked: By getting access to Facebook users’ “profiles, likes, even private messages, [Cambridge Analytica] could build a personality profile on each person and know how best to target them with messages.”<sup>134</sup> Facebook users’ profiles “contained enough information, including places of residence, that [Cambridge Analytica] could match users to other records and build psychographic profiles.”<sup>135</sup> Mr. Wylie has said: “We exploited Facebook to

<sup>133</sup> Def. Facebook, Inc.’s Resps. & Objs. to Pls.’ First Set of Interrogs. at pp. 7-8 (Sept. 7, 2018).

<sup>134</sup> Parmy Olson, *Face-To-Face With Cambridge Analytica’s Elusive Alexander Nix*, *Forbes* (Mar. 20, 2018), <https://www.forbes.com/sites/parmyolson/2018/03/20/face-to-face-with-cambridge-analytica-alexander-nix-facebook-trump/#54972c48535f>.

<sup>135</sup> Matthew Rosenberg, et al., *How Trump Consultants Exploited the Facebook Data of Millions*, *N.Y. Times* (Mar. 17, 2018), <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>.

harvest millions of people’s profiles. And built models to exploit what we knew about them and target their inner demons. That was the basis the entire company was built on.”<sup>136</sup>

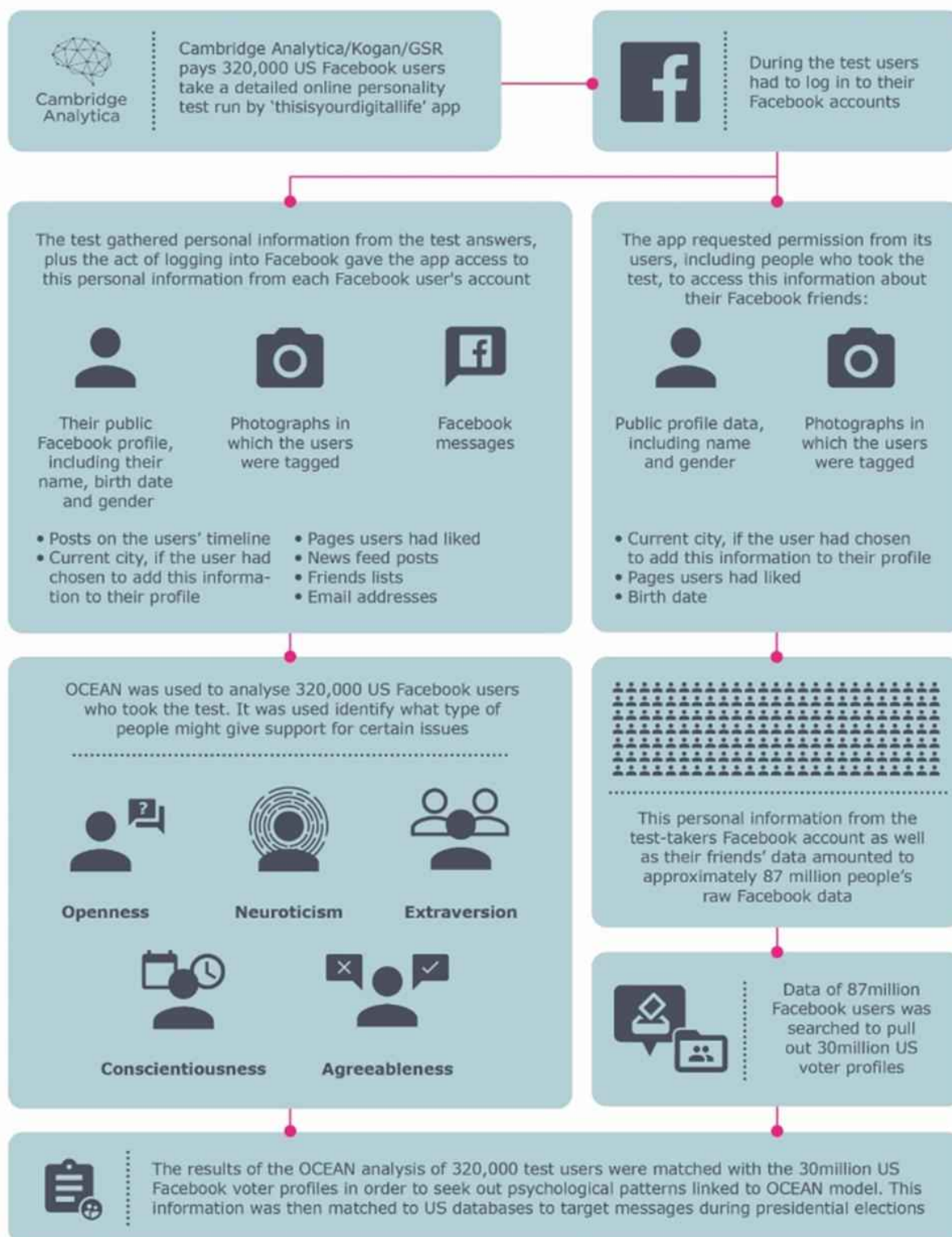
406. The figure below was created by the United Kingdom Information Commissioner’s Office (“ICO”), which is a government agency set up to uphold information rights in the public interest, and to promote openness by public bodies and data privacy for individuals. The figure describes how Cambridge Analytica accessed and harvested the content and information of millions of Facebook users.<sup>137</sup>

---

<sup>136</sup> Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, The Guardian (Mar. 17, 2018), <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.

<sup>137</sup> *Investigation Into the Use of Data Analytics in Political Campaigns – Investigation Update*, (July 11, 2018), Information Commissioner’s Office, (“ICO Report”) at 17, <https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf>.

## Data harvesting of the Facebook data



407. As outlined above, the ICO has found that GSR obtained the following information from users who downloaded the MyDigitalLife App:

Public Facebook profile, including their name and gender; Birth date; Current city, if the user had chosen to add this information to their profile; Photographs in which the users were tagged; Pages that the users had liked Posts on the users' timelines; News feed posts; Friends lists; Email addresses; and Facebook messages.<sup>138</sup>

408. The ICO reports that GSR obtained the following information from the App Users' Friends: "Public profile data, including their name and gender; Birth date; Current city if the friends had chosen to add this information to their profile; Photographs in which the friends were tagged; and Pages that the friends had liked."<sup>139</sup>

409. GSR obtained access to users' and users' Friends likes.<sup>140</sup> This information would include specific video information about these users. GSR shared this like information with Cambridge Analytica.<sup>141</sup> Thus, Facebook allowed GSR to access and share the specific video preferences of its users through this "likes" information.

410. GSR obtained access to the "posts on the users' timelines" for users who installed the MyDigitalLife App.<sup>142</sup> This access would have been available under the "read\_stream" query. Facebook claims that they denied Aleksandr Kogan's request to access this query.<sup>143</sup> But this claim contradicts the U.K.'s ICO's published report on this matter. Through this query, GSR obtained additional access to any information about a user's video preferences posted on that user's timeline.

411. Only after the Cambridge Analytica Scandal became public in March 2018, did Facebook

---

<sup>138</sup> ICO Report, *supra* note 137 at 19-20.

<sup>139</sup> *Id.* at 20.

<sup>140</sup> *Id.* at 19-20.

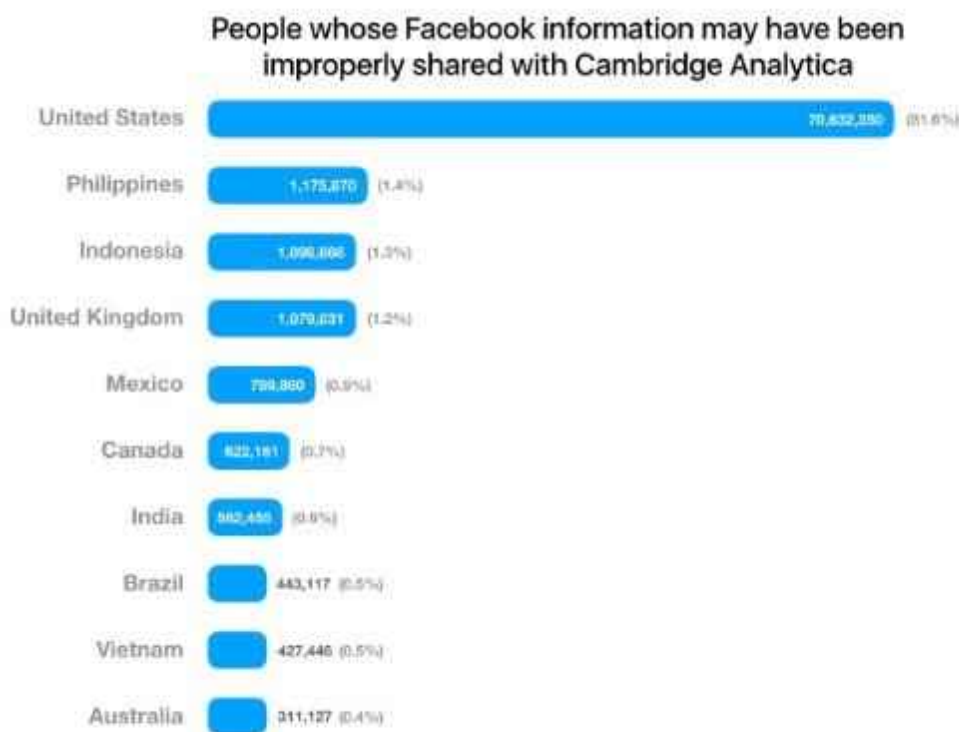
<sup>141</sup> *Id.*; *see also* U.K. House of Commons, Digital, Culture, Media and Sport Committee, Testimony of Dr. Aleksandr Kogan (Apr. 24, 2018), at Q1930, <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/fake-news/oral/81931.html>.

<sup>142</sup> ICO Report, *supra* note 137 at 19-20.

<sup>143</sup> Def. Facebook, Inc.'s Resps. & Objs. to Pls.' First Set of Interrogs. at pp. 6-7 ("Dr. Kogan's App Review application sought extended permissions for the App . . . Facebook rejected Dr. Kogan's application the next day, stating that the App would not be using the data requested to enhance the user's in-app experience.").

announce that it was suspending Cambridge Analytica and its parent company, Strategic Communication Laboratories (“SCL”), from Facebook. It stated that, in 2015, it learned it had been lied to by Dr. Kogan and that Kogan had violated Facebook’s Platform Policies—contracts between Facebook and third-party Apps—“by passing data from an app that was using Facebook Login to SCL/Cambridge Analytica . . . .”<sup>144</sup> Seeking to avoid liability, SCL and its related entities, like Cambridge Analytica, have all filed for bankruptcy, as has GSR.

412. On April 4, 2018, Facebook released the following statement: “In total, we believe the Facebook information of up to 87 million people—mostly in the United States—may have been improperly shared with Cambridge Analytica.” Facebook also released a country-by-country breakdown of the millions of users affected by the GSR App, pictured below:<sup>145</sup>



We do not know precisely what data the app shared with Cambridge Analytica or exactly how many people were impacted. Using an expansive methodology as possible, this is our estimate of the maximum number of unique accounts that directly installed the ThisIsMyData app as well as those whose data may have been shared with the app by their friends.

<sup>144</sup> Paul Grewal, *Suspending Cambridge Analytica and SCL Group From Facebook*, Facebook Newsroom (Mar. 16, 2018), <https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/>.

<sup>145</sup> Mike Schroepfer, *An Update on Our Plans to Restrict Data Access on Facebook*, Facebook Newsroom (Apr. 4, 2018), <https://newsroom.fb.com/news/2018/04/restricting-data-access/>.

413. On May 1, 2018, Facebook updated this blog post to include a state-by-state breakdown of the millions of users who may have had their information shared with Cambridge Analytica, shown below:<sup>146</sup>

---

<sup>146</sup> *Id.*



**State-by-State Breakdown of People Whose Facebook Information May Have  
Been Improperly Shared with Cambridge Analytica**

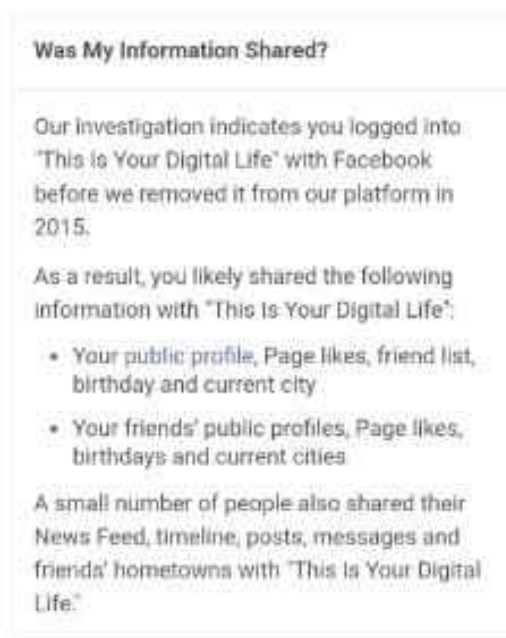
State	Total Impacted Users	State	Total Impacted Users
California	6,787,507	Oklahoma	962,267
Texas	5,655,677	Mississippi	871,695
Florida	4,382,697	Arkansas	829,598
New York	4,368,051	Oregon	798,959
Pennsylvania	2,960,311	Iowa	685,777
Illinois	2,949,469	Connecticut	655,062
Ohio	2,927,388	Kansas	647,563
Georgia	2,857,971	Nevada	631,062
North Carolina	2,521,064	Utah	619,277
Michigan	2,414,438	West Virginia	557,046
Tennessee	1,783,650	Nebraska	384,815
Virginia	1,709,835	New Mexico	348,472
Indiana	1,698,230	District of Columbia	345,652
New Jersey	1,605,868	Idaho	326,248
Missouri	1,574,855	Maine	309,546
Washington	1,434,126	Hawaii	279,583
Alabama	1,385,169	New Hampshire	258,772
Kentucky	1,310,682	Rhode Island	239,240
Massachusetts	1,265,149	Delaware	201,553
Louisiana	1,263,851	Montana	183,744
South Carolina	1,258,400	South Dakota	153,382
Arizona	1,252,103	North Dakota	143,243
Wisconsin	1,200,116	Alaska	139,997
Maryland	1,102,857	Vermont	135,960
Minnesota	1,032,670	Wyoming	112,440
Colorado	966,492		

414. In his April 2018 testimony to the U.K. House of Commons, Facebook Chief Technology

Officer Mike Schroepfer testified that Facebook did not read terms and conditions of any Developer's Apps that were put on Facebook.<sup>147</sup> In this litigation, in its interrogatory responses, Facebook has averred that it could not possibly have read the terms and conditions of these Apps, because there were millions of them.<sup>148</sup> This is one more indication that Facebook did not protect user content and information once it gave access to App Developers.

415. On April 9, 2018, with a notification at the top of News Feeds, Facebook began notifying individual users if their data had been shared with Cambridge Analytica. For example, Plaintiff Fischer received a notification from Facebook in April 2018 that she had logged into "This is Your Digital Life" and her public profile, page likes, friend list, birthday, current city, friend's public profiles, friends' page likes, friends' birthdays, and friends' current cities were likely shared with "This is Your Digital Life." The notification also explained that a small number of people also shared their News feed, timeline, posts, messages, and friends' hometowns with "This is Your Digital Life."

416. The notification that Plaintiff Fischer received looked like this:



<sup>147</sup> U.K. House of Commons, Digital, Culture, Media and Sport Committee, Testimony of Mike Schroepfer (Apr. 26, 2018), at Q2141, <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake-news/oral/82114.pdf>.

<sup>148</sup> Def. Facebook, Inc.'s Resps. & Objs. to Pls.' First Set of Interrogs. at p. 20.



417. On April 22, 2018, Dr. Kogan finally broke his silence in an interview with CBS News Correspondent Lesley Stahl on 60 Minutes. Kogan stated he had terms of service up on his application for a year and a half—terms providing that he could sell the data he obtained through the App—and yet Facebook never enforced its agreement with Kogan or its rules against selling data during this time. Kogan also explained that the ability to gather people’s Facebook Friends’ data without their permission was a Facebook core feature, available to anyone who was a Developer. He explained that there are likely tens of thousands of applications that did what he did, as this was not a bug, but a feature of which Facebook was aware.

418. Among scores of other regulators, the Justice Department and FBI are now investigating Cambridge Analytica, which filed for Chapter 7 bankruptcy on May 17, 2018.

**5. The Cambridge Analytica Scandal Has Triggered Additional Revelations of Apps’ Misuse of User Content and Information.**

419. Following the Cambridge Analytica Scandal, Facebook conducted its own internal audit into other App Developers, but has not made the details public, with scant exception. Audit reports prepared by PricewaterhouseCoopers have been heavily redacted. Nonetheless, it is known that millions of Apps had access to users’ data prior to Facebook’s 2014 platform changes. Facebook has now admitted that it has suspended 400 of them “due to concerns around the Developers who built them or how the information people chose to share with the app may have been used.” Facebook’s review appears to have been limited to Apps that had access to user content and information prior to 2014, when Facebook changed its platform policies. However, reports continue to emerge regarding abuse of user content and information even after this platform change.

420. Facebook has admitted that the conduct at the heart of the Cambridge Analytica Scandal—Kogan’s brazen and expansive access to user content and information for commercial purposes in the guise of research—constituted a breach of Facebook’s promises and agreements with its users.

421. On March 21, 2018, Mr. Zuckerberg took to Facebook to acknowledge Facebook’s breach of trust, while Ms. Sandberg acknowledged that Facebook allowed Apps to access more user

content and information than necessary.

422. In a March 21, 2018 Facebook post, Mr. Zuckerberg acknowledged a “breach of trust between Facebook and the people who share their data with us and expect us to protect it” and said, “We need to fix that.”<sup>149</sup> His post stated that in addition to investigating Cambridge Analytica, Facebook was also investigating “all Apps that had access to large amounts of information.”<sup>150</sup>

423. Mr. Zuckerberg repeated the same sentiment in full-page ads in several British and American newspapers a few days later.

424. Also on March 21, 2018, Sheryl Sandberg posted to her Facebook account that Facebook is “taking steps to reduce the data [Facebook users] give an app” when they use their Facebook account, and the Company intends to “make it easier” for users to have a better understanding of which Apps they have “allowed to access [their] data.”<sup>151</sup>

425. However, it appears that Facebook made these conciliatory statements only to assuage public outcry and prevent users from leaving the platform and to placate regulators until attention died down. Facebook’s attempts to distance itself from these statements when called to account in this lawsuit should not be countenanced.

426. Further, in the wake of the Cambridge Analytica Scandal, Facebook suspended two other companies from its platform in April 2018 for improper data collection: Canadian consulting firm AggregateIQ and CubeYou.

427. On or about April 6, 2018, Facebook suspended AggregateIQ, who played a pivotal role in the Brexit campaign, from the platform, following reports it may be connected to Cambridge Analytica’s parent company, SCL. This was nearly three years after Facebook learned of Cambridge Analytica’s psychographic marketing.

428. On or about April 8, 2018, Facebook suspended the CubeYou App from the platform

---

<sup>149</sup> Mark Zuckerberg, Facebook (Mar. 21, 2018), <https://www.facebook.com/zuck/posts/10104712037900071>.

<sup>150</sup> *Id.*

<sup>151</sup> Lila MacLellan, *Sheryl Sandberg wants you to know she regrets Cambridge Analytica*, Quartz at Work (Mar. 21, 2018), <https://qz.com/work/1234977/facebook-coo-sheryl-sandberg-is-finally-speaking-out-about-cambridge-analytica/>.

after CNBC notified them that CubeYou had misled users by collecting data from quizzes inaccurately labeled “non-profit academic research” and then selling the findings to marketers, and had business ties to Cambridge Analytica.

429. Facebook announced the suspension of hundreds of other Apps, but has not provided additional detail on those suspensions, including the sale and misuse of user content and information.

**6. Facebook Also Enabled Device Makers and Other Business Partners to Access Users’ Content and Information Through Friends.**

430. Facebook partnered with a diverse set of companies, including Business Partners, to develop and integrate Facebook’s User Platform on multiple devices and operating systems. As part of these agreements, Facebook gave Business Partners access to users’ content and information. Facebook created private APIs to transfer users’ content and information to these Business Partners.

431. Facebook has identified 53 Business Partners. These companies include:

- Accedo
- Acer
- Airtel
- Alcatel / TCL
- Alibaba
- Amazon
- Apply
- AT&T
- Blackberry
- Dell
- DNP
- Docomo
- Garmin
- Gemalto
- HP / Palm
- HTC
- Huawei
- INQ
- Kodak
- LG
- MediaTek / Mstar
- Microsoft
- Miyowa / Hape Esia
- Motorola / Lenovo
- Mozilla

- Myriad
- Nexian
- Nokia
- Nuance
- O2
- Opentech ENG
- Opera Software
- OPPO
- Orange
- Pantech
- PocketNet
- Qualcomm
- Samsung
- Sony
- Sprint
- T-Mobile
- TIM
- Tobii
- U2topia
- Verisign
- Verizon
- Virgin Mobile
- Vodafone
- Warner Bros.
- Western Digital
- Yahoo
- Yandex<sup>152</sup>
- Zing Mobile

432. Facebook notes that this list is “comprehensive to the best of our ability.” However, it further stated that “[i]t is possible we have not been able to identify some integrations, particularly those made during the early days of our company when our records were not centralized. It is also possible that early records may have been deleted from our system.”<sup>153</sup>

433. Facebook formed Business Partnerships as early as 2007. These deals allowed Facebook

---

<sup>152</sup> After providing the original list to Congress in June 2018, Facebook has since added Russian search engine, Yandex, to its list of Business Partners.

<sup>153</sup> Letter from Facebook, Inc. to Chairman Greg Walden, Ranking Member Frank Pallone, Energy & Commerce Committee, and U.S. House of Representatives, *Facebook’s Response to House Energy and Commerce Questions for the Record* at 22 (June 29, 2018) <https://docs.house.gov/meetings/IF/IF00/20180411/108090/HHRG-115-IF00-Wstate-ZuckerbergM-20180411.pdf>.

to expand its reach by outsourcing to Business Partners the time, labor and money required to build Facebook's Platform on different devices and operating systems. In exchange, Facebook allowed these Business Partners to access users' content and information. Facebook partnered with a diverse set of companies including device makers, such as Blackberry and Huawei, and other types of internet companies, such as Alibaba, Yahoo, and Yandex. Facebook allowed users' content and information to be accessed by "tens of millions of mobile devices, game consoles, televisions and other systems" that were not in Facebook's direct control.<sup>154</sup>

434. These partnerships were built in part on "data reciprocity." Facebook and its partners agreed to exchange information about users' activities with each other. This was not disclosed to users.

435. Like Apps, the content and information that the Business Partners accessed varied. As on Graph API, Business Partners gained access not only TO the content and information of the user who downloaded or used the Facebook service that the Business Partner provided, but also to the content and information of the user's Friends.<sup>155</sup> Sandy Parakilas, a whistleblower and a former operations manager at Facebook, asserts that the same "feature" is behind both the Cambridge Analytica Scandal and Facebook's data sharing with device makers. In both cases, "developers had access" to a user's Friend data.<sup>156</sup> Indeed, Parakilas equated device makers to "apps."

436. For instance, Blackberry, had access to the App User's messages and other personal information of the App User's Friends, such as their political and religious preferences, education and work history, events they plan to attend, and whether they were currently online.<sup>157</sup> Some Business Partners, like Yahoo, were able to read the streams of users' and users' Friends posts, while others, like

---

<sup>154</sup> Gabriel J.X. Dance, et al., *Facebook Gave Device Makers Deep Access to Data on Users and Friends*, N.Y. Times (June 3, 2018), <https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html>.

<sup>155</sup> *Id.*

<sup>156</sup> Sandy Parakilas (@mixblendr), Twitter (June 4, 2018, 12:44 AM), <https://twitter.com/mixblendr/status/1003542895507501057>.

<sup>157</sup> Dance, et al., *Facebook Gave Device Makers Deep Access*, *supra* note 154.

Sony, Microsoft and Amazon, were able to obtain the users' and users' Friends emails.<sup>158</sup>

437. Facebook also gave Business Partners access to the unique Facebook identifiers of users, ("Facebook ID") including the user's Friends, and the user's Friends' Friends ("Friends of Friends"). For instance, Blackberry had access as recently as 2017 to the unique Facebook identifiers of Blackberry users', users' Friends, and users' Friends of Friends. The Wall Street Journal reported on the dangers associated with providing third parties Facebook users' unique ID in October 2010.<sup>159</sup> In that same article, the Journal reported that Facebook would stop giving this information to third parties due to privacy concerns:

"A Facebook user ID may be inadvertently shared by a user's Internet browser or by an application," the [Facebook] spokesman said. Knowledge of an ID "does not permit access to anyone's private information on Facebook," he said, adding that the company would introduce new technology to contain the problem identified by the Journal.<sup>160</sup>

438. In May 2015, Facebook recognized the need for an even more secure way to process IDs, and switched to "unique App IDs" whereby each App is now given a unique App ID.<sup>161</sup>

439. Despite the acknowledged risks of providing users' Facebook ID to third parties, Facebook continued giving Business Partners, such as BlackBerry and Yandex, access to this information.

440. Some Business Partners were able to download and store users' content and information directly to their servers much like App Developers.<sup>162</sup> Other Partners claimed to have kept the information on the device itself. However, in this instance, users' content and information could have

---

<sup>158</sup> Gabriel J.X. Dance, Michael LaForgia, and Nicholas Confessore, *As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants*, N.Y. Times (Dec. 18, 2018), <https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html>.

<sup>159</sup> Emily Steel and Geoffrey A. Fowler, *Facebook in Privacy Breach*, Wall Street Journal (Oct. 18, 2010), <https://www.wsj.com/articles/SB10001424052702304772804575558484075236968> ("The apps reviewed by the Journal were sending Facebook ID numbers to at least 25 advertising and data firms, several of which build profiles of Internet users by tracking their online activities.").

<sup>160</sup> *Id.*

<sup>161</sup> *Facebook Application Development FAQ*, Facebook for Developers, <https://developers.facebook.com/docs/apps/faq/> (last visited February 21, 2019).

<sup>162</sup> Steel and Fowler, *supra* note 159.

left the device when it was synced or backed up to the Partner's servers.

**7. Facebook Extended Certain “Whitelisted” Companies Access to Friends’ Information Despite Facebook’s Contrary Representations to Users.**

441. Following the FTC inquiry, at Facebook’s f8 Developers’ conference in April 2014, Facebook informed the public that it was restricting access to user content and information by cutting off third parties’ ability to download information via Graph API v1.0 and stated it would give App Developers one year, or until May 2015, to continue accessing Friends’ information.<sup>163</sup> Mark Zuckerberg announced “we are going to make it so now everyone has to choose to share their own data with an app themselves.”<sup>164</sup> Facebook unveiled its new theme “putting people first” and stated, “We are giving people more control over these experiences so they can be confident pressing the blue button.”<sup>165</sup>

442. Likewise, on April 28, 2015, Facebook’s Simon Cross commented on the transition to a more restrictive Graph API stating, “[I]f people don’t feel comfortable using Facebook and specifically logging in [to] Facebook and using Facebook in apps, we don’t have a platform, we don’t have developers.”<sup>166</sup> Cross further told reports that the privacy changes were the result of Facebook’s “People First” goal.<sup>167</sup>

443. However, Facebook did not disclose that, while restricting Graph API v1.0 for general third parties, Facebook allowed certain companies to continue accessing content and information of users and users’ Friends. This special access, termed “whitelisting,” allowed Apps to “access user data without permission” and “to circumvent users’ privacy [or] platform settings and access Friends’

---

<sup>163</sup> *f8 2014: Stability for Developers & More Control for People*, Facebook Newsroom (Apr. 30, 2018), <https://newsroom.fb.com/news/2014/04/f8-2014-stability-for-developers-and-more-control-for-people-in-apps/>.

<sup>164</sup> Larry Magid, *Zuckerberg Pledges More User Control of Facebook App Privacy –Unveils Anonymous Log-In*, Forbes (Apr. 30, 2014), <https://www.forbes.com/sites/larrymagid/2014/04/30/zuckerberg-pledges-more-user-control-of-app-privacy-unveils-anonymous-log-in/#7bea50036de7>.

<sup>165</sup> *f8 2014: Stability for Developers*, *supra* note 163.

<sup>166</sup> Josh Constatine, *Facebook Is Shutting Down Its API for Giving Your Friends’ Data to Apps*, TechCrunch (Apr. 28, 2015), <https://techcrunch.com/2015/04/28/facebook-api-shut-down/>.

<sup>167</sup> *Id.*



information, even when the user disabled the Platform.”<sup>168</sup> To facilitate whitelisting, Facebook developed and promulgated “Private Extended APIs,” which enabled App Developers to access content and information, including the content and information of users’ Friends, beyond that available to non-whitelisted applications. According to Facebook’s “Private Extended API Addendum,” Whitelisted Apps could “retrieve data or functionality relating to Facebook *that is not generally available under Platform*, which may include persistent authentication, photo upload, video upload, messaging and phonebook connectivity.”<sup>169</sup>

444. Such whitelisting extended to thousands of companies. According to the DCMS Committee, Facebook’s whitelisting “resulted in a large number of companies striking special deals,” and “[a] November 2013 email discussion reveals that Facebook was managing 5,200 Whitelisted Apps, including Lyft, AirBnB, and Netflix.”<sup>170</sup> Facebook granted these whitelisted companies special access in exchange for value provided by those companies to Facebook. The level of access varied by agreement based on Facebook’s relationship with the particular company and the purpose of the company’s App. The Whitelisted Apps all entered into lucrative agreements with Facebook to purchase advertising. Facebook began forming these agreements as early as 2013 and still allows some companies special access today.<sup>171</sup> These agreements conflict with Facebook’s statements regarding Graph API and its disclosures to users, in that Facebook stated Apps would no longer have access to users’ Friends’ data after May 2015.<sup>172</sup>

445. According to the DCMS Committee, “increasing revenues from major App developers was one of the key drivers behind the policy changes made by Facebook,” and “[t]he idea of linking

---

<sup>168</sup> DCMS Report, *supra* note 28 ¶ 83.

<sup>169</sup> *Id.* ¶ 85 (emphasis added).

<sup>170</sup> *Id.* ¶ 84.

<sup>171</sup> U.K. House of Commons, *Note by Damian Collins MP, Chair of the DCMS Committee: Summary of Key Issues from the Six4Three files* (Dec. 5, 2018), <https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Note-by-Chair-and-selected-documents-ordered-from-Six4Three.pdf>; Dance, et al, *As Facebook Raised a Privacy Wall*, *supra* note 158.

<sup>172</sup> *Changelog—Graph API*, Facebook for Developers, <https://web.archive.org/web/20141208030452/https://developers.facebook.com/docs/apps/changelog#> (last visited on Feb. 20, 2019).

access to Friends' data to the financial value of the developers' relationship with Facebook was a recurring feature of the documents" considered by the DCMS Committee.<sup>173</sup>

446. Facebook hid these whitelist agreements from users even after the Cambridge Analytica Scandal. In testimony to U.K. House of Commons, on April 26, 2018, Facebook's Chief Technical Officer Mike Schroepfer, responding to questions regarding the one-year transition period from Graph API v.1.0 to 2.0 during 2014 to 2015, failed to state that tens of companies were given special whitelist access beyond May 2015.<sup>174</sup> This was a material omission.

447. A day later, Facebook provided a response to questions from German Congressional Committees regarding Cambridge Analytica. In its response, Facebook stated:<sup>175</sup>

In addition to public APIs, Facebook also has some APIs that are available only to certain partners for specific uses. Generally these APIs provide access to public information, such as to enable news and media organizations to follow breaking news. . . .

448. This statement fails to materially describe any of the whitelisted companies or what access they had. Furthermore, contrary to this statement, Facebook granted tens of whitelisted companies access to users' non-public information.

449. Finally, the truth began to come to light on June 8, 2018, when the *Wall Street Journal* reported that Facebook struck whitelist deals allowing certain companies special access through APIs.<sup>176</sup> The report made clear that these agreements were separate from the custom deals Facebook entered into with Business Partners. The report also stated that Facebook struck these deals with "companies including Royal Bank of Canada and Nissan Motor Co., who advertised on Facebook or were valuable for other reasons."<sup>177</sup> The report identified Nuance Communications as getting whitelist

---

<sup>173</sup> DCMS Report, *supra* note 28, ¶ 87.

<sup>174</sup> Mike Schroepfer Testimony to U.K. House of Commons, *supra* note 147, at Q2202.

<sup>175</sup> Facebook responses to open questions from the 'Committee on Legal Affairs and Consumer Protection' and the 'Committee on Digital Agenda', Facebook Newsroom (Apr. 27, 2018), <https://fbnewsroomde.files.wordpress.com/2018/05/final-responses-to-german-committees.pdf>.

<sup>176</sup> Deepa Seetharaman and Kristen Grind, *Facebook Gave Some Companies Special Access to Additional Data About Users' Friends*, The Wall Street Journal (June 8, 2018), <https://www.wsj.com/articles/facebook-gave-some-companies-access-to-additional-data-about-users-friends-1528490406>.

<sup>177</sup> *Id.*

access until November 2015 for a “special news feed it had built” for Fiat Chrysler Automobiles.<sup>178</sup>

The report further stated:<sup>179</sup>

Early on, Facebook brokered special deals with certain companies, some people with knowledge of the deals said. “Ninety-nine percent of developers were treated the same, but 1% got special treatment because they accounted for all the value of the platform,” one former Facebook employee said, referring to popular apps and services that attracted users.

450. Clearly, Facebook granted special access to users’ information based on the value a company brought to Facebook. In short, Facebook traded access to its users’ information – without users’ knowledge or consent – in exchange for whitelist companies’ significant expenditures on Facebook advertising.

451. Facebook responded to this report, stating that a “small number” of partners had access to users’ Friends after May 2015. But Facebook did not identify any further whitelisted companies, or state what information these Developers had access to.

452. Then, in response to questions posed by the U.S. House of Representative on June 29, 2018, Facebook stated that 60 companies were “given a one-time extension of less than six months beyond May 2015 to come into compliance” with Facebook’s new API.<sup>180</sup>

453. The list of companies includes:

- ABCSocial, ABC Television Network
- Actiance
- Adium
- Anschutz Entertainment Group
- AOL
- Arktan / Janrain
- Audi
- biNu
- Cerulean Studios
- Coffee Meets Bagel
- DataSift

---

<sup>178</sup> *Id.*

<sup>179</sup> *Id.*

<sup>180</sup> *Facebook’s Response to House Energy and Commerce Questions for the Record*, *supra* note 153, at Pallone, Jr. § 4 ¶ 6.

- Dingtone
- Double Down Interactive
- Endomondo
- Flowics, Zauber Labs
- Garena
- Global Relay Communications
- Hearsay Systems
- Hinge
- HiQ International AB
- Hootsuite
- Krush Technologies
- LiveFyre / Adobe Systems
- Mail.ru
- MiggoChat
- Monterosa Productions Limited
- never.no AS
- NIKE
- Nimbuzz
- Nissan Motor Co. / Airbiquity Inc.
- Oracle
- Panasonic
- Playtika
- Postano, TigerLogic Corporation
- Raidcall
- RealNetworks, Inc.
- RegED / Stoneriver RegED
- Reliance / Saavn
- Rovi
- Salesforce / Radian6
- SeaChange International
- Serotek Corp.
- Shape Services
- Smarsh
- Snap
- Social SafeGuard
- Socialeyes LLC
- SocialNewsdesk
- Socialware / Proofpoint
- SoundayMusic
- Spotify
- Spredfast
- Sprinklr / Sprinklr Japan
- Storyful Limited / News Corp
- Tagboard

- Telescope
- Tradable Bits, TradableBits Media Inc.
- UPS
- Vidpresso
- Vizrt Group AS
- Wayin

454. According to Facebook, during this six-month extension, these companies continued to have access to the content and information of users and users' Friends. Facebook did not clarify why this group of companies were given special access to this content and information. Furthermore, subsequent reporting has revealed that some companies listed above were given access beyond the six months, while additional companies should have been included on this list to Congress.<sup>181</sup>

455. In its congressional testimony, Facebook also listed five additional companies that "could have accessed limited friends' data as a result of API access that they received in the context of a beta test."<sup>182</sup> These companies include:

- Activision / Bizarre Creations
- Fun2Shoot
- Golden Union Co.
- IQ Zone / PicDial
- PeekSocial

456. Facebook has not provided an explanation for why these five companies received this special access.

457. Next, on December 5, 2018, the UK Parliament released a cache of documents internal to Facebook.<sup>183</sup> These documents consist of internal emails shared between Facebook employees; emails with outside Developers and Business Partners; and internal presentation materials. These documents showed a further series of undisclosed companies that Facebook traded whitelist access to. They include:

- Airbnb
- Badoo

---

<sup>181</sup> Dance, et al, *As Facebook Raised a Privacy Wall*, *supra* note 158.

<sup>182</sup> *Facebook's Response to House Energy and Commerce Questions for the Record*, *supra* note 153, at Pallone, Jr. § 4 ¶ 7.

<sup>183</sup> *Note by Damian Collins MP, Chair of the DCMS Committee: Summary of Key Issues from the Six4Three files*, *supra* note 171.

- Bumble
- Hot or Not
- Lyft
- Netflix

458. The released documents reveal that Facebook granted these companies varying levels of access depending on the App's needs and on Facebook's relationship with the App. Several of the Apps listed above had access to non-App Friend lists. Others also had access to the private messages of App users.

459. Facebook responded:

We changed our platform policies in 2014/15 to prevent apps from requesting permission to access friends' information. The history of Cambridge Analytica shows this was the right thing to do. For most developers, we also limited their ability to request a list of who someone's friends were, unless those friends were also using the developer's app. **In some situations, when necessary, we allowed developers to access a list of the users' friends. This was not friends' private information but a list of your friends (name and profile pic).**

...

In addition, white lists are also common practice when testing new features and functionality with a limited set of partners before rolling out the feature more broadly (aka beta testing). Similarly, it's common to help partners transition their apps during platform changes to prevent their apps from crashing or causing disruptive experiences for users.<sup>184</sup>

460. Facebook's statement is false because Facebook's internal emails and subsequent news articles have revealed that Hootsuite, Netflix, Royal Bank of Canada and Spotify also had access to users' messenger mailbox, which would include messages sent from users' Friends.

461. The statement is also misleading. Since May 2010, users could set a non-public privacy designation for their Friends list at any time. Thus, even where the App User and her Friends set their Friends list to private, Whitelisted Apps who gained access to the App User's Friends list would still be able to see all of the Friends of that user. For Friends seeking to limit who could view their social connections, this was a violation of privacy.

---

<sup>184</sup> Mark Zuckerberg, Facebook (Dec. 5, 2018), <https://newsroom.fb.com/news/2018/12/response-to-six4three-documents/> (emphasis added).

462. On December 18, 2018, the *New York Times* reported that Facebook had entered into over 150 previously undisclosed data sharing agreements with a variety of organizations. The report stated:

Facebook shared data with more than 150 companies — not only tech businesses but automakers and media organizations — through apps on its platform even if users disabled sharing. Apps from many of these “integration partners” never even showed up in user application settings, with the company considering them an extension of its own network. The deals dated back as far as 2010 and were all active in 2017, with some still in effect this year.”<sup>185</sup>

463. The Times identified Spotify, Netflix and the Royal Bank of Canada as being able to “read, write and delete Facebook users’ private message, and to see everyone on a message thread.”<sup>186</sup> The report stated that Facebook’s own internal documents show that these companies had access to users’ messages beyond the time that the companies needed to integrate Facebook into their systems. For instance, “Spotify, which could view messages of more than 70 million users a month, still offers the option to share music through Facebook Messenger.”<sup>187</sup> Yet, Facebook had previously identified Spotify in its list to Congress as only having access for six months beyond May 2015.

464. Facebook also had purportedly removed access to users’ mailboxes in Graph API v2.4, released on July 8, 2015, and had purportedly removed this permission for all APIs on October 6, 2015.<sup>188</sup> Thus, users reasonably expected App Developers to no longer have access to any Facebook messages after October 2015 at the latest. However, as stated above, Facebook continued allowing many companies to access messages beyond this date.

**D. Facebook Failed to Monitor and to Protect User Content and Information from Third Parties’ Unauthorized Use.**

465. While Facebook allowed third-party App Developers, whitelisted companies and Business Partners to access incredible amounts of users’ content and information, Facebook failed to implement reasonable security measures, such as conducting regular audits and monitoring third

---

<sup>185</sup> Dance, et al, *As Facebook Raised a Privacy Wall*, *supra* note 158.

<sup>186</sup> *Id.*

<sup>187</sup> *Id.*

<sup>188</sup> *Changelog*, *supra* note 104.



parties' access and use of users' content and information. Facebook also failed to ensure that third parties complied with its Platform and Privacy policies. Facebook's failure to act was a direct result of its reckless quest for growth at the expense of users' privacy.

**1. Facebook Has a History of Discarding Its Promises to Protect User Privacy in Reckless Pursuit of Growth.**

466. Throughout its history, Facebook has repeatedly ignored users' privacy interests and its own promises to protect user content and information in a reckless quest to maximize its growth and maximize its profits. In light of the company's history of privacy abuses, it is apparent that the company's motto to "move fast and break things" applies even to users' privacy.

467. In 2006, Facebook launched its News Feed feature to display users' posts on their Friends' and networks' pages. This feature was immediately controversial because users' posts were automatically revealed regardless of users' intention to keep these posts private. Zuckerberg's response to this controversy was that "we did a bad job of explaining what the new features were and an even worse job of giving you control of them."<sup>189</sup>

468. In 2007, Facebook launched Beacon, a feature that automatically shared users' website and App history with advertisers, who in turn shared users' activity with other Facebook users on the third-party sites. Users were not given the opportunity to opt-out of this feature, and were shocked to discover their formerly inaccessible activities had been repackaged and revealed by Facebook in order to attract Business Partners and hone its advertising program. Third-party participants in the Beacon program not only received user content and information, the sites also gave Facebook ad-targeting data. After myriad privacy complaints and a class action lawsuit, Beacon was shut down. In response, Zuckerberg stated, "We've made a lot of mistakes building this feature, but we've made even more with how we've handled them. We simply did a bad job with this release, and I apologize for it."<sup>190</sup> Yet, Facebook continued to violate users' expectation of privacy.

469. In May 2008, the Canadian Internet Policy and Public Interest Clinic ("CIPPIC") filed a

<sup>189</sup> Mark Zuckerberg, *An Open Letter From Mark Zuckerberg*, Facebook (Sept. 8, 2006), <https://www.facebook.com/notes/facebook/an-open-letter-from-mark-zuckerberg/2208562130/>.

<sup>190</sup> Mark Zuckerberg, *Thoughts on Beacon*, Facebook (Dec. 5, 2007), <https://www.facebook.com/notes/facebook/thoughts-on-beacon/7584397130/>.

complaint against Facebook with the Canadian Privacy Commissioner (“CPC”) over a number of user privacy concerns, including the user content and information shared by Facebook with third party App Developers without express consent by users. The CPC launched an investigation in response to CIPPIC’s complaint, which resulted in Facebook agreeing to user consent-centered reform in August 2009. The CPC’s announcement indicated the following:

Facebook has agreed to retrofit its application platform in a way that will prevent any application from accessing information until it obtains express consent for each category of personal information it wishes to access. Under this new permissions model, users adding an application will be advised that the application wants access to specific categories of information. The user will be able to control which categories of information an application is permitted to access. There will also be a link to a statement by the developer to explain how it will use the data.<sup>191</sup>

470. Despite users’ and regulators’ repeated efforts to get Facebook to rein in its privacy abuses, including private litigation and the CPC settlement, Facebook continued to exploit users’ content and information for commercial gain without consent.

471. In November 2009, Facebook changed its Terms of Service to greatly expand the amount of personal information categorized as available to the public. *See supra* at IV.B. In response to the change in privacy settings, ten privacy organizations, including the Electronic Privacy Information Center (“EPIC”), filed complaints to the FTC alleging that Facebook had changed users’ privacy settings and disclosed personal content and information to third parties without consent. EPIC warned “[t]he Facebook Platform transfers Facebook users’ personal data to application developers without users’ knowledge or consent.”<sup>192</sup>

472. Zuckerberg responded with an apology to users, stating that, “[s]ometimes we move too fast—and after listening to recent concerns, we’re responding.”<sup>193</sup> Zuckerberg vowed to add privacy

---

<sup>191</sup> *News Release, Facebook Agrees to Address Privacy Commissioner’s Concerns*, Office of the Privacy Commissioner of Canada (Aug. 27, 2009), [https://www.priv.gc.ca/en/opc-news/news-and-announcements/2009/nr-c\\_090827/](https://www.priv.gc.ca/en/opc-news/news-and-announcements/2009/nr-c_090827/).

<sup>192</sup> *Facebook Privacy*, Electronic Privacy Information Center (last accessed on February 11, 2019), <https://www.epic.org/privacy/facebook/>.

<sup>193</sup> Mark Zuckerberg, *From Facebook, Answering Privacy Concerns with New Settings*, The Wash. Post (May 24, 2010), <http://www.washingtonpost.com/wp-dyn/content/article/2010/05/23/AR2010052303828.html>.

controls that are simpler to use, stating, “Many people choose to make some of their information visible to everyone so people they know can find them on Facebook. We already offer controls to limit the visibility of that information and we intend to make them even stronger.”<sup>194</sup>

473. In October 2010, the *Wall Street Journal* reported that Facebook had been sending users’ names and Facebook identification numbers to its advertisers without users’ knowledge and consent.<sup>195</sup>

474. Despite continuous and consistent feedback from users, privacy advocates, and regulators, in July 2010, while giving a speech at a technology awards show in San Francisco, Zuckerberg announced that privacy is no longer a “social norm.”<sup>196</sup> Zuckerberg stated, “People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time.”<sup>197</sup> Zuckerberg’s proclamation that social norms have changed serves as a thin veil to Facebook’s continued violations of users’ trust.

475. On November 29, 2011, Facebook agreed to settle the FTC charges that it had deceived users by telling them they could keep their information on Facebook private and then repeatedly allowed it to be shared and made public without their consent. The FTC adopted the final Consent Order on August 10, 2012. The order requires Facebook to take steps including, “giving consumers clear and prominent notice and obtaining their express consent before sharing their information beyond their privacy settings, by maintaining a comprehensive privacy program to protect consumers’ information, and by obtaining biennial privacy audits from an independent third party.”<sup>198</sup>

476. Facebook has also failed to implement features that would help users secure their information on Facebook. For example, in April 2014, at the f8 Developer Conference, Zuckerberg announced a new anonymous login feature for users. This feature would allow users to try an App

---

<sup>194</sup> *Id.*

<sup>195</sup> Steel and Fowler, *supra* note 159.

<sup>196</sup> Bobbie Johnson, *Privacy no longer a social norm, says Facebook founder*, The Guardian (Jan. 10, 2010), <https://www.theguardian.com/technology/2010/jan/11/facebook-privacy>.

<sup>197</sup> *Id.*

<sup>198</sup> *FTC approves Final Settlement With Facebook*, Federal Trade Commission (Aug. 10, 2012), <https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook>.

without sharing any content and information.<sup>199</sup> Mark Zuckerberg made this announcement in order to reassure users' that Facebook valued their privacy, stating that this will allow users to "try apps without fear."<sup>200</sup> Despite this announcement, the anonymous login feature was never taken out of development.

477. In May 2018, at Facebook's f8 conference, Zuckerberg announced plans to add a "Clear History" feature that would enable users to see the websites and Apps that send their information to Facebook when they use them. Zuckerberg promised that this feature would allow users to "clear this information from their accounts, and turn off [Facebook's] ability to store it . . . going forward."<sup>201</sup>

478. Zuckerberg made this announcement in the wake of the Cambridge Analytica Scandal and claimed Facebook would release this feature "in the coming months," but has not as of this filing.<sup>202</sup> Reporting suggests that Zuckerberg made this announcement for the optics without any plan on how it would actually work.<sup>203</sup> As of the date of this filing, Facebook has not implemented a Clear History feature.

479. While Facebook promised users privacy and security, in reality, Facebook has continued to follow its relentless quest for growth.

480. For example, in 2016, Andrew Bosworth, a vice president at Facebook, defended the company's growth tactics in an internal memo. Bosworth's memo explains that despite any ramifications, Facebook's growth is "\*de facto\* good":

---

<sup>199</sup> *Id.*

<sup>200</sup> *Facebook's Mark Zuckerberg Introduces Anonymous Login*, YouTube, at 01:10 (Apr. 30, 2014), <https://www.youtube.com/watch?v=rOCcYRIZUGU>.

<sup>201</sup> Letter from Facebook, Inc. to Chairman Greg Walden, Ranking Member Frank Pallone, Energy & Commerce Committee, and U.S. House of Representatives, *Facebook's Response to House Energy and Commerce Questions for the Record*, at Walden § 2(b) ¶ 7 (June 29, 2018) <https://docs.house.gov/meetings/IF/IF00/20180411/108090/HHRG-115-IF00-Wstate-ZuckerbergM-20180411.pdf>.

<sup>202</sup> Chris Welch, *Facebook to introduce clear history privacy tool in coming months*, Verge (May 1, 2018), <https://www.theverge.com/2018/5/1/17307346/facebook-clear-history-new-privacy-feature>.

<sup>203</sup> Ben King, *Mark Zuckerberg Promised A Clear History Tool Almost A Year Ago. Where Is It?*, BuzzFeed.News (Feb. 22, 2019), <https://www.buzzfeednews.com/article/ryanmac/facebook-privacy-optics-clear-history-zuckerberg>.

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

...

[M]ake no mistake, growth tactics are how we got here. If you joined the company because it is doing great work, that's why we get to do that great work. We do have great products but we still wouldn't be half our size without pushing the envelope on growth. Nothing makes Facebook as valuable as having your friend on it, and no product decisions have gotten as many friends on as the ones made in growth.<sup>204</sup>

481. The reason that "growth was good" is that it fueled Facebook's business model as data broker.

482. While growth was good for Facebook's business model, it left users' susceptible to unfettered access by third parties.

## **2. Facebook Ignored Internal Warnings Regarding Risks Posed by Third Parties' Access to Users' Content and Information.**

483. Numerous Facebook employees and investors voiced concerns regarding the privacy risks posed by third party access to Facebook users' content and information, including directly to Mr. Zuckerberg and others in Facebook leadership.

484. For instance, during the lead up to Facebook's 2012 initial public offering, Facebook's operations manager, Sandy Parakilas, raised concerns about Facebook's handling of misuse of user data by App Developers accessing user content and information from Graph API v1.0. Parakilas described concerns including that as of 2010, Facebook had never audited any App Developers using Facebook's Graph API v1.0, and he also raised concerns about data vulnerabilities on Facebook Platform to Facebook executives.<sup>205</sup> Parakilas was also concerned that when Developers violated Facebook's Data

---

<sup>204</sup> Ryan Mac, Charlie Warzel, and Alex Kantrowitz, *Growth At Any Cost: Top Facebook Executive Defended Data Collection in 2016 Memo – And Warned That Facebook Could Get People Killed*, BuzzFeed News (Mar. 29, 2018, 6:36pm), <https://www.buzzfeednews.com/article/ryanmac/growth-at-any-cost-top-facebook-executive-defended-data#.lbeaWaPKk4>.

<sup>205</sup> U.K. House of Commons, Digital, Culture, Media and Sport Committee, Testimony of Sandy Parakilas (Mar. 21, 2018), at Q1191-194, <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/fake-news/oral/80809.html>.

Use Policy, Facebook users were (to the best of his knowledge) never notified that Developers had inappropriately accessed their data.<sup>206</sup>

485. In a November 2017 op-ed in the *New York Times*, Parakilas wrote of the reaction he received from Facebook personnel after he raised concerns about App Developers misusing user content and information obtained through Graph API v1.0:

[W]hen I was at Facebook, the typical reaction I recall looked like this: try to put any negative press coverage to bed as quickly as possible, with no sincere efforts to put safeguards in place or to identify and stop abusive developers. When I proposed a deeper audit of developers' use of Facebook's data, one executive asked me, "Do you really want to see what you'll find?" The message was clear: The company just wanted negative stories to stop. It didn't really care how the data was used.<sup>207</sup>

486. Following the Cambridge Analytica Scandal, The Guardian reported in March 2018 on Parakilas' concerns. Parakilas "always assumed there was something of a black market" for Facebook data that had been passed to external developers; yet, when he told other executives the company should proactively "audit developers directly and see what's going on with the data" they were not receptive. One executive at Facebook "advised [Parakilas] against looking too deeply at how the data was being used." Facebook, Parakilas said, "felt that it was better not to know."<sup>208</sup>

487. On March 21, 2018, Parakilas testified to the U.K. House of Commons, stating that Facebook had few ways of discovering abuse or enforcing on abuse once it was discovered. Parakilas stated:<sup>209</sup>

[Facebook] could do one of four things: it could call up the developer and demand to know what they were doing with the data; it could demand an audit of the developer's application, their data storage, and that was a right that was granted to Facebook in [their] policies, the platform policies; it could delete the app and potentially ban the developer

---

<sup>206</sup> *Id.* at Q1200-201.

<sup>207</sup> Sandy Parakilas, *We Can't Trust Facebook to Regulate Itself*, N.Y. Times (Nov. 19, 2017), <https://www.nytimes.com/2017/11/19/opinion/facebook-regulation-incentive.html>.

<sup>208</sup> Paul Lewis, 'Utterly horrifying': ex-Facebook insider says covert data harvesting was routine, The Guardian (Mar. 20, 2018), <https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas>.

<sup>209</sup> U.K. House of Commons, Digital, Culture, Media and Sport Committee, Testimony of Sandy Parakilas, *supra* note 205, at Q1188.

from using Facebook Platform or even using other Facebook products such as advertising; or it could sue the developer and pursue that app.

...

In terms of the frequency of the use of those four means, I can tell you that in my experience, during my 16 months in that role at Facebook, I do not remember a single physical audit of a developer's storage. I do not remember that happening once. There were only a handful of lawsuits and bans. Those were both quite rare. Mostly what I did was call developers and threaten to do other things, basically saying that they needed to follow the policies. That was effectively the main enforcing mechanism during my time.

The other thing to note is that Facebook had relatively low detection of policy violations and most of the reports that it got about policy violations were either from the press or from other developers who were competitors of a particular company and they would call up or talk to someone at Facebook and say, 'I think this person is doing X, Y and Z,' and they were doing that largely for competitive reasons.

488. Parakilas raised concerns that these four options were all insufficient enforcement mechanisms.

489. Also, when asked whether the data could be used to target advertising, Parakilas responded that while there were rules "attempting to prevent developers from using the data targeting advertising . . . there was very little detection, or enforcement and it is very difficult to tell how an ad is being targeted . . . ." <sup>210</sup> Parakilas noted that he and others raised multiple concerns to executives that users' information could wind up in the hands of data brokers but, Parakilas said, Facebook found that was a "risk that they were willing to take." <sup>211</sup>

490. Parakilas further testified that he raised concerns about the lack of oversight into the flow of users' data. In a PowerPoint presentation Parakilas mapped out data vulnerabilities of the Facebook platform and showed that presentation to senior executives at the company. Some of those executives are still at Facebook today.

491. Parakilas also testified that Facebook's business model depended on this open and unfettered access to users' data. Parakilas stated: <sup>212</sup>

---

<sup>210</sup> *Id.* at Q1210.

<sup>211</sup> *Id.* at Q1215.

<sup>212</sup> *Id.* at Q1209.



[T]he ability to access a tremendous amount of data was a selling point to developers and Facebook wanted a lot of developers to build a lot of applications because they would draw more people to use Facebook more and more. Developers would for free build features that Facebook did not have itself, and the way that it got developers to want to go through Facebook was, first, they would give the huge audience of Facebook to the developer so you could get a lot of users very quickly and, secondly, you could get a ton of data from Facebook to build your application and understand those users.

492. Indeed, Parakilas states that Facebook’s model was to “grow the platform as quickly as possible, and data was one of the key ways to do that.”<sup>213</sup>

493. Likewise, in October 2016, Roger McNamee (an early investor in Facebook) attempted to engage with Facebook’s leadership regarding the risks posed by Facebook’s failure to protect its users. McNamee sent a draft of an op-ed outlining security risks of election interference on Facebook to Mr. Zuckerberg and Ms. Sandberg ahead of publishing. According to Mr. McNamee:<sup>214</sup>

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

494. And in July 2017, Alex Stamos, Facebook’s then-Chief of Security, raised similar security and privacy concerns, stating, “We have made intentional decisions to give access to data and systems to engineers to make them ‘move fast’ but that creates other issues for us.”<sup>215</sup> Stamos raised these concerns in the context of having authored a white paper that was later scrubbed for mentions of Russia. Facebook now admits that it was too slow to act on this issue.

495. Moreover, internal emails released by the DCMS Committee reveal that the highest

---

<sup>213</sup> *Id.* at Q1214./

<sup>214</sup> Roger McNamee, *How to Fix Facebook – Before It Fixes Us*, Wash. Monthly, (Jan. 2018) <https://washingtonmonthly.com/magazine/january-february-march-2018/how-to-fix-facebook-before-it-fixes-us/>.

<sup>215</sup> Zack Whittaker, *Leaked: Facebook security boss says its corporate network is run “like a college campus”*, ZDNet (Oct. 19, 2017), <https://www.zdnet.com/article/leaked-audio-facebook-security-boss-says-network-is-like-a-college-campus/>.



levels of Facebook’s leadership were aware of the risk of sharing user information with App Developers, but disregarded that risk because it did not present a direct threat to Facebook’s business interests. For example, Zuckerberg stated in an internal email dated October 27, 2012 that “I’m generally sceptical [sic] that there is as much data leak strategic risk as you [Sam Lessin] think.”<sup>216</sup> Further, Zuckerberg stated that “*I agree there is clear risk on the advertiser side,*” and “I think *we leak info to developers*, but I just can’t think if [sic] instances where that data has leaked from developer to developer and caused a real issue for us.”<sup>217</sup> As the DCMS Committee noted, this is, “of course, exactly what happened during the Cambridge Analytica scandal.”<sup>218</sup>

496. Despite numerous warnings regarding misuse of user content and information by third parties, including potential harm to national security and election integrity in the United States, year after year, Facebook allowed third parties unmonitored access to users’ content and information.

### **3. Facebook Failed to Monitor Business Partners’ and Whitelisted Companies’ Use of Users’ Content and Information.**

497. On November 12, 2018, the *New York Times* reported on another area in which Facebook failed to protect users’ content and information against misuse: Facebook’s failure to monitor Business Partners’ access to and use of users’ content and information.<sup>219</sup> Facebook had agreed under the FTC Consent Decree to have PricewaterhouseCoopers (“PwC”) periodically assess its oversight of Business Partners. The article described Facebook’s disclosure to Senator Ron Wyden’s office that in its 2013 initial assessment report, PwC identified a problem with how Facebook was monitoring certain Business Partners. The *Times* published a copy of the letter, which stated that “[t]here is limited evidence retained to demonstrate that Facebook monitored or assessed the service provider’s compliance with Facebook’s Data Use Policies,” and “[l]ack of comprehensive monitoring makes it more difficult to detect inappropriately implemented privacy settings within these third-party developed

---

<sup>216</sup> DCMS Report, *supra* note 28, ¶ 98.

<sup>217</sup> *Id.* ¶ 98 (emphases added).

<sup>218</sup> *Id.*

<sup>219</sup> Nicholas Confessore, et al., *Facebook Failed to Police How Its Partners Handled User Data*, N.Y. Times (Nov. 12, 2018), <https://www.nytimes.com/2018/11/12/technology/facebook-data-privacy-users.html>.

applications.”<sup>220</sup>

498. Wyden’s aide, based on a review of unredacted versions of PwC’s later 2015 and 2017 assessment reports, told the *Times* that while PwC did not identify the same problem in the later reports, there was “no evidence that Facebook had ever addressed the original problem.”<sup>221</sup> Rather, it appeared that Facebook had simply changed the assessment methodology that PwC applied, making it easier for Facebook to “comply.”

499. Sandberg appeared for questioning before the United States Senate on September 4, 2018. At that hearing, Wyden pressed Sandberg to release the unredacted PwC assessments, calling parts of the reports “very troubling.”<sup>222</sup> Sandberg and Facebook did not release unredacted reports, and to date, have refused to produce them to Plaintiffs in this litigation.<sup>223</sup>

500. Senator Wyden’s comments as well as reporting by The New York Times reveal Facebook’s failure to adequately monitor Business Partners’ access to and subsequent use of users’ content and information.

501. Similarly, in its 2011 Complaint, the FTC “found that Facebook misrepresented its claims regarding their app oversight programme, specifically the ‘verified apps programme’, which was a review allegedly designed to give users additional assurances and help them identify trustworthy applications.”<sup>224</sup> Contrary to Facebook’s claims, “[t]he review was non-existent and there was no oversight of those apps,” and consequently some Apps, such as Yelp and Rotten Tomatoes, “were able to circumvent users’ privacy settings or platform settings, and to access friends’ information as well as users’ information, such as birthdays and political affiliation, even when the user disabled the

---

<sup>220</sup> Kevin Martin, *Letter to Senator Ron Wyden*, Oct. 10, 2018, available at <https://int.nyt.com/data/documenthelper/480-facebook-wyden-letter-data-privacy/078dfb39ba0b2fa70867/optimized/full.pdf#page=1>.

<sup>221</sup> Confessore, et al., *Facebook Failed to Police*, *supra* note 219.

<sup>222</sup> Mary Clare Jalonick and Barbara Ortutay, *WATCH: Twitter’s Jack Dorsey, Facebook’s Sheryl Sandberg testify to Congress on foreign election interference* at 58:30, PBS (Sept. 5, 2018, 5:42pm) ; <https://www.pbs.org/newshour/nation/watch-live-twitters-jack-dorsey-facebooks-sheryl-sandberg-testify-to-congress-on-foreign-election-interference>.

<sup>223</sup> *Id.* at 58:50.

<sup>224</sup> DCMS Report, *supra* note 28, ¶ 88.

platform.”<sup>225</sup>

502. Likewise, the DCMS Report found that Facebook not only failed to audit or monitor Apps for evidence of malfeasance relating to user content and information, but also willfully turned a blind eye to Apps that it knew were misusing user content and information. Thus, the DCMS Committee stated that “Facebook has not provided us with one example of a business excluded from its platform because of serious data breaches,”<sup>226</sup> and “Facebook acts only when serious breaches become public.”<sup>227</sup> Further, “[f]ar from Facebook acting against ‘sketchy’ or ‘abusive’ apps, of which action it has produced no evidence at all, *it, in fact, worked with such apps as an intrinsic part of its business model.*”<sup>228</sup>

**4. Facebook Failed to Limit Business Partners’ and Whitelisted Companies’ Access to Users’ Content and Information.**

503. Facebook also allowed its Business Partners and other whitelisted companies to access users’ information beyond what was necessary for the specific purpose for which Facebook has asserted access was granted. For example, where third parties were granted access to support a specific function and that function was discontinued, Facebook failed to cut off access.

504. On December 18, 2018, the *New York Times* published another article detailing Facebook’s data sharing deals with Business Partners and whitelisted companies.<sup>229</sup> The article highlighted several companies that had discontinued their Facebook partnerships but, as late as 2017, still had access to users’ personal information. For example, the Royal Bank of Canada and Netflix had access to users’ Facebook messages after they had deactivated the related feature that incorporated it.<sup>230</sup> Up to 2017, Yahoo had access to users’ newsfeed—including posts from users’ Friends—for 100,000

---

<sup>225</sup> *Id.*

<sup>226</sup> *Id.* ¶ 134.

<sup>227</sup> *Id.* ¶ 133.

<sup>228</sup> *Id.* (emphasis added).

<sup>229</sup> Dance, et al, *As Facebook Raised a Privacy Wall*, *supra* note 158.

<sup>230</sup> *Id.*

users per month for a feature that Yahoo had discontinued in 2012.<sup>231</sup>

505. The *New York Times* itself was one of nine media companies that in 2017, still “had access [to] users’ friend lists for an article-sharing application it had discontinued in 2011.”<sup>232</sup>

506. In addition, Facebook continued allowing Microsoft’s Bing, Pandora and Rotten Tomatoes to access users’ content and information as late as 2017.<sup>233</sup> Facebook represented that it shared user content and information to allow these companies to implement Facebook’s instant personalization feature. Though Facebook ended its instant personalization feature in 2014, it continued allowing these three companies to access users’ content and information as late as 2017.

507. Likewise, Yandex, a Russian search engine and Business Partner to Facebook, still had access as late as 2017 to “Facebook’s unique user IDs even after the social network stopped sharing them with other applications, citing privacy risks.”<sup>234</sup> Facebook continued allowing this access even though the company “has long been suspected of having special ties to the Kremlin.”<sup>235</sup>

508. Facebook’s failure to shut down access to users’ content and information when the basis for doing so had become obsolete speaks to Facebook’s cavalier attitude toward users’ privacy.

509. At least two of Facebook’s Business Partners have confirmed that Facebook did not audit their access to users’ information. When asked by the *New York Times*, neither BlackBerry nor Yandex could find evidence that Facebook ever audited them or their access to user data.<sup>236</sup>

##### **5. Facebook Allowed Business Partners and Whitelisted Companies to Deceive Users About Their Access to Users’ Content and Information.**

510. Facebook purposefully allowed its Business Partners to hide their access from users and to share information even where users expressly attempted to prevent this access:<sup>237</sup>

---

<sup>231</sup> Nicholas Confessore, et. al, *Facebook’s Data Sharing and Privacy Rules: 5 Takeaways From Our Investigation*, N.Y. Times (Dec. 18, 2018), <https://www.nytimes.com/2018/12/18/us/politics/facebook-data-sharing-deals.html>.

<sup>232</sup> Dance, et al, *As Facebook Raised a Privacy Wall*, *supra* note 158.

<sup>233</sup> *Id.*

<sup>234</sup> *Id.*

<sup>235</sup> Fred Vogelstein, *Why Should Anyone Believe Facebook Anymore?*, *Wired* (Dec. 19, 2018), <https://www.wired.com/story/facebook-data-sharing-privacy-investigation/>

<sup>236</sup> Dance, et al, *As Facebook Raised a Privacy Wall*, *supra* note 158.

<sup>237</sup> *Id.*

Facebook empowered Apple to hide from Facebook users all indicators that its devices were asking for [Facebook user] data. Apple devices also had access to the contact numbers and calendar entries of people who had changed their account settings to disable all sharing, the records show.

511. Facebook’s “comprehensive privacy program,” which the Company implemented following the FTC Consent Decree in 2012, had significant limitations that were not disclosed to users.<sup>238</sup>

[T]he privacy program faced some internal resistance from the start, according to four former Facebook employees with direct knowledge of the company’s efforts. Some engineers and executives, they said, considered the privacy reviews an impediment to quick innovation and growth. And the core team responsible for coordinating the reviews — numbering about a dozen people by 2016 — was moved around within Facebook’s sprawling organization, sending mixed signals about how seriously the company took it, the ex-employees said.

*Critically, many of Facebook’s special sharing partnerships were not subject to extensive privacy program reviews, two of the former employees said.* Executives believed that because the partnerships were governed by business contracts requiring them to follow Facebook data policies, they did not require the same level of scrutiny. The privacy team had limited ability to review or suggest changes to some of those data-sharing agreements, which had been negotiated by more senior officials at the company.

Facebook officials said that members of the privacy team had been consulted on the sharing agreements, but that the level of review “depended on the specific partnership and the time it was created.”

512. Thus, even where Facebook did implement its privacy program, it exempted certain third parties from review. Facebook has admitted that certain partnerships are “high-touch relationships” and that they rarely managed them closely.<sup>239</sup>

513. Moreover, internal documents show that Facebook may not have maintained adequate records of its own agreements with third parties. In December 2014, DNP, a Facebook Business Partner that allows Walgreens customers to access their Facebook photos at kiosks in Walgreens retail

---

<sup>238</sup> *Id.* (emphasis added)

<sup>239</sup> *Id.*

locations, contacted Facebook about changes to their platform access on Graph API v2.0.<sup>240</sup> The email was then shared internally between Eddie O’Neil, Konstantinos Papamiltiadis and Simon Cross.

514. In the email chain, the Facebook employees note that they are unable to locate the original contract between Facebook and Walgreens/DNP.<sup>241</sup> Facebook’s failure to locate its contractual agreement with DNP speaks to Facebook’s larger failure to adequately monitor whether third parties were accessing users’ information in compliance with their agreements.

515. In sum, Facebook failed to protect users’ content and information in numerous ways despite its obligations under the FTC Consent Order to do so. Facebook failed to implement an effective independent review of its privacy protections by excluding its Business Partners from the review and manipulating testing rather than addressing exceptions detected by PwC. Additionally, Facebook failed to audit the access it granted to third parties to ensure that third party access to user content and information was limited to the purpose for which it was granted; and Facebook failed to ensure its partners complied with Facebook’s policies or even the contract between Facebook and the third party.

**6. Facebook Also Took No Action to Ensure App Developers Followed Its Platform and Privacy Policies.**

516. Facebook’s Platform Policy, which governed its relationship with third-party App Developers, like GSR, and their operation on the Facebook Platform, prohibited the transfer and sale of consumer data accessed from Facebook. And during 2010-2015, Facebook’s user Privacy Policy stated that applications would be allowed to use App users’ Friends’ information “only *in connection with* the person that gave the permission and no one else.” Yet, Facebook did not take any meaningful action to enforce compliance with either its Platform Policy with third parties or its Privacy Policy with users; instead, Facebook permitted App Developers, like GSR, to harvest and sell users’ information without oversight.

517. In the case of Cambridge Analytica, GSR’s “End User Terms and Conditions” were

---

<sup>240</sup> *Note by Damian Collins MP, Chair of the DCMS Committee: Summary of Key Issues from the Six4Three files, supra* note 171.

<sup>241</sup> *Id.*

posted publicly and were provided to Facebook. These terms expressly state that GSR intended to “sell” and “license (by whatever means and on whatever terms)” the personal content it obtained through the MyDigitalLife App. Kogan has stated that he “never heard a word” from Facebook concerning his intent to “sell” data even though he had publicly posted his intention to do so for a year and a half before Facebook discontinued his access.

518. Facebook has admitted that it did not monitor the policies of Apps operating on its Platform.<sup>242</sup>

519. In May 2014, in advance of Facebook’s switch to Graph API v2.0, Kogan requested extended permissions. Facebook denied this request, but continued to allow Kogan’s App to access users’ information on Graph API v1.0 until May 1, 2015. Zuckerberg himself has admitted that if Facebook had acted to disable Graph API v1.0 one year earlier it could have prevented the Cambridge Analytica Scandal:

We’ve focused on preventing abusive apps for years, and that was the main purpose of this major platform change starting in 2014. In fact, this was the change required to prevent the situation with Cambridge Analytica. While we made this change several years ago, if we had only done it a year sooner we could have prevented that situation completely.<sup>243</sup>

520. Moreover, as the DCMS Committee found, had Facebook simply complied with its settlement with the FTC, the Cambridge Analytica Scandal likewise would not have happened.<sup>244</sup>

521. Facebook’s failure to monitor and enforce its own Platform and Privacy Policies allowed third parties, like Cambridge Analytica, to abuse users’ content and information.

**7. Facebook Failed to Adequately Mitigate Harm Caused by Kogan and Cambridge Analytica or to Prevent Further Risk of Harm.**

522. A December 2015 *Guardian* article described Kogan’s and Cambridge Analytica’s conduct in connection with the Ted Cruz campaign. Though Facebook conducted an internal

---

<sup>242</sup> Def. Facebook, Inc.’s Resps. & Objs. to Pls.’ First Set of Interrogs. at p. 20 (Sept. 7, 2018) (“Facebook is not able to review the content of apps’ terms of service or privacy policies as part of its Platform enforcement efforts or during the App Review process.”).

<sup>243</sup> Mark Zuckerberg, Facebook (Dec. 5, 2018), <https://newsroom.fb.com/news/2018/12/response-to-six4three-documents/>.

<sup>244</sup> DCMS Report, *supra* note 28, ¶ 76.



investigation in reaction to the article, it did not warn users at the time that their content and information had been accessed by unauthorized entities. Instead, in March 2016, Facebook began negotiating with Kogan to settle related claims. Facebook ignored its duty to protect its users at this time when it failed to take adequate steps to determine the scope and impact of the content and information that Cambridge Analytica had obtained and to ensure its deletion.

523. Elizabeth Denham, head of the U.K. Information Commissioner's Office, which is investigating the Cambridge Analytica Scandal, has stated that Facebook did not take the appropriate steps to ensure that Cambridge Analytica had deleted Facebook users' data. Denham described Facebook's follow up with Cambridge Analytica as "less than robust."<sup>245</sup>

**Q3957 Chair:** Do you see any evidence of how Facebook sought to ensure that the Facebook data had been deleted? To my mind, the fact that you are still investigating where the Facebook data is would suggest that it has not been deleted, that it is still out there in some form.

What have you seen from your investigations or what has Facebook told you about the process it has followed to ensure the data had been destroyed?

**Elizabeth Denham:** They required confirmation in writing by the heads of organisations that they knew had the data or that they thought had the data that they had deleted it, but we have found some problems with the signing of those authorisations. Some of them were not signed at all. Again, we have evidence and it says in our report that Cambridge Analytica may have partially deleted some of the data, but even as recently as spring 2018 some of the data was still there at Cambridge Analytica. The follow-up was less than robust and that is one of the reasons why we fined Facebook the £500,000.

524. Denham further confirmed that Facebook's only follow up with Cambridge Analytica

**Q3960 Chair:** Until Facebook sent those contractors in, would it be fair to say that the only enforcement action they took against Cambridge Analytica was really to ask them whether they had deleted the data and to promise that they had?

**Elizabeth Denham:** That is correct.

**Q3961 Chair:** Nothing more than that?

**Elizabeth Denham:** No.

<sup>245</sup> U.K. House of Commons, Digital, Culture, Media and Sport Committee, Testimony of Elizabeth Denham, (Nov. 8, 2018), at Q3957,

<http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake-news/oral/92327.pdf>.



was to ask whether it had deleted the data and to accept Cambridge Analytica's representation that it had without further due diligence:<sup>246</sup>

As it turned out, this failure proved detrimental to users, as Cambridge Analytica had not deleted all of the user data in its possession, nor had it destroyed work that had relied on the data.

525. So even after Facebook discovered that its Platform Policy had been abused and that an unauthorized third party had and was making use of users' content and information, Facebook failed to take steps to ensure that users' content and information was deleted.

526. Instead, Facebook's priority was to enter into an agreement with GSR and Kogan binding Kogan to a confidentiality clause in exchange for the release and waiver of all claims related to the misappropriated data.<sup>247</sup>

527. Facebook then waited over two years to make any type of public disclosure.

528. Facebook's failure to take timely and appropriate remedial measures harmed users by leaving them exposed to manipulative psychographic messaging and their users' sensitive personal information irretrievably beyond the users' control promised by Facebook. Facebook's failures show that Facebook did not take seriously its promises to protect users' content and information.

#### **8. Facebook's Failure to Notify Plaintiffs of the Misuse of Their Data Hindered User's Ability to Take Remedial Measures.**

529. At least by the end of 2015, Facebook had actual knowledge that Plaintiffs' content and information had been accessed, downloaded by third parties, and misused without users' authorization. Further, Facebook was aware that such misuse of Plaintiffs' data presented substantial risk of further misuse, fraud, and identity theft to Plaintiffs. Despite this knowledge, and in contravention of its repeated assurances to users that privacy and trust were important parts of Facebook's service, Facebook failed to provide notification to Plaintiffs of the misuse of their content and information without and/or in excess of users' authorization, until March 2018—more than two years after it was

---

<sup>246</sup> *Id.* at Q3960-61.

<sup>247</sup> FB-CA-MDL-00000306; *see also* U.K. House of Commons, Digital, Culture, Media and Sport Committee, Testimony of Mike Schroepfer (Apr. 24, 2018), at Q2164, <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake-news/oral/82114.pdf>.

informed of the Cambridge Analytica Scandal.

530. In the intervening years between 2015 and 2018, Facebook failed to inform Plaintiffs that their sensitive content and information had been used without and/or in excess of their authorization and, as a result of this failure, denied users the opportunity to take steps to protect themselves and mitigate their heightened risk of identity theft and other harms.

531. Plaintiffs were therefore blindsided when they learned that Facebook had permitted unauthorized third parties to access and retain user content and information without and/or in excess of users' authorization, and that their content and information was allegedly used by Cambridge Analytica to create targeted psychographic messaging and advertising on behalf of now-President Donald J. Trump's 2016 Presidential campaign.

**E. Plaintiffs Did Not Consent to Facebook's Misconduct.**

532. Facebook points to certain documents on its website to try to show that users consented to its misconduct. Yet those documents necessarily could not have created consent to conduct that affirmatively *violated* those documents, as much of Facebook's conduct did. Moreover, when the documents simply failed to disclose certain practices, those documents could not have created consent. And when Facebook began to disclose certain kinds of practices well into the Class Period, it failed to inform existing users that it had updated its disclosures—thereby keeping them ignorant. Finally, Facebook relies on certain disclosures that appeared in a document that was neither contractually binding (thus failing to create express consent) nor sufficiently prominent and accessible (thus failing to create implied consent).

533. Nor did anything else in Facebook's website tip users off to the misconduct. Facebook is thus left with documents that for a number of independent reasons were simply inadequate to create express or implied consent to its misconduct.

**1. Facebook's SRR and Data Policy Did Not Create Consent.**

534. For most of the Class Period, Facebook's terms of service were referred to as the

Statement of Rights and Responsibilities (SRR).<sup>248</sup> A second document was referred to as the Privacy Policy initially and then the Data Policy.<sup>249</sup> The names of these documents, and their material terms, were changed at Facebook’s discretion and without meaningful notice to users.

535. Facebook relies on these documents to argue that users consented to its misconduct. But these documents do not establish—and certainly do not establish as a matter of law—that Plaintiffs expressly or impliedly consented. In fact, numerous regulators who have reviewed Facebook’s policies and conducted extensive investigations of its conduct have found that Facebook did not obtain users’ consent for the conduct described in this Complaint. The ICO, for example, recently stated: “We fined Facebook [the maximum amount] because it allowed applications and application developers to harvest the personal information of its customers who had not given their informed consent—think of Friends, and Friends of Friends— and then Facebook failed to keep the information safe.” That conclusion was correct.

**a. Facebook’s SRR and Data Policy Did Not Create Consent with Respect to the VPPA.**

536. Facebook relies upon statements in the SRR and Data Policy to argue that users consented to some of Facebook’s conduct.

537. Even before the January 10, 2013 amendment of the VPPA, the VPPA required a consumer’s affirmative, contemporaneous consent to disclosure of personally identifiable information by a video tape service provider. *See* Video Privacy Protection Act of 1988, Pub. L. 100-618, § 2, 102 Stat. 3195, 3195 (requiring “informed, written consent of the consumer given at the time the disclosure is sought”). No Facebook document was sufficient to provide such consent.

538. The current version of the VPPA, effective January 10, 2013, is even more stringent. It requires the “informed, written consent” to be “in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer.” 18 U.S.C. § 2710(b)(2)(B). No Facebook

---

<sup>248</sup> Before 2009, the SRR was called the “Terms of Service.” For clarity and consistency, this Complaint uses SRR to refer to the Terms of Service and the Statement of Rights and Responsibilities.

<sup>249</sup> Before September 7, 2011, the Data Policy was called the “Privacy Policy.” Between September 7, 2011 and January 30, 2015, it was called the “Data Use Policy.” For the sake of clarity and consistency, this Complaint uses “Data Policy” to refer to the Privacy Policy and the Data Use Policy.

document complied with this requirement.

**b. Facebook’s SRR and Data Policy Did Not Create Consent to Conduct that Violated the SRR and Data Policy.**

539. The documents could not have obtained consent for practices that affirmatively *violated* the terms of the documents.

**(i) By Allowing Users No Control over Sharing with Business Partners, Facebook Violated Its Pledge That Users Would Have Control over How Their Content and Information Was Shared.**

540. At all relevant times, the SRR told users, “You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy [hyperlinked] and application [hyperlinked] settings.”

541. The Data Policy did not contradict this statement in the SRR. Rather, it discussed in more detail how users could use the Privacy Settings and App Settings to control whether and how other users or other entities could access one’s own content and information.

542. Despite Facebook’s pledge that users would have control over how their content and information was shared, users had *no* control over whether and how their content and information was shared with Business Partners. This lack of control directly contradicted Facebook’s disclosures.

**(ii) Facebook Violated Its Pledge That Apps and Websites Would Use Users’ Content and Information Merely “in Connection with” Their Friends.**

543. Even in its most expansive versions, the Data Policy said that if a user’s Friend allowed a third-party application or website to access the user’s content and information, the application or website could use that content and information *only* “in connection with” the Friend that granted permission. Even giving this language its broadest possible reading, Facebook allowed the conduct to occur that was directly contrary to it.

544. From April 22, 2010 to January 30, 2015, the Data Policy said that if a user’s “friend grants specific permission to [an] application or website,” the application or website “will only be allowed to use that content and information *in connection with that friend*” (April 22, 2010 to September 23, 2011) or could use the information “*only in connection with the person that gave the permission and*

*no one else*” (September 23, 2011 to January 30, 2015).

545. The truth, however, was that Apps and websites used Facebook users’ information far more broadly than merely “in connection with” their Friends. Rather, as the Cambridge Analytica Scandal shows, Apps and websites were able to use Facebook users’ data in ways that were not even connected with the App through which the data was gathered, let alone the Friend that had granted permission to the App. When GSR passed along Facebook users’ content and information to Cambridge Analytica, it was not using that content and information merely “in connection with” the Friend that had used the MyDigitalLife App and through whom GSR had gathered data. And when Cambridge Analytica targeted individual Facebook users with specially crafted messages about political candidates, that targeting was specific to the individual user, and was not done “in connection with” the Friend that had granted permission to the MyDigitalLife App.

**(iii) By Continuing to Allow Whitelisted Apps and Business Partners’ Apps to Have Access Even to Users That Had Turned off All App Access, Facebook Violated Its Pledge That Users Could Bar Apps from Accessing Their Data.**

546. Facebook told users that by using their App settings, they could prevent an App from accessing their data via a Friend that used the App. This was true at all relevant times. In one version of the Data Policy, for example, Facebook said that users could “use [their] application settings to limit which of your information your Friends can make available to applications and websites.”<sup>250</sup> In a later version of the Data Policy, it stated that if users turned off “all Platform applications”—that is, by disabling their own ability to use Facebook-integrated games, applications, or websites—users could “completely block applications from getting [their] information when [their] friends and others use” the applications.<sup>251</sup>

547. Contrary to this pledge, Facebook allowed Apps that had been “whitelisted”—i.e., those

---

<sup>250</sup> *Facebook’s Privacy Policy*, Facebook (Feb. 12, 2010), [www.facebook.com/policy](http://www.facebook.com/policy) [<http://web.archive.org/web/20100212024707/facebook.com/policy.php>].

<sup>251</sup> *Other websites and applications*, Facebook (Apr. 16, 2014), [www.facebook.com/about/privacy/your-info-on-other](http://www.facebook.com/about/privacy/your-info-on-other) [<http://web.archive.org/web/20140416060858/.facebook.com/about/privacy/your-info-on-other>].

that had paid Facebook money directly for privileged access to content and information—to continue to access Friends’ data even after users attempted to disable this feature.<sup>252</sup>

548. Recent reports count 5,200 such Whitelisted Apps.<sup>253</sup> These documents also did not inform users that some Apps could obtain their content and information even in violation of the restrictions that users had set to prevent Apps obtaining content.<sup>254</sup>

549. Further, Apps of certain Business Partners (for more on which, see below) had access to user content and information as well, but users’ App settings simply did not control these Apps’ ability access user content and information. Indeed, even if users declined any App access, these Business Partners’ Apps still could access users’ content and information through their Friends that used the Business Partners’ Apps.

**(iv) Facebook Violated Its Pledge Not to Give Content and Information to Advertisers by Permitting Access by Apps, Websites, and Business Partners That Were Also Advertisers.**

550. During the Class Period, the SRR promised users, “We do not give your content or information to advertisers without your consent.”<sup>255</sup>

551. The Data Policy confirmed these terms throughout the Class Period, telling users that their information would be provided to advertisers only after users’ content was removed from it. For example:

When we deliver ads, we do not share your information (information that personally identifies you, such as your name or contact information) with advertisers unless you give us permission. We may provide advertisers with information when we have removed your name and other personally identifying information from it or combined it with other information so that it no longer personally identifies you.<sup>256</sup>

552. Despite this promise, Facebook allowed third-party Apps and websites to access users’ content, even if the Apps or websites were also advertisers. Nothing in the Data Policy—not even the

---

<sup>252</sup> DCMS Report, *supra* note 28, ¶ 81-83.

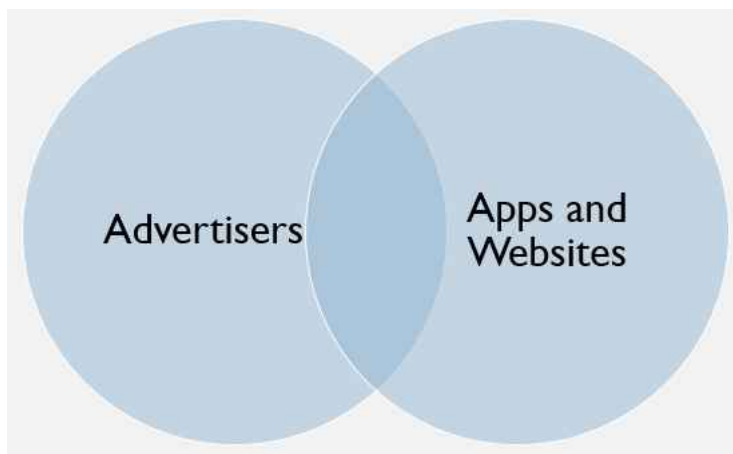
<sup>253</sup> DCMS Report, *supra* note 28, ¶ 84.

<sup>254</sup> *Id.* ¶ 83.

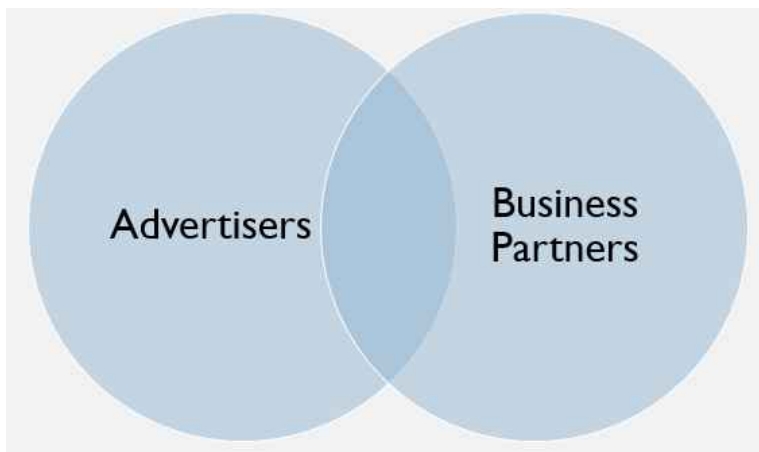
<sup>255</sup> Before August 28, 2009, this portion of the SRR read, “We do not give your content to advertisers.”

<sup>256</sup> *Data Use Policy*, Facebook (July 10, 2014), [https://www.facebook.com/full\\_data\\_use\\_policy](https://www.facebook.com/full_data_use_policy) [[http://web.archive.org/web/20140710224014/https://www.facebook.com/full\\_data\\_use\\_policy](http://web.archive.org/web/20140710224014/https://www.facebook.com/full_data_use_policy)].

portion of the Data Policy discussing how an App could access users' information via a Friend who used the App or website—disclosed that Apps or websites that advertised on Facebook could access users' nonpublic content and information. The problem, to put it in graphic terms, was this:



553. Facebook also allowed Business Partners to access users' content even if the Business Partners were also advertisers, like Amazon and Netflix. Nothing in the Data Policy, not even the portion of the Data Policy discussing “vendors” or “service providers,” disclosed that Business Partners that advertised on Facebook could access users' nonpublic content and information. The problem, once again, was this:



(v) **By Stripping Metadata from Content and Information, Facebook Violated Its Pledge That Apps Would Respect Users' Privacy.**

554. When photos and videos from users passed through Facebook's Graph API v1.0, the interface stripped privacy metadata from the photos and videos.

555. To understand what it means to strip metadata, one must first understand what metadata is: it is data about data. The data in a Microsoft Word file, for example, include the characters in the file, their order, font, size, layout on the page, and so on. Metadata, by contrast, provides context to the data itself—for example, when the file was created, the user who created it, or the title of the file.

556. The data in Facebook had privacy-related metadata, indicating the privacy restrictions that the user who created the data put on it.

557. But when Facebook made photos and videos available to Apps and websites via the Graph API v1.0, the metadata reflecting the user's privacy designations associated with the photos and videos was "stripped" out—even though other metadata remained.

558. This means that when a Facebook user used an App, it was impossible for that App to know, and to abide by, the privacy restrictions that the user had placed on his or her photos and videos.

559. This created situations that were directly contrary to what Facebook told users at all relevant times. It told users, "We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information."<sup>257</sup> Many (if not most) applications did not affirmatively tell users that their privacy settings would simply be ignored. Thus, when users used these applications and their privacy settings for their photos and videos were *not* obeyed because those settings had been stripped from the data, Facebook violated its pledge to these users.

c. **Users Did Not Consent to Misconduct That the Documents Wholly Failed to Disclose.**

560. The documents wholly failed to disclose large parts of Facebook's misconduct. Plaintiffs therefore neither contractually agreed to the misconduct (no express consent) nor had actual notice of

---

<sup>257</sup> *Statement of Rights and Responsibilities*, Facebook (June 18, 2010), <http://www.facebook.com/terms> [<https://web.archive.org/web/20100618224059/http://www.facebook.com/terms.php>].



the misconduct (no implied consent).

**(i) Facebook Failed to Disclose Its Data Sharing with Business Partners**

561. The documents failed to clearly and prominently communicate to users that Facebook shared users' non-public content and information with Facebook's Business Partners at Facebook's sole discretion and without any notice.

562. Facebook gave users' content and information to roughly 150 Business Partners, including Acer, Alibaba, Amazon, Apple, AT&T, Dell, Garmin, Huawei, Microsoft, Qualcomm, Samsung, Sony, and Warner Brothers.<sup>258</sup> Facebook never disclosed this practice. It came to light only after the Cambridge Analytica scandal as a result of investigative journalism and the subsequent congressional inquiry.

563. To defend its sharing of data with Business Partners, Facebook has pointed to certain language in its Data Policy. The most expansive pre-2015 version of this language stated that Facebook might give users' information to "the people and companies that help us provide, understand and improve the services we offer," including "outside vendors" who "help host our website, serve photos and videos, process payments, analyze data, conduct and publish research, measure the effectiveness of ads, or provide search results." Beginning on January 30, 2015, Facebook changed this language slightly to say that it might send users' content and information to "[v]endors, service providers, and other partners who globally support our business."

564. This vague language did not disclose that Facebook gave users' content and information to an extraordinarily wide range of entities, such as media and entertainment companies (e.g., Netflix, Sony, Warner Brothers); software makers (e.g., Microsoft, Opera); companies that make eye-tracking software (Tobii) and speech-recognition software (Nuance); security firms (Gemalto); digital-commerce

---

<sup>258</sup> The list that Facebook provided Congress named the following companies: Accedo, Acer, Airtel, Alcatel/TCL, Alibaba, Amazon, Apple, AT&T, Blackberry, Dell, DNP, Docomo, Garmin, Gemalto, HP/Palm, HTC, Huawei, INQ, Kodak, LG, MediaTek/Mstar, Microsoft, Miyowa/Hape Esia, Motorola/Lenovo, Mozilla, Myriad, Nexian, Nokia, Nuance, O2, Opentech ENG, Opera Software, OPPO, Orange, Pantech, PocketNet, Qualcomm, Samsung, Sony, Sprint, T-Mobile, TIM, Tobii, U2topia, Verisign, Verizon, Virgin Mobile, Vodafone, Warner Brothers, Western Digital, Yahoo, and Zing Mobile.

companies (Alibaba, Amazon); the chip designer Qualcomm; and even the Russian company Yandex and the Chinese company Huawei. Both Yandex and Huawei are suspected of anti-American espionage.

565. Furthermore, Facebook has provided no information whatsoever regarding how these Business Partners can use users' content and information.

**(ii) Facebook Failed to Disclose Psychographic Profiling.**

566. No language in the SRR or in the Data Policy even hinted that once Facebook had allowed third parties to access users' content and information, that content and information could be aggregated with other information to build psychographic profiles on Facebook users.

567. As explained in more detail elsewhere in this complaint, these psychographic profiles can then be used for intrusive psychographic marketing.

**(iii) Facebook Failed to Disclose That When Apps and Websites Accessed Data from the Friends of Users, Those Friends' Privacy Metadata Was Stripped.**

568. No language in the SRR or in the Data Policy discloses that when Apps or websites accessed Facebook users' content and information via a Friend that used the Apps or websites, privacy metadata was stripped from that content and information.

569. Thus, when an App or website accessed a Facebook user's photos or videos through a Friend that used the App or website, the metadata stripping meant that the App or website could no longer know the privacy restrictions that the user had placed on the data. Sensitive data meant to be shared with just a few Friends could thus be made entirely public.

**d. Users Who Were Not Notified of New Disclosures After Initiating Their Accounts Did Not Provide Consent to the Newly Disclosed Conduct.**

**(i) Facebook did not notify users of updates to the Data Policy or SRR.**

570. When the Data Policy or SRR was changed in the three material ways discussed below so as to make new disclosures, users did not receive notice that the Policy or SRR had been changed, beyond a revised Policy or SRR being posted to Facebook.

571. Because users did not receive notice of these changes, they did not expressly agree to them. To the extent Facebook claims a contractual power to unilaterally change the SRR or Data Policy

without notice (beyond posting a revised SRR or Data Policy to the Facebook website), that power is unenforceable under California law.

572. Since the Plaintiffs who signed up before the changes did not receive notice of the changes, they had no reason to consult, and did not consult, the changed SRR or Data Policy. They therefore did not impliedly agree to the changes.

**(ii) Users who signed up before December 9, 2009 did not consent to allowing third-party Apps and websites to access their content and information via their Friends.**

573. Before December 9, 2009, the Data Policy at most stated that if a user's Friends used third-party applications, those applications "may access and share certain information about you with others in accordance with your privacy settings. You may opt-out of any sharing of certain or all information through Platform Applications on the Privacy Settings [hyperlink] page."<sup>259</sup>

574. The vague statement that the applications could access "certain information about you" failed to disclose the extraordinarily broad range of information that applications and websites were able to access using Graph API v1.0, including content that was shared non-publicly like videos, photos and their metadata which included geolocation information, activities, birthdays, education history, hometown, interests, likes, habits, medical information, relationships and relationship details.

575. In addition, once App Settings became the sole tool that Facebook users had to control whether and how applications and websites could access their content and information via their Friends, it became false that users could "opt-out of any sharing" with Apps and websites using their "Privacy Settings." And this was always false with regard to Business Partner Apps.

576. The SRR also omitted these facts to users who signed up before December 9, 2009. That is because, before June 8, 2012, the SRR did not contain *any* language about how applications and websites could access a user's content and information via that user's Friends. When the SRR was changed on June 8, 2012 to include such language, users were not notified of the change beyond the mere fact that a revised SRR was posted to the Facebook website. The significance of this change—that

---

<sup>259</sup> *Facebook Principles*, Facebook (Jan. 16, 2009), [www.facebook.com/policy](http://www.facebook.com/policy) [<http://web.archive.org/web/20090116032231/facebook.com/policy.php>].

Friends could hand over nonpublic content to any entity they connected with—merited direct, clear disclosure and express consent from users. Facebook did the opposite, seeking to hide this change through complex and confusing partial disclosures.

**(iii) Users who signed up from December 9, 2009 to April 22, 2010 did not consent to the broad access that applications and websites had to users’ content and information via their Friends.**

577. From December 9, 2009 to April 22, 2010, the Data Policy had only the following two things to say about access that third-party Apps and websites had to users’ content and information via their Friends. First, it said that users could “limit how your friends share your information with applications through your privacy settings [hyperlink].”<sup>260</sup> Second, further along in the Policy, it said, “You can use your application settings [hyperlink] to limit which of your information your friends can make available to applications and websites.”<sup>261</sup> (There was no disclosure that users could turn off Friends sharing entirely, for the reason that Facebook did not want users to turn off this back door way to funnel user content and information to its Business Partners.)

578. This language utterly failed to disclose what kind of information Apps could access via a user’s Friends. At most, it disclosed the bare fact that Apps *could* access a user’s information via that user’s Friends. Even then, it did so only by implication—that is, only by noting that users could limit the information their Friends could share with applications. And of course it was untrue that users could turn off App sharing with Business Partners.

579. Note, moreover, that the Data Policy is internally inconsistent. It first says that a user can control App sharing using Privacy Settings; it then says that a user can control App sharing using Application Settings. This internal inconsistency negates consent, because it fails to meaningfully disclose how App sharing could be controlled.

580. The SRR also failed to disclose these facts to users who signed up from December 9, 2009 to April 22, 2010. That is because, before June 8, 2012, the SRR did not contain any language at all about how applications and websites could access a user’s content and information via that user’s

---

<sup>260</sup> *Facebook’s Privacy Policy*, Facebook (Feb. 12, 2010), [www.facebook.com/policy](http://www.facebook.com/policy) [<http://web.archive.org/web/20100212024707/facebook.com/policy.php>].

<sup>261</sup> *Id.*

Friends. When the SRR was changed on June 8, 2012 to include such language, users were not notified of the change (beyond the mere fact that a revised SRR was posted to the Facebook website).

**(iv) Users who signed up before September 7, 2011 did not consent to any sharing with Business Partners.**

581. As discussed above, Facebook wholly failed to disclose that Business Partners could access users' content and information during the entire Class Period.

582. The SRR never contained *any* language on which Facebook has relied to argue that it disclosed data sharing with Business Partners. Rather, Facebook has relied only on the Data Policy.

583. But even if one were to agree *arguendo* that the Data Policy disclosed data sharing with Business Partners at *some* point and in *some* form during the Class Period, it wholly failed to disclose any data sharing with Business Partners before September 7, 2011.

584. That is because the Data Policy before September 7, 2011, even at its most expansive, stated that the "service providers" that Facebook allowed access to user information could "have access to your personal information for use *for a limited time*."<sup>262</sup>

585. If this "limited time" language was ever true, it became totally false once Facebook allowed Business Partners to have long-term access to users' content and information.

**e. Because the Data Policy Was Not Part of a Contract and Was Not Reasonably Prominent or Accessible, Users Did Not Consent to Two Matters That the Data Policy, but Not the SRR, Disclosed.**

586. There are two important matters that the SRR never disclosed at any time during the Class Period.

587. ***First***, the SRR never disclosed that users had to use App Settings, not Privacy Settings, to control whether and how third-party Apps and websites could access their content and information via their Friends. Even when the SRR could be read to disclose the bare fact that third-party Apps and websites could access users' content and information via their Friends, it left users with the impression that users could control that access using their Privacy Settings. Thus, for example, the SRR stated that an application could ask for a user's permission to access "content and information that others have

---

<sup>262</sup> *Id.* (emphasis added).

shared with you.”<sup>263</sup> But the SRR failed to specify how that access could be controlled. It simply told users: “To learn more about Platform, including how you can control what information other people may share with applications, read our Data Use Policy and Platform Page.”<sup>264</sup>

588. **Second**, before June 8, 2012, the SRR wholly failed to disclose that third-party applications could access a user’s content and information via a Friend. Instead, at its most expansive, the pre-June 8, 2012 version of the SRR simply said, “When you use an application, your content and information is shared with the application. We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information. (To learn more about Platform, read our Privacy Policy [hyperlink] and About Platform [hyperlink] page.)”<sup>265</sup> This language discloses that an application will access the content and information of a Facebook user who uses the application. It does not disclose that an application may access the content and information of the *Friend* of a Facebook user who uses the application.

589. Facebook argues that these two matters *were* disclosed; however, in so doing, it has relied on language in the Data Policy, not the SRR. Facebook’s reliance on the language in the Data Policy is unavailing, as the Data Policy was never part of a binding contract between users and Facebook, and hence could not manufacture express consent. Nor was the Data Policy sufficiently noticeable or accessible that users were on actual notice of it; for that reason, the Data Policy could not manufacture implied consent either.

(i) **Users Did Not Expressly Consent to Sharing with Third-Party Apps and Websites Because the Data Policy Was Not Incorporated into a Binding Contract.**

590. The Data Policy was never properly incorporated into a binding contract between the users and Facebook. Users did not agree to the Data Policy when they signed up, and they did not agree

---

<sup>263</sup> *Statement of Rights and Responsibilities*, Facebook (Dec. 5, 2012), <https://www.facebook.com/legal/terms> [<https://web.archive.org/web/20121205191915/https://www.facebook.com/legal/terms>].

<sup>264</sup> *Id.*

<sup>265</sup> *E.g.*, *Statement of Rights and Responsibilities*, Facebook (June 18, 2010), <http://www.facebook.com/terms> [<https://web.archive.org/web/20100618224059/http://www.facebook.com/terms.php>].

to the Data Policy merely because they agreed to the SRR.

(1) Users did not agree to the Data Policy at sign-up.

591. Because the sign-up process changed throughout the Class Period, the reason that Plaintiffs did not agree to the Data Policy at sign up changed slightly depending on when Plaintiffs first signed up.

592. ***March 2009 to February 2012.*** In March 2009, Facebook began to omit any reference to the Statement of Rights and Responsibilities or the Privacy Policy on its initial sign-up page.<sup>266</sup> This initial screen required the user to fill in fields for their name, email, password, sex, and birthday:

---

<sup>266</sup> See Chris Glavan, *Facebook –Create new account*, YouTube (Mar. 5, 2011) <https://www.youtube.com/watch?v=PL8MdQcU9cE>; see also Facebook (Mar. 24, 2009), <http://www.facebook.com> [<https://web.archive.org/web/20090324054710/http://www.facebook.com/>];





[Forgot your password?](#)

Facebook helps you connect and share with the people in your life.



**Sign Up**  
It's free and always will be.

**Security Check**  
Enter both words below, separated by a space.  
Can't read the words below? Try different words or see another example.



Text in the box:  What's this?

[Back](#)

By clicking Sign Up, you are indicating that you have read and agree to the Terms of Use and Privacy Policy.

English (US) Español Português (Brasil) Français (France) Deutsch Italiano العربية (مغرب) বাংলা (বাংলাদেশ) 中文 (台灣) +

Facebook © 2011 - English (US) Mobile Find Friends Settings Privacy Pages About Advertising Developers Careers Privacy Terms Help



594. This screen required users to engage in a “Security Check.” This check required users to type out the displayed words in a text box (a “CAPTCHA” test). The text on the security screen was distorted such that users would be distracted by and forced to concentrate on the security image.

595. Deceptively, on this same screen and in very small font (likely eight-point in contrast to



much larger font above), Facebook placed the following statement below the second sign on screen: “By clicking Sign Up, you are indicating that you have read and agree to the Terms of Use [hyperlink] and Privacy Policy [hyperlink].”<sup>267</sup> Because users had already submitted their own personal information and affirmatively agreed to sign up, they could have easily mistaken or not seen this statement.

596. From March 2009 to February 2012, then, users did not agree to the Data Policy as it was not reasonably prominent because (1) the relevant text was small and (2) Facebook affirmatively directed their attention *away* from that text by placing large, distorted text elsewhere on the page and requiring users to concentrate solely on that text.

597. **February 2012 to April 2018.** After February 2012, Facebook changed its sign-up

<sup>267</sup> Chris Glavan, *Facebook – Create new account*, YouTube (Mar. 5, 2011) <https://www.youtube.com/watch?v=PL8MdQcU9cE>.

process to state: “By clicking Sign Up, you agree to our Terms [hyperlinked] and that you have read our Data Use Policy [hyperlinked], including our Cookie Use [hyperlinked].”<sup>268</sup> Notably—and in contrast to Facebook’s past language—this statement does not require agreement to the Data Policy. Rather, it states merely that the user has read the Policy.

(2) Users did not agree to the Data Policy by agreeing to the SRR.

598. The SRR contained a “Privacy” section. This section was a mere three sentences that “encourage[d],” but in no way required, a user to read or consent to the Data Policy.

599. This “Privacy” section of the SRR read as follows:

Your privacy is very important to us. We designed our Privacy Policy [or Data Use Policy] [hyperlinked] to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Privacy Policy [or Data Use Policy], and to use it to help make informed decisions.<sup>269</sup>

600. The SRR did not contain the full text of the Data Policy, did not require users to review the Data Policy, and did not require any form of affirmative acknowledgement of or consent to the Data Policy.

601. The language that the SRR used to refer to the Data Policy simply did not contain any indication that the Data Policy was intended to be a *legally binding contract* between the user and Facebook.

602. At the bottom of the SRR, the Data Policy was hyperlinked in a long list of documents that Facebook casually suggested users “may also want to review.” Facebook explained in this list that the “Privacy Policy is designed to help you understand how [they] collect and use information”—in other words, Facebook presented the information to users as a help page, *not* an agreement.<sup>270</sup>

---

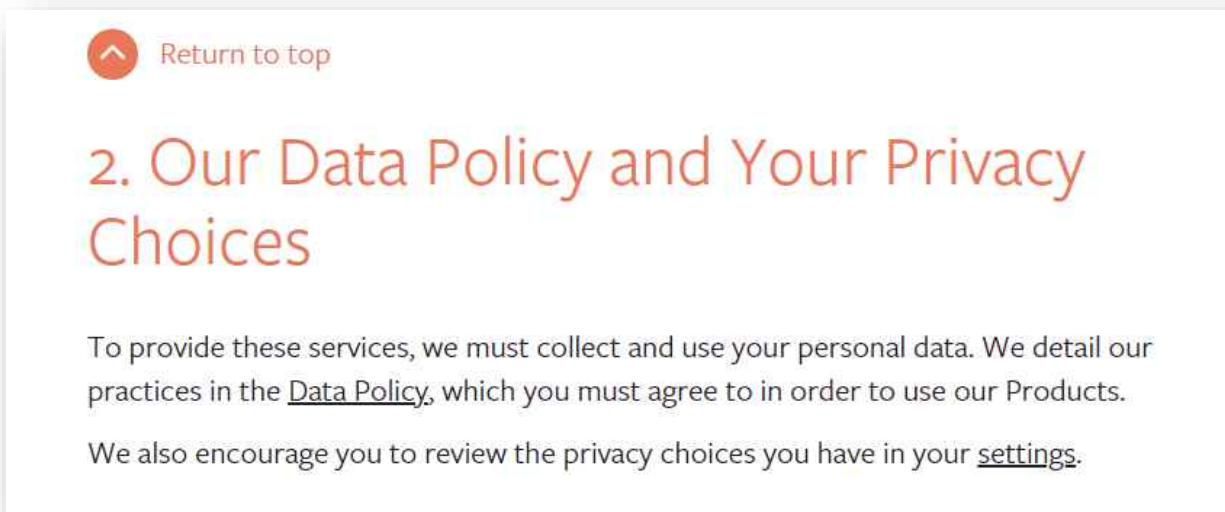
<sup>268</sup> When the “Data Use Policy” was renamed the “Data Policy,” this text began to reference the “Data Policy.”

<sup>269</sup> See, e.g., *Statement of Rights and Responsibilities*, Facebook (Aug. 28, 2009), [www.facebook.com/terms.php](http://www.facebook.com/terms.php) [<http://web.archive.org/web/20090918000730/facebook.com/terms.php>]; *Statement of Rights and Responsibilities*, Facebook (June 8, 2012), <http://www.facebook.com/legal/terms> [<http://web.archive.org/web/20120712173816/https://www.facebook.com/legal/terms>].

<sup>270</sup> *Id.*; *Statement of Rights and Responsibilities*, Facebook (June 18, 2010), <http://www.facebook.com/terms.php?ref=pf> [<https://web.archive.org/web/20100618213653/http://www.facebook.com/terms.php?ref=pf>].

603. Contrast the way that the SRR *used* to refer to the Data Policy with what it now says:

- (ii) **The Data Policy Did Not Create Implied Consent Because It Was Not Reasonably Prominent or Accessible.**



604. On its home page, Facebook did not prominently display the Data Policy or a hyperlink to the Data Policy. Moreover, as discussed below, even if users had somehow noticed the hyperlink to the Data Policy during the sign-up process or otherwise, Facebook at times made it extremely difficult to read the Data Policy.

605. Facebook provided a hyperlink to the Data Policy near the bottom of its home screen. This hyperlink read in small print, "Privacy."

606. Before September 2011, if a user happened to see and then click on this hyperlink, she would be routed to one webpage that contained the entire Policy.

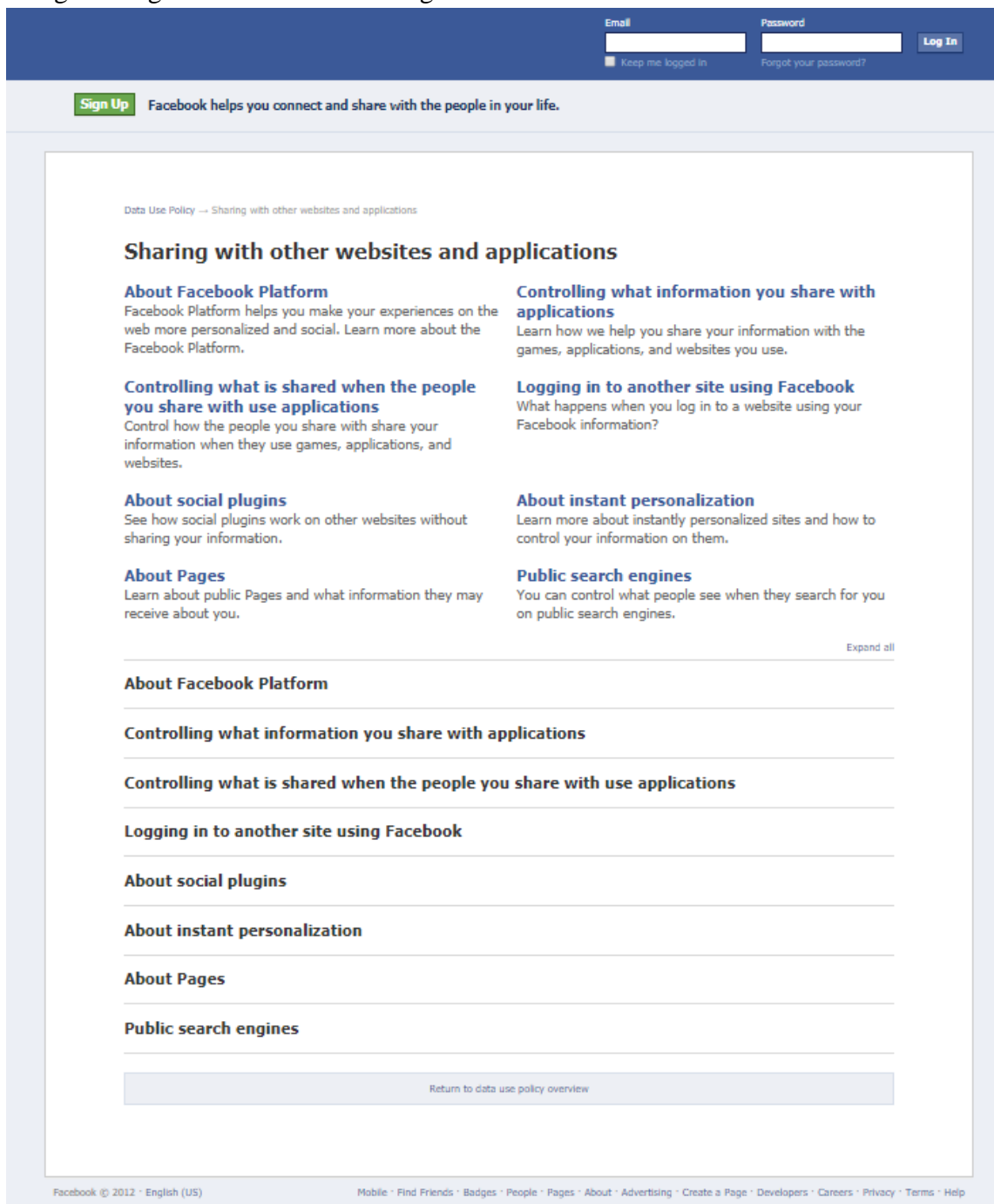
607. Beginning by at least September 2011, if users were to click on “Privacy,” they would be routed to a page that listed subheadings of the “Data Use Policy.” For example:<sup>271</sup>



608. From September 2011 to June 2012, even if users clicked a subheading on this webpage, they *still* would not be able to see the contents of the Data Use Policy. Instead, clicking those subheadings routed users to yet another webpage containing yet more subheadings. Users would then need to read and click on the subheadings or click “*expand all*” to actually read the content of the relevant subsection of the Data Use Policy. For example, if users decided they wanted to read more about “Sharing with other websites and applications,” they would be routed to a screen that required

<sup>271</sup> *Data Use Policy*, Facebook (Sept. 22, 2011), <http://www.facebook.com/about/privacy/your-info-on-other> [<https://web.archive.org/web/20110922195234/http://www.facebook.com/about/privacy/>].

users to go through even *more* subheadings:<sup>272</sup>



<sup>272</sup> *Sharing with other websites and applications*, Facebook (Jan. 12, 2012), <http://www.facebook.com/about/privacy/your-info-on-other> [https://web.archive.org/web/20120112084445/http://www.facebook.com/about/privacy/your-info-on-other].

609. Thus, from September 2011 to June 2012, if a user wanted to read the actual contents of the Data Policy, the user would have had to read several subheading descriptions and to click at least three different hyperlinks before seeing any content. And, if the user wanted to read the *full* Data Policy, the user would need to click back and forth between multiple webpages. It would take a user at least eighteen separate clicks of the mouse to read the entire Data Policy.

610. Even after June 2012, Facebook still required users to click on one of the six separate subheadings of the Data Policy.<sup>273</sup> But even with this change, from June 2012 to January 2015, a user would need to click back and forth at least twelve times in order to read the full contents of the Data Policy contained within six separate subheadings.

611. Starting in January 2015, Facebook again changed the Data Use Policy so that all content was displayed on one webpage.

**2. Nothing Outside the SRR and Data Policy Created Consent Either—to the Contrary, Statements That Facebook Made Lulled Users into Believing Their Privacy Was Protected.**

612. Just as neither the SRR nor the Data Policy created the consent Facebook has claimed, so nothing outside the documents created the necessary consent either.

613. Merely by way of example, no contemporaneous notice was given each time Facebook permitted Apps, websites, or Business Partners to access users' content and information. And when one user allowed an App to access his or her Friends' data, Facebook did not give contemporaneous notice to those Friends, let alone allow those Friends to opt out of the sharing.

614. Even now, Facebook has failed to give its users the full picture of what it did with their data. It still has not informed users which Apps and other third parties have accessed their content and information. They still have not informed users that their content and information was used for psychographic marketing.

---

<sup>273</sup> *Other websites and applications*, Facebook (Dec. 9, 2012), <https://www.facebook.com/about/privacy/your-info-on-other> [<https://web.archive.org/web/20121209131947/https://www.facebook.com/about/privacy/your-info-on-other>].

615. Moreover, the statements that Facebook made and actions it took outside the SRR and Data Policy affirmatively misled users into expecting that when they used the Privacy Controls to limit the audience for their content, those Privacy Controls truly did limit that content to the designated audience.

616. Indeed, the extensive Privacy Controls *themselves*—particularly those Controls that controlled the audience for individual posts—gave reasonable users the misimpression that they could use them to control sharing with others. Indeed, because Facebook, for much of the Class Period, allowed users to designate a limited audience for each individual post, Facebook could easily have permitted that designation also to limit sharing with third-party Apps, websites, and Business Partners. It chose not to do so.

617. Furthermore, for much of the Class Period, users had to actively sign up in order to access Facebook. This fact—the fact that Facebook, for much of the Class Period, was a subscriber-only site—also reinforced users’ reasonable expectation of privacy for content whose audience they limited.

618. Finally, throughout the Class Period, Mark Zuckerberg issued repeated reassurances that Facebook was committed to protecting its users’ privacy and to giving them understandable and accessible tools to limit the sharing of their data. Far from creating consent, these reassurances helped to deceive users about the misconduct complained of here.

**F. Facebook’s Sharing User Content and Information with Third Parties Without Users’ Consent Violates the 2012 Federal Trade Commission Consent Decree**

619. The FTC’s Consent Decree required Facebook to change certain disclosures and practices because, among other things, Facebook was misleading consumers about its treatment of users’ content and information. The subject matter of the Consent Decree bears directly on the practices challenged by this Complaint. Thus, while this action is not brought to enforce the Consent Decree, the FTC’s previous findings and the agreements Facebook reached with them bear on what reasonable consumers expected from Facebook.

620. In December 2009, the nonprofit organization Electronic Privacy Information Center (“EPIC”), a public interest research center based in Washington, D.C., filed a complaint and request for



investigation, injunction, and other relief against Facebook before the Federal Trade Commission (“FTC”).<sup>274</sup>

621. EPIC’s complaint alleged that the “Facebook Platform transfer[red] Facebook users’ personal data to application developers without users’ knowledge or consent.”<sup>275</sup>

622. The FTC investigated EPIC’s claims. Thereafter, the FTC issued its Complaint on November 29, 2011,<sup>276</sup> listing a number of instances in which Facebook made promises that it did not keep:

- In December 2009, Facebook changed its website so certain information that users may have designated as non-public, including their Friends List, was made public. Facebook didn’t warn users about this change or get their approval in advance;
- Facebook represented that third-party Apps that users installed would have access only to user information that they needed to operate. In fact, the Apps could access nearly all of users’ personal data—data the Apps didn’t need to operate;
- Facebook told users they could restrict sharing of data to limited audiences—for example, with Friends. In fact, selecting Friends did not prevent their information from being shared with third-party applications their Friends used;
- Facebook claimed it audited and monitored the security practices of Apps participating in its “Verified Apps program,” but the company did not do so;
- Facebook shared users’ personal details with advertisers even though they promised not to do so; and
- Facebook claimed that it complied with the U.S.-EU Safe Harbor Framework that governs data transfer between the U.S. and the European Union, but failed to do so.<sup>277</sup>

---

<sup>274</sup> EPIC Complaint, Request for Investigation, Injunction, and Other Relief, *In re Facebook, Inc.* (F.T.C. Dec. 17, 2009), <https://www.epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf>.

<sup>275</sup> *Id.* ¶ 54.

<sup>276</sup> FTC Complaint, *supra* note 75.

<sup>277</sup> *Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises*, F.T.C. (Nov. 29, 2011), <https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep>.

623. On November 29, 2011, the FTC announced that Facebook had agreed to settle FTC charges that Facebook had “deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public.”<sup>278</sup> On July 27, 2012, the FTC finalized and issued its Consent Decree, which ordered, in part, that Facebook:

[S]hall 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 [Facebook] and the steps a consumer must take to implement such controls;
- C. the extent to which [Facebook] makes or has made covered information accessible to third parties;
- D. the steps [Facebook] takes or has taken to verify the privacy or security protections that any third party provides . . . .<sup>279</sup>

624. The Consent Decree further ordered, in part, that:

[P]rior to any sharing of a user’s nonpublic user information by [Facebook] with any third party, which materially exceeds the restrictions imposed by a user’s privacy setting(s), [Facebook] 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.<sup>280</sup>

625. Facebook violated the Consent Decree by failure to cure the very conduct that was the subject of the FTC Complaint:

- The FTC Complaint alleged: “Facebook has represented, expressly or by implication,

---

<sup>278</sup> *Id.*

<sup>279</sup> FTC Consent Decree, *supra* note 6, at 3-4.

<sup>280</sup> *Id.* at 4.

that, through their Profile Privacy Settings, users can restrict access to their content and information to specific groups, such as [Friends]. In truth and in fact, in many instances, users could not restrict access to their profile information to specific groups, such as [Friends] through their Profile Privacy Settings. Instead, such information could be accessed by [Apps] that their Friends used,” including Business Partners, Whitelisted Apps, and advertisers.<sup>281</sup> Further, after Facebook discontinued Graph API v1.0, there was no way to disable or to control sharing with Whitelisted Apps, including advertisers.<sup>282</sup>

- The FTC Complaint alleged: “Facebook has represented, expressly or by implication, that Facebook does not provide advertisers with information about its users.”<sup>283</sup> But in truth and in fact, as described in the FTC Complaint, Facebook has provided advertisers with information about its users.<sup>284</sup>

626. Facebook also violated the Consent Decree by failing to perform actions required by the Consent Decree, including:

- Facebook has continued to “misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information,” by putting a user’s application-related privacy settings on a page completely different from all other privacy settings.<sup>285</sup>
- Facebook shared nonpublic user information with third parties, including Apps, Whitelisted Apps, and Business Partners, so as to “materially exceed[] the restrictions imposed by a user’s privacy setting(s)” —but it failed to “clearly and prominently disclose” details regarding this sharing with users.<sup>286</sup>

---

<sup>281</sup> FTC Complaint, *supra* note 75, ¶¶ 17-18.

<sup>282</sup> *Id.* ¶ 18.

<sup>283</sup> *Id.* ¶ 41.

<sup>284</sup> *Id.* ¶ 42.

<sup>285</sup> FTC Consent Decree, *supra* note 6, at 3; *see also* FTC Complaint, *supra* note 75, ¶¶ 17-18.

<sup>286</sup> FTC Consent Decree, *supra* note 6, at 4.

- Facebook failed to make any such disclosure separate and apart from its Privacy Policy, Data Use Policy, or Statement of Rights and Responsibilities.<sup>287</sup>
  - Facebook failed to “obtain the user’s affirmative express consent” before sharing nonpublic user information with third parties including Apps, Whitelisted Apps, Business Partners, and advertisers; instead, Facebook’s default setting was that users’ personal information could be shared with third parties via the users’ Friends.<sup>288</sup>
- Likewise, Facebook obtained no consent from its users for the sharing of their content and information with Whitelisted Apps and Business Partners, including advertisers, because there were no Privacy Controls or App Settings that controlled such sharing.

627. Because of these and other apparent violations of the Consent Decree, the FTC reopened its investigation of Facebook, as confirmed by the FTC in March 2018.<sup>289</sup> As detailed by the *New York Times*, at issue in the FTC’s reopened investigation is whether Facebook violated the Consent Decree through conduct such as the following:

- Facebook shared user data with more than 150 Business Partners without users’ consent and despite users’ privacy settings;
- Microsoft’s Bing was allowed to see the names of virtually all Facebook users’ Friends without users’ consent;
- Netflix, Spotify, and the Royal Bank of Canada were given access to private messages of Facebook users, allowing them to read, write, and delete users’ private messages and to see all participants on a thread;
- Amazon was allowed to obtain users’ names and contact info through their Friends;
- Yahoo was allowed to view streams of Friends’ posts as recently as summer 2018;
- Facebook allowed Apple to access to the contact numbers and calendar entries of people

---

<sup>287</sup> *Id.*

<sup>288</sup> *Id.*

<sup>289</sup> *Statement by the Acting Director of FTC’s Bureau of Consumer Protection Regarding Reported Concerns About Facebook Privacy Practices*, F.T.C. (Mar. 26, 2018), <https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection>.

who had changed their account settings to disable all sharing, and empowered Apple to hide from Facebook users all indicators that its devices were asking for data;

- Russian search giant Yandex, which has been accused of funneling data to the Kremlin, had access to Facebook’s unique user IDs as recently as 2017, even after Facebook had stopped sharing this information with many other applications, citing privacy risks.<sup>290</sup>

628. Roger McNamee, an early investor in Facebook, has also weighed in, stating: “I don’t believe it is legitimate to enter into data-sharing partnerships where there is not prior informed consent from the user.”<sup>291</sup>

629. Subsequently, it has been reported that Facebook and the FTC are negotiating a “record-setting” fine of approximately \$2 billion against Facebook for violating the Consent Decree.<sup>292</sup>

630. Moreover, the DCMS Committee considered whether Facebook violated the Consent Decree through its subsequent conduct, including that revealed by the Cambridge Analytica Scandal and other revelations regarding Business Partners. In its February 14, 2019 report, the DCMS Committee found that, after entering into the 2012 Consent Decree, Facebook continued “to override its users’ privacy settings in order to transfer data to some App developers” and “to charge high prices in advertising to some developers, for the exchange of that data”—and, for this reason, “[i]t seems clear that Facebook was, at the very least, in violation of its [FTC] settlement.”<sup>293</sup>

631. Moreover, Facebook executive Richard Allan, Vice President of Policy Solutions at Facebook, acknowledged to the DCMS Committee that Facebook continued the same conduct at issue in the FTC Complaint and Consent Decree for at least two years after Facebook entered into the Consent Decree. In particular, the DCMS Report states that, “[w]hen Richard Allan was asked at what point Facebook had made such changes to its own systems, to prevent developers from receiving

---

<sup>290</sup> Dance, et al, *As Facebook Raised a Privacy Wall*, *supra* note 158.

<sup>291</sup> *Id.*

<sup>292</sup> Tony Romm & Elizabeth Dwoskin, *U.S. Regulators Have Met to Discuss Imposing a Record-Setting Fine Against Facebook for Privacy Violations*, Wash. Post (Jan. 18, 2019), [https://www.washingtonpost.com/technology/2019/01/18/us-regulators-have-met-discuss-imposing-record-setting-fine-against-facebook-some-its-privacy-violations/?utm\\_term=.177c44fd0618](https://www.washingtonpost.com/technology/2019/01/18/us-regulators-have-met-discuss-imposing-record-setting-fine-against-facebook-some-its-privacy-violations/?utm_term=.177c44fd0618).

<sup>293</sup> DCMS Report, *supra* note 28, ¶ 135.

information (which resulted in circumventing Facebook users' own privacy settings), he replied that the change had happened in 2014," referring "to the change from Version 1 of Facebook's Application Programming Interface (API) to its more restrictive Version 2."<sup>294</sup>

632. In fact, although Facebook announced Graph API v2.0 in 2014, Apps were still allowed to access users' content and information through Graph API v1.0 until 2015. Accordingly, Allan's testimony to the DCMS Committee stands as an admission by Facebook that it violated the Consent Decree for approximately three years—and even longer for Whitelisted Apps and Business Partners, which maintained access to the content and information of App users' Friends for years after Facebook made the transition to Graph API v2.0.

633. Moreover, "[i]n reply to a question as to whether CEO Mark Zuckerberg knew that Facebook continued to allow developers access to that information, after the agreement, Richard Allan replied that Mr. Zuckerberg and '**all of us**' **knew that the platform continued to allow access to information.**"<sup>295</sup> In this regard, the DCMS Report accused Facebook of deceit:

The fact that Facebook continued to allow this access after the Consent Decree is not new information; the new information is the admission by Richard Allan that the CEO and senior management— "all of us"—knew that Facebook was continuing to allow the practice to occur, despite the public statements about its change of policy. That, people might well contest, constituted deceit and we would agree with them.<sup>296</sup>

634. Further, Allan argued "that, while Facebook continued to allow the same data access—highlighted in the first count of the FTC's complaint and of which the CEO, Mark Zuckerberg, was also aware—that was acceptable due to the fact that Facebook had supposedly put 'controls' in place that constituted consent and permission."<sup>297</sup> In this regard, Allan testified that "[w]e were confident that the controls we implemented constituted consent and permission—others would contest that, but we believed we had controls in place that did that and that covered us for that period up to 2014."<sup>298</sup> Thus,

---

<sup>294</sup> *Id.* ¶ 68.

<sup>295</sup> *Id.* ¶ 69 (emphasis added).

<sup>296</sup> *Id.* ¶ 75 (emphasis added).

<sup>297</sup> *Id.* ¶ 71.

<sup>298</sup> *Id.* ¶ 68 (emphasis added).

Facebook acknowledged the need to obtain affirmative express consent from users and “admitted to [the DCMS Committee] that people might indeed take issue with Facebook’s position.”<sup>299</sup>

635. Similarly, Allan’s statement that the only way that Facebook purportedly obtained affirmative express consent from users was through “controls” stands as a tacit admission that Facebook never obtained affirmative express consent from users. In this regard, Allan “did not specify what controls had been put in place by Facebook, but they did not prevent app developers, who were not authorised by a user, from accessing data that the user had specified should not to be shared.”<sup>300</sup> Hence, Facebook’s apparent position is that it was already obtaining the affirmative express consent of users when the FTC issued its initial complaint. This is unsustainable, as Allan admits: “others would contest that.”<sup>301</sup>

636. If it had not been for the Cambridge Analytica Scandal, Facebook’s violation of the Consent Decree may never have come to light. This is so because “the consent decree’s enforcement provision gave Facebook a ‘get out of jail free’ card,” in that “[t]he FTC allowed Facebook to both pick and pay the third-party auditor whose certification of compliance with the consent decree would be required.”<sup>302</sup> For this reason, “Facebook did not have to worry about compliance,” and “received passing grades every time, even as it failed to comply with the spirit of the decree.”<sup>303</sup>

637. As a result, “requests [by former Facebook privacy manager Sandy Parakilas] for engineering resources to enforce the decree were denied with an exhortation to ‘figure it out.’”<sup>304</sup> Consequently, “[i]n the run-up to Facebook’s May 2012 IPO, . . . [a] series of privacy issues emerged that related to Facebook Platform, specifically to the tool that enabled third-party Apps to harvest data from users’ friends.”<sup>305</sup> According to Parakilas, “Facebook’s lack of commitment to user data privacy created issues of disclosure and legal liability that could and should have been addressed before the

---

<sup>299</sup> *Id.* ¶ 75.

<sup>300</sup> *Id.* ¶ 74 (emphasis added).

<sup>301</sup> *Id.* ¶ 68.

<sup>302</sup> McNamee, *Zucked: Waking up to the Facebook Catastrophe* 189 (2019).

<sup>303</sup> *Id.*

<sup>304</sup> *Id.*

<sup>305</sup> *Id.* at 190.



initial public offering.”<sup>306</sup> Consequently, [r]ecognizing that Facebook did not intend to enforce the spirit of the FTC consent decree—and would blame him if ever there was bad press about it—Sandy quit his job.”<sup>307</sup>

**G. Facebook Has Faced Numerous Regulatory and Governmental Agency Investigations for Disregarding the Privacy of Its Users.**

638. On October 24, 2018, the United Kingdom’s Information Commissioner’s Office (“ICO”), an independent body set up to uphold information rights, issued the maximum monetary penalty of £500,000 to Facebook for its transfer of users’ information with consent.<sup>308</sup> In the notice, the ICO set forth the facts underlying its penalty decision, including that Facebook did not obtain informed consent from users and failed to take adequate steps, such as auditing Apps, to prevent the improper use of users’ data.

639. In its monetary penalty notice, the ICO found that, “to the extent that such processing of personal data was purportedly based on consent, any such consent was invalid and ineffective, since it was not freely given, specific, or informed.”<sup>309</sup> Similarly, the ICO found that “[i]t was unfair for the Facebook Companies to rely on a Facebook user’s privacy settings as enabling apps installed by the user’s Facebook friends to collect extensive personal data from the user’s account,” and Facebook “ought instead to have ensured that, before access to such personal data took place, the Facebook user: was informed that the app wished to access such personal data; was told what data was sought, and how it would be used; and was given the opportunity to give or withhold their consent for such access.”<sup>310</sup> Further, Facebook “failed to provide adequate information to Facebook users that this could occur, and as to the steps that they needed to take to prevent this,” and “[i]ndividuals would not reasonably have expected their personal data to be collected in this way merely because of a choice made by other

---

<sup>306</sup> *Id.*

<sup>307</sup> *Id.*

<sup>308</sup> Supervisory Powers of the Information Commissioner, *Monetary Penalty Notice*, Information Commissioner’s Office (Oct. 24, 2018), <https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf>.

<sup>309</sup> *Id.* at 15.

<sup>310</sup> *Id.* at 16.

individuals to use a particular app.”<sup>311</sup> Finally, the ICO found that Facebook “took no steps, or no adequate steps, to guard against such unauthorised or unlawful processing.”<sup>312</sup>

640. Regarding this fine, the Information Commissioner, Elizabeth Denham, stated that “[w]e fined Facebook because it allowed applications and application developers *to harvest the personal information of its customers who had not given their informed consent*,” such as “friends, and friends of friends,” and “then Facebook failed to keep the information safe.”<sup>313</sup> Further, the Commissioner said that the fact that the ICO “found their business practices and the way applications interact with data on the platform to have contravened data protection law” is “a big statement and a big finding.”<sup>314</sup> However, as to rulings imposed by international regulators including the federal privacy commissioner in Canada or the ICO, the Commissioner believes that Facebook does not view these rulings “as anything more than advice.”<sup>315</sup> Based on the evidence given by Facebook executive Richard Allan, the Commissioner “thought ‘that unless there is a legal order compelling a change in their business model and their practice, they are not going to do it.’”<sup>316</sup> The Commissioner also stated, “[c]ompanies are responsible for proactively protecting personal information,” and “Facebook broke data protection law, and it is disingenuous for Facebook to compare that to email forwarding, because that is not what it is about; *it is about the release of users’ profile information without their knowledge and consent*.”<sup>317</sup>

641. On October 25, 2018, members of the European Parliament adopted a resolution calling for EU bodies to carry out full investigation of Facebook following the Cambridge Analytica Scandal.<sup>318</sup> Members of Parliament stated Facebook breached the trust of EU citizens and violated EU laws.

---

<sup>311</sup> *Id.*

<sup>312</sup> *Id.* at 18.

<sup>314</sup> DCMS Report, *supra* note 28, ¶ 58.

<sup>315</sup> *Id.*

<sup>316</sup> *Id.*

<sup>317</sup> *Id.*, ¶ 57 (emphasis added).

<sup>318</sup> *Facebook-Cambridge Analytica: MEPs demand action to protect citizens’ privacy*, European Parliament, (October 25, 2018), <http://www.europarl.europa.eu/news/en/press-room/20181018IPR16525/facebook-cambridge-analytica-meps-demand-action-to-protect-citizens-privacy>.

Members further recommended that Facebook make changes to its platform to comply with EU data protection law.

642. On December 7, 2018, the Italian Competition Authority (“AGCM”) issued two fines totaling \$11.4 million against Facebook.<sup>319</sup> The AGCM found that Facebook misled users into signing up without fully informing them of the ways that their content and information would be used for commercial purposes. The AGCM further criticized Facebook for pre-selecting users’ settings to allow for the sharing of their data to third-party Apps and websites and then discouraging consumers from changing their settings by telling them that doing so risked “significant limitations” on the usability of the Facebook Platform and third-party Apps.<sup>320</sup>

643. Lawmakers from nine countries, led by the United Kingdom, have convened to investigate Facebook’s role in privacy, including lawmakers from Argentina, Belgium, Brazil, Canada, France, Ireland, Latvia and Singapore.<sup>321</sup>

644. On December 19, 2018, Washington D.C.’s attorney general issued a complaint against Facebook for its “lax oversight and misleading privacy settings.” The complaint alleges that<sup>322</sup>:

First, Facebook misrepresented the extent to which it protects its consumers’ personal data, requires third-party developers to respect its consumers’ personal data, and how consumers’ agreements with third-party applications control how those applications use their data. Second, Facebook failed to adequately disclose to Facebook consumers that their data can be accessed without their knowledge or affirmative consent by third-party applications downloaded by their Facebook friends. Third, Facebook failed to disclose to affected consumers when their data was improperly harvested and used by third-party applications and others in violation of Facebook’s policies, such as in the Kogan and

---

<sup>319</sup> IANS, *Italy fines Facebook 10 million euros for misleading users*, Financial Express (Dec. 8, 2018, 10:47am), <https://www.financialexpress.com/world-news/italy-fines-facebook-10-million-euros-for-misleading-users/1407281/>.

<sup>320</sup> *Id.*; Alex Hern, Italian regulator fines Facebook £8.9m for misleading users, The Guardian (Dec. 7, 2018), <https://www.theguardian.com/technology/2018/dec/07/italian-regulator-fines-facebook-89m-for-misleading-users>.

<sup>321</sup> Natasha Lomas, *‘The problem is Facebook,’ lawmakers from nine countries tell Zuckerberg’s accountability stand-in*, TechCrunch (Nov. 27, 2018), <https://techcrunch.com/2018/11/27/the-problem-is-facebook-lawmakers-from-nine-countries-tell-zuckerbergs-accountability-stand-in/>.

<sup>322</sup> Complaint for Violations of the Consumer Protection Procedures Act, *D.C. v. Facebook, Inc.*, No. 2018 CA 008715 B (D.C. Super. Ct., Dec. 19, 2018) <http://oag.dc.gov/sites/default/files/2018-12/Facebook-Complaint.pdf>.

Cambridge Analytica example. Fourth, compounding these misrepresentations and disclosure failures, Facebook’s privacy settings are ambiguous, confusing, and difficult to understand. Finally, Facebook failed to disclose that it granted certain companies, many of whom were mobile device makers, special permissions that enabled those companies to access consumer data and override consumer privacy settings.

645. In addition, by April 2018, thirty-seven state attorneys general had opened investigations into Facebook’s mishandling of user content and information, including related privacy-violation claims. In January 2019, it was reported that the several of these states had joined their investigations together.<sup>323</sup>

646. Even before the Cambridge Analytica Scandal, numerous legal actions questioned Facebook’s commitment to its users’ privacy.

647. In 2012, for example, Facebook faced a class action lawsuit from users for sharing users’ “likes” of advertisers without compensation or allowing them to opt out. Facebook settled this case for \$20 million.

648. On May 14, 2015, a class action lawsuit was filed against Facebook alleging that Facebook’s photo scanning technology violates users’ privacy rights.

649. In June 2015, the Belgium Privacy Commission filed a lawsuit against Facebook, alleging that Facebook broke the privacy law of Belgium and the European Union laws by tracking people on third-party sites without first obtaining their consent. In February 2018, a Belgian court ordered Facebook to stop this practice or face daily fines.<sup>324</sup>

650. In 2016, Germany’s Consumer Federation announced it would fine Facebook €100,000 for failing to comply with a previous court order requiring Facebook to make clear the extent to which users’ intellectual property “could be used by Facebook and licensed to third parties.”

651. On May 16, 2017, the Dutch and French Data Protection Authorities (“DPA”) announced

---

<sup>323</sup> Erik Larson, et. al, *Facebook Privacy Lapses Art the Target of More Probes in the U.S.*, Bloomberg (Jan. 31, 2019), <https://www.bloomberg.com/news/articles/2019-01-31/facebook-privacy-lapses-said-to-be-target-of-more-probes-in-u-s>.

<sup>324</sup> Samuel Gibbs, *Facebook ordered to stop collecting user data by Belgian court*, The Guardian (Feb. 16, 2018), <https://www.theguardian.com/technology/2018/feb/16/facebook-ordered-stop-collecting-user-data-fines-belgian-court>.

that Facebook had not provided users sufficient control over how their information was being used. The French DPA fined Facebook €150,000 for failure to stop tracking non-users' web activity without their consent and transferring personal information to the United States.<sup>325</sup> The French DPA stated: "the cookie banner and the mention of information collected 'on and outside Facebook' do not allow users to clearly understand that their personal data are systematically collected as soon as they navigate on a third-party website that includes a social plug in."<sup>326</sup>

652. On May 18, 2017, the European Union's antitrust commission fined Facebook \$122 million for misleading regulators about combining data from the messaging service App WhatsApp.

653. In September 2017, the Spanish data protection authority (the AEPD) fined Facebook €1.2 million (\$1.44 million) for its collection of data on "people's ideologies and religious beliefs, sex and personal tastes" without users consent and for not deleting information that was not relevant.

654. On February 14, 2019, the U.K. House of Common's DCMS Committee issued its *Disinformation and 'Fake News': Final Report*, which represents "the accumulation of many months of collaboration with other countries, organisations, parliamentarians and individuals from around the world," for which the DCMS Committee "held 23 oral evidence sessions, received over 170 written submissions, heard evidence from 73 witnesses, asking over 4,350 questions at these hearings, and had many exchanges of public and private correspondence with individuals and organisations."<sup>327</sup> The DCMS Committee also convened, for the purposes of preparing its report, "an 'International Grand Committee' in November 2018, inviting parliamentarians from nine countries: Argentina, Belgium, Brazil, Canada, France, Ireland, Latvia, Singapore and the UK."<sup>328</sup>

655. The DCMS Report directly considered and includes findings regarding the conduct that came to light in the Cambridge Analytica Scandal. The DCMS Committee "argues that, had Facebook abided by the terms of an agreement struck with US regulators in 2011 to limit developers' access to

---

<sup>325</sup> *Common Statement by the Contact Group of the Data Protection Authorities of the Netherlands, France, Spain, Hamburg and Belgium*, CNIL (May 16, 2017), <https://www.cnil.fr/fr/node/23602>.

<sup>326</sup> *Id.*

<sup>327</sup> DCMS Report, *supra* note 28, ¶ 6.

<sup>328</sup> *Id.* ¶ 1.

user data, the scandal would not have occurred,” concluding that “[t]he Cambridge Analytica scandal was facilitated by Facebook’s policies.”<sup>329</sup> Further, “Zuckerberg is also personally criticised by the committee in scathing terms, with his claim that Facebook has never sold user data dismissed by the report as ‘simply untrue.’”<sup>330</sup> Moreover, the DCMS Report “highlights the link between friends’ data and the financial value of the developers’ relationship with Facebook,” and states that the Cambridge Analytica Scandal has not meaningfully impacted Facebook’s approach to data security: “Facebook continues to choose profit over data security, taking risks in order to prioritise their aim of making money from user data,” and “[i]t seems clear to us that Facebook acts only when serious breaches become public.”<sup>331</sup>

656. The DCMS Report directly accuses Facebook of “intentionally and knowingly violat[ing] both data privacy and anti-competition laws.”<sup>332</sup> In this regard, the DCMS Report branded Facebook as a “digital gangster[]” that consider “to be ahead of and beyond the law.”<sup>333</sup> Likewise, by his refusal to appear before the DCMS Committee, “Zuckerberg has shown contempt towards both the UK Parliament and the ‘International Grand Committee’, involving members from nine legislatures from around the world.”<sup>334</sup> In conclusion, the DCMS Report states that companies including Facebook “must not be allowed to expand exponentially, without constraint or proper regulatory oversight,” and that “only governments and the law are powerful enough to contain them.”<sup>335</sup>

657. Based on the extensive evidence considered by the DCMS Committee, the DCMS Report includes numerous findings and statements regarding and directly relevant to Facebook’s conduct resulting in the Cambridge Analytica Scandal, including:

- a. “[T]he advertising profile that Facebook builds up about users cannot be accessed,

---

<sup>329</sup> David Pegg, *Facebook labelled ‘digital gangsters’ by report on fake news* (Feb. 17, 2019, 7:01pm), <https://www.theguardian.com/technology/2019/feb/18/facebook-fake-news-investigation-report-regulation-privacy-law-dcms>.

<sup>330</sup> *Id.*

<sup>331</sup> *Id.*

<sup>332</sup> DCMS Report, *supra* note 28 ¶ 136.

<sup>333</sup> *Id.* ¶ 139.

<sup>334</sup> *Id.* ¶ 29.

<sup>335</sup> *Id.* 5.

controlled or deleted by those users. It is difficult to reconcile this fact with the assertion that users own all ‘the content’ they upload”;<sup>336</sup>

- b. “The Cambridge Analytica scandal was facilitated [sic] by Facebook’s policies. If it had fully complied with the FTC settlement, it would not have happened. . . . Elizabeth Denham, the Information Commissioner, told us: ‘I am very disappointed that Facebook, being such an innovative company, could not have put more focus, attention and resources into protecting people’s data.’ We are equally disappointed”;<sup>337</sup>
- c. The fact that Apps including Whitelisted Apps and Business Partners “were able to circumvent users’ privacy of platform settings and access friends’ information, even when the user disabled the Platform,” is “an example of Facebook’s business model driving privacy violations”;<sup>338</sup>
- d. Documents obtained by the DCMS Committee, which had originally been filed under seal in the context of ongoing litigation in the Superior Court of California, County of San Mateo, reveal that “increasing revenues from major app developers was one of the key drivers behind the policy changes [including the shift from Graph API v1.0 to v2.0] made by Facebook. The idea of linking access to friends’ data to the financial value of the developers’ relationship with Facebook was a recurring feature of the documents”;<sup>339</sup>
- e. These documents also “demonstrate the interlinkages between the value of access to friends’ data to advertising spending, and Facebook’s preferential whitelisting process.” In this regard, “it is clear that spending substantial sums with Facebook, as a condition of maintaining preferential access to personal data, was part and parcel of the company’s strategy of platform development as it embraced the mobile advertising world”;<sup>340</sup>
- f. These documents include emails from Zuckerberg, including one in which he “discusses

---

<sup>336</sup> *Id.* ¶ 41.

<sup>337</sup> *Id.* ¶ 76.

<sup>338</sup> *Id.* ¶ 83.

<sup>339</sup> *Id.* ¶ 87.

<sup>340</sup> *Id.* ¶¶ 95-96.



the concept of reciprocity and data value, and also refers to ‘pulling non-App friends out of friends.get,’ thereby prioritising developer: . . . access to data from users who had not granted data permission to the developer: access to app friends.” In this email, Zuckerberg stated: “We also need to figure out how we’re going to charge for it [access to app friends]. I want to make sure this is explicitly tied to pulling non-app friends out of friends.get [allowing access to information about app friends]. . . . What I’m assuming we’ll do here is have a few basic thresholds of API usage and once you pass a threshold you either need to pay us some fixed amount to get to the next threshold or you get rate limited at the lower threshold. . . . I think this finds the right balance between ubiquity, reciprocity and profit.” On November 19, 2012, Sandberg replied to this email, expressing her agreement with this approach, stating, “I like full reciprocity and this is the heart of why”;<sup>341</sup>

- g. The concept of “reciprocity,” to which Zuckerberg and Sandberg refer in the email exchange above, “highlights the outlook and the business model of Facebook. ‘Reciprocity’ agreements with certain Apps enabled Facebook to gain as much information as possible, by requiring Apps that used data from Facebook to allow their users to share of their data back to Facebook (with scant regard to users’ privacy)”;<sup>342</sup>
- h. Another email by Zuckerberg, dated on or around January 24, 2013, demonstrates that Facebook denied access to friends data for anticompetitive reasons, “targeting [] Twitter’s Vine app, a direct competitor to Instagram, by shutting down its use of Facebook’s Friends API.” In response to an email advising him of the launch of Vine, and Facebook’s plan to “shut down their friends API access today,” as well as Facebook’s preparation of “reactive PR,” Zuckerberg responded “Yup, go for it.”<sup>343</sup> Ultimately Twitter shut down its Vine App “in part due to the fact that they could not

---

<sup>341</sup> *Id.* ¶ 105.

<sup>342</sup> *Id.* ¶ 106.

<sup>343</sup> *Id.* ¶ 116 (emphasis in original).

grow their user base”;<sup>344</sup>

- i. These documents also “reveal[] the fact that Facebook’s profit comes before anything else,” and that “Facebook continues to choose profit over data security, taking risks in order to prioritise their aim of making money from user data.” Further, “Facebook has continually hidden behind obfuscation,” and “[w]hen they are exposed, ***Facebook ‘is always sorry, they are always on a journey,’***” as Charlie Angus, MP (Vice-Chair of the Canadian Standing Committee on Access to Information, Privacy and Ethics, and member of the ‘International Grand Committee’) described them”;<sup>345</sup>
- j. These documents “indicate[] that Facebook was willing to override its users’ privacy settings in order to transfer data to some app developers, to charge high prices in advertising to some developers, for the exchange of that data.” Further, from these documents “it is evident that Facebook intentionally and knowingly violated both data privacy and anti-competition laws,” and “was, at the very least, in violation of its Federal Trade Commission settlement”;<sup>346</sup> and
- k. “In portraying itself as a free service, Facebook gives only half the story.”<sup>347</sup> Ashkan Soltani, former Chief Technologist to the FTC, stated that, in fact, Facebook involves a transaction involving value provided to Facebook by its users: “it is an exchange of personal information that is given to the platform, mined, and then resold to or reused by third-party developers to develop Apps, or resold to advertisers to advertise with.”<sup>348</sup> In this regard, the DCMS Report stated that “[w]e consider that data transfer for value is Facebook’s business model and that Mark Zuckerberg’s statement that ‘we’ve never sold anyone’s data’ is simply untrue.”<sup>349</sup>

---

<sup>344</sup> *Id.* ¶ 117.

<sup>345</sup> *Id.* ¶ 125.

<sup>346</sup> *Id.* ¶¶ 135-36.

<sup>347</sup> *Id.* at ¶ 128.

<sup>348</sup> *Id.*

<sup>349</sup> *Id.* ¶ 134.

**H. In the Wake of the Cambridge Analytica Scandal, Facebook Has Acknowledged That It Breached Users' Trust.**

658. On March 21, 2018, Facebook issued a statement acknowledging that it had breached users' trust: "What happened with Cambridge Analytica was a breach of Facebook's trust. More importantly, it was a breach of the trust people place in Facebook to protect their data when they share it."<sup>350</sup>

659. Days later, Facebook admitted that its current disclosures and privacy settings were confusing and ineffective. On March 28, 2018, Facebook issued a press release stating that it would take steps to making their privacy controls easier to find. Facebook stated its purpose in changing these controls was to "put people more in control of their privacy."<sup>351</sup>

660. On April 4, 2018, Facebook announced that it would update its documents to "better spell out what data we collect and how we use it."<sup>352</sup> Facebook's statement is an implicit admission that its documents were confusing to users. Facebook also announced a series of changes to its third-party APIs. Mark Zuckerberg commented on the changes being made to Facebook's APIs stating: "The basic idea here is that you should be able to sign into apps and share your public information easily, but anything that might also share other people's information . . . should be more restricted."<sup>353</sup> This statement acknowledges the need to better protect the information from third parties accessing users' information through users' Friends.

---

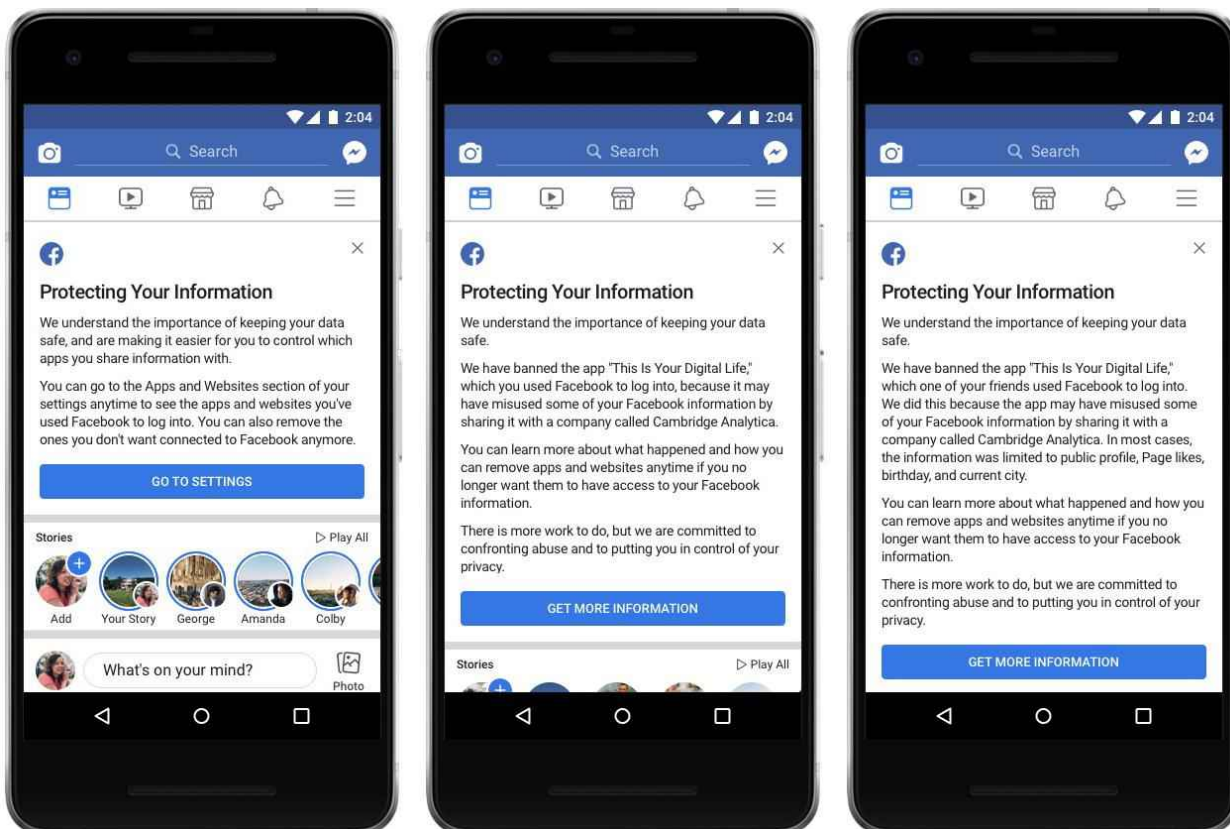
<sup>350</sup> *Cracking Down on Platform Abuse*, Facebook Newsroom (Mar. 21, 2018), <https://newsroom.fb.com/news/2018/03/cracking-down-on-platform-abuse/>.

<sup>351</sup> Erin Egan, *It's Time to Make Our Privacy Tools Easier to Find*, Facebook Newsroom (Mar. 28, 2018), <https://newsroom.fb.com/news/2018/03/privacy-shortcuts/>.

<sup>352</sup> Erin Egan, *We're Making Our Terms and Data Policy Clearer, Without New Rights to Use your Data on Facebook*, Facebook Newsroom (Apr. 4, 2018), <https://newsroom.fb.com/news/2018/04/terms-and-data-policy/>.

<sup>353</sup> *Hard Questions: Q&A With Mark Zuckerberg on Protecting People's Information*, Facebook Newsroom (Apr. 4, 2018), <https://newsroom.fb.com/news/2018/04/hard-questions-protecting-peoples-information/>.

661. Facebook has also acknowledged its duty to protect users' information. On April 9, 2018,



Facebook placed one of the following three messages at the top of users' News Feed:<sup>354</sup>

662. The blue link allowed users to view what Apps they used and what information they shared with Apps. In each message, Facebook stated that it “understand[s] the importance of keeping [users'] data safe.” This statement is an acknowledgment of its duty to users.

663. The DCMS Report analyzed comments made by Facebook's Richard Allan, wherein Allan acknowledged Facebook's inadequate disclosures:<sup>355</sup>

Richard Allan also admitted to us that people might indeed take issue with Facebook's position: “we were confident that the controls we implemented constituted consent and permission—others would contest that”. He seemed to justify Facebook's continued allowance of data access by app developers, by stating that the users had given their

<sup>354</sup> Mike Schroepfer, *An Update on Our Plans to Restrict Data Access on Facebook*, Facebook Newsroom (Apr. 4, 2018), <https://newsroom.fb.com/news/2018/04/restricting-data-access/>.

<sup>355</sup> DCMS Report, *supra* note 28, ¶ 75.

consent to this data access. *The fact that Facebook continued to allow this access after the Consent Decree is not new information; the new information is the admission by Richard Allan that the CEO and senior management—“all of us”—knew that Facebook was continuing to allow the practice to occur, despite the public statements about its change of policy. That, people might well contest, constituted deceit and we would agree with them.* (Emphasis added)

664. Facebook’s statements as well as the changes it made to strengthen privacy controls and restrict third-party’s access to Friends’ information in the wake of the Cambridge Analytica Scandal are an acknowledgment that Facebook breached its duty to protect users’ information.

## **I. Facebook’s CEO Authorized Decisions That Gave Rise to Privacy Violations**

### **1. Statements by Facebook’s CEO Give Rise to a Duty to Disclose and Admit to Injury from Lack of Disclosure.**

665. Defendant Mark Zuckerberg exerts immense personal control over the direction and decisions of the Company. When Facebook staged its initial public offering six years ago, it implemented a dual-class share structure that allows Zuckerberg to personally control a majority of the voting stock even though other investors own the majority of the financial value of the Company. In this regard, former Facebook employee and insider Tavis McGinn “realized that even on the inside, [he] was not going to be able to change the way that the company does business,” because “Facebook is Mark, and Mark is Facebook.”<sup>356</sup> Likewise, McGinn stated, “Mark has 60 percent voting rights for Facebook. So you have one individual, 33 years old, who has basically full control of the experience of 2 billion people around the world. That’s unprecedented. Even the president of the United States has checks and balances. At Facebook, it’s really this one person.”

666. Zuckerberg has promised users over and over again that it cares about privacy and that it would protect their content and information. In an op-ed in The Washington Post in May 2010, Zuckerberg outlined the “principles under which Facebook operates” respecting privacy and users’ content and information. “You have control over how your information is shared,” he wrote. “We do not share your personal information with people or services you don’t want. We do not give advertisers access to your personal information. We do not and never will sell any of your information to

---

<sup>356</sup> McNamee, *supra* note 302, at 168.

anyone.”<sup>357</sup>

667. Zuckerberg also created the illusion of security for personal content shared by Plaintiffs. Creating “Zuckerberg’s Law,” Zuckerberg built a user base and platform that was designed to encourage users to share an endless stream of content and information: “I would expect that next year, people will share twice as much information as they share this year, and next year, they will be sharing twice as much as they did the year before,” he said. “That means that people are using Facebook, and the applications and the ecosystem, more and more.”<sup>358</sup>

668. Zuckerberg created this false sense of security by stressing that, while Facebook was built on sharing, it “encouraged” privacy. On June 2, 2010, Zuckerberg stated at a f8 conference:

Privacy is very important to us. I think there are some misperceptions. People use Facebook to share and to stay connected. You don’t start off on Facebook being connected to your friends, you’ve got to be able to find them. So having some information available broadly is good for that. Now, there have been misperceptions that we’re trying to make all information open, but that’s false. We encourage people to keep their most private information private.<sup>359</sup>

Facebook did not disclose that, in fact, its default settings were precisely the opposite of what Zuckerberg described. A trove of content and information that was the most private and intimate to Plaintiffs—such as photographs, videos, “likes,” location information, and “status updates”—were by default set to be disclosed to App Developers through their Friends. Facebook also failed to tell users that the content and information shared with their Friends would be accessed by Business Partners and Whitelisted Apps.

669. Zuckerberg also made control of content and information by Plaintiffs a foundational pledge. Following the FTC’s investigation, he posted on his Facebook page on November 29, 2011,

---

<sup>357</sup> Mark Zuckerberg, *From Facebook, answering privacy concerns with new settings*, The Wash. Post (May 24, 2010), <http://www.washingtonpost.com/wp-dyn/content/article/2010/05/23/AR2010052303828.html>.

<sup>358</sup> Saul Hansell, *Zuckerberg’s Law of Information Sharing*, N.Y. Times (Nov. 6, 2008, 7:03pm), <https://bits.blogs.nytimes.com/2008/11/06/zuckerbergs-law-of-information-sharing/>.

<sup>359</sup> Chad Catacchio, *Zuckerberg at D8: ‘we recommend privacy settings, we did not change any settings’*, TNW (June 2, 2010), <https://thenextweb.com/socialmedia/2010/06/03/zuckerberg-at-d8-we-recommend-privacy-settings-we-did-not-change-any-settings/>.



I founded Facebook on the idea that people want to share and connect with people in their lives, but to do this *everyone needs complete control over who they share with at all times*. This idea has been the core of Facebook since day one. When I built the first version of Facebook, almost nobody I knew wanted a public page on the internet. That seemed scary. *But as long as they could make their page private, they felt safe sharing with their friends online. Control was key.* With Facebook, for the first time, people had the tools they needed to do this. That's how Facebook became the world's biggest community online. We made it easy for people to feel comfortable sharing things about their real lives.<sup>360</sup>

670. In the same post, Zuckerberg doubled down on his promise of privacy and security of content and information:

[G]iving you tools to control who can see your information and then making sure only those people you intend can see it. . . . As a matter of fact, privacy is so deeply embedded in all of the development we do that every day tens of thousands of servers worth of computational resources are consumed checking to make sure that on any webpage we serve, that you have access to see each of the sometimes hundreds or even thousands of individual pieces of information that come together to form a Facebook page. . . . We do privacy access checks literally tens of billions of times each day to ensure we're enforcing that only the people you want see your content. These privacy principles are written very deeply into our code.<sup>361</sup>

In reality, however, Facebook did not give Plaintiffs the “tools” they needed to prevent their information from being shared to App Developers, Business Partners, Whitelisted Apps, advertisers, and other third parties.

671. After a report of court-ordered U.S. government surveillance requests through Facebook surfaced in 2014 relating to the National Security Agency's “Prism” effort,<sup>362</sup> Zuckerberg reiterated Facebook's commitment to securing content and information, even though he was aware that Facebook had refused to perform audits as recommend by its executives with oversight responsibilities over App Developers:

---

<sup>360</sup> Mark Zuckerberg, *Our Commitment to the Facebook Community*, Facebook (Nov. 29, 2011), <https://www.facebook.com/notes/facebook/our-commitment-to-the-facebook-community/10150378701937131/>.

<sup>361</sup> *Id.*

<sup>362</sup> Glenn Greenwald and Ewen MacAskill, *NSA Prism program taps in to user data of Apple, Google and others*, *The Guardian* (June 7, 2013, 3:23pm), <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>.



To keep the internet strong, we need to keep it secure. That's why at Facebook we spend a lot of our energy making our services and the whole internet safer and more secure. We encrypt communications, we use secure protocols for traffic, we encourage people to use multiple factors for authentication and we go out of our way to help fix issues we find in other people's services. . . . Unfortunately, it seems like it will take a very long time for true full reform. So it's up to us—all of us—to build the internet we want. Together, we can build a space that is greater and a more important part of the world than anything we have today, but is also safe and secure.<sup>363</sup>

672. Zuckerberg began 2018 by admitting that Facebook had failed to protect Plaintiffs' content and information:

The world feels anxious and divided, and Facebook has a lot of work to do—whether it's protecting our community from abuse and hate, defending against interference by nation states, or making sure that time spent on Facebook is time well spent. My personal challenge for 2018 is to focus on fixing these important issues. We won't prevent all mistakes or abuse, but *we currently make too many errors enforcing our policies and preventing misuse of our tools.*<sup>364</sup>

673. When the Cambridge Analytica Scandal broke in March 2018, Zuckerberg admitted that this revelation demonstrated that Facebook had failed to secure Plaintiffs' content and information: “This was clearly a mistake. We have a basic responsibility to protect people's data, and if we can't do that then we don't deserve to have the opportunity to serve people.”<sup>365</sup>

674. Zuckerberg also issued a statement on March 21, 2018 acknowledging that the Cambridge Analytica Scandal is a “breach of trust between Facebook and the people who share their data with us and expect us to protect it.”<sup>366</sup> He announced that due to Facebook's past errors, it was “going to review thousands of apps” and that it would be “an intensive process, but this is important.”

---

<sup>363</sup> Mark Zuckerberg, Facebook (Mar. 13, 2014), <https://www.facebook.com/zuck/posts/10101301165605491>.

<sup>364</sup> Mark Zuckerberg, Facebook (Jan. 4, 2018), <https://www.facebook.com/zuck/posts/10104380170714571>.

<sup>365</sup> Danielle Wiener-Bronner, *Mark Zuckerberg has regrets: 'I'm really sorry that this happened'*, CNN (Mar. 21, 2018, 10:17pm), <http://money.cnn.com/2018/03/21/technology/mark-zuckerberg-apology/index.html>; *Mark Zuckerberg in his own words: The CNN interview*, CNN (Mar. 21, 2018, 11:35pm), <http://money.cnn.com/2018/03/21/technology/mark-zuckerberg-cnn-interview-transcript/>.

<sup>366</sup> Mark Zuckerberg, Facebook (Mar. 21, 2018), <https://www.facebook.com/zuck/posts/10104712037900071>.

Zuckerberg conceded, “[T]his is something that in retrospect we clearly should have done, upfront, with Cambridge Analytica. We should not have trusted the certification that they gave us. And we’re not gonna make that mistake again. I mean this is our responsibility to our community, is to make sure that we secure the data that they’re sharing with us.”<sup>367</sup>

675. In a Q&A with reporters in April 2018 regarding the Cambridge Analytica Scandal, Zuckerberg stated that it is an “idealistic and optimistic company” but that “it’s clear now that we didn’t do enough.”<sup>368</sup> Zuckerberg further stated:

We didn’t focus enough on preventing abuse and thinking through how people could use these tools to do harm as well. That goes for fake news, foreign interference in elections, hate speech, in addition to developers and data privacy. We didn’t take a broad enough view of what our responsibility is, and that was a huge mistake. It was my mistake.

676. In response to a question regarding the company did not audit the use of Graph API from the 2010 to 2015 period, Zuckerberg stated:<sup>369</sup>

[I]n retrospect, I think we clearly should have been doing more all along. But just to speak to how we were thinking about it at the time, as just a matter of explanation, I’m not trying to defend this now. . . . I think today, given what we know, not just about developers, but across all of our tools, and across what our place in society is, it’s such a big service that’s so central in peoples’ lives. I think we need to take a broader view of our responsibility. We’re not just building tools, but we need to take full responsibility for the outcome and how people use those tools as well. That’s at least why we didn’t do it at the time, but knowing what I know today, clearly we should have done more. And we will going forward.

677. In his April 2018 testimony before Congress, Zuckerberg publicly claimed responsibility for Plaintiffs’ privacy on the Facebook platform. “We didn’t take a broad enough view of our responsibility, and that was a big mistake,” Zuckerberg admitted. “It was my mistake, and I’m sorry. I started Facebook, I run it, and I’m responsible for what happens here.” Zuckerberg’s statements

---

<sup>367</sup> Seth Fiegerman, *Mark Zuckerberg tells CNN he is 'happy to' testify before Congress*, CNN (Mar. 21, 2018, 9:03 PM ET) (emphasis added), <https://money.cnn.com/2018/03/21/technology/mark-zuckerberg-cnn-interview/index.html?iid=EL>.

<sup>368</sup> *Hard Questions: Q&A With Mark Zuckerberg on Protecting People’s Information*, Facebook Newsroom (Apr. 4, 2018), <https://newsroom.fb.com/news/2018/04/hard-questions-protecting-peoples-information/>.

<sup>369</sup> *Id.*

conceded that Facebook had failed to fulfill its promise that Facebook users owned and controlled their content and information: “It’s not enough to just give people control over their information, we need to make sure that the developers they share it with protect their information too.”<sup>370</sup>

678. In an end-of-year Facebook post on his own profile, Zuckerberg disclosed that in 2018, one of his “personal challenges” was “addressing some of the most important issues facing our community [including] making sure people have control of their information.” Acknowledging Facebook’s past failure to take any steps in this direction, Zuckerberg explained, “[W]e changed our developer platform to reduce the amount of information apps can access. . . . We reduced some of the third-party information we use in our ads systems.”<sup>371</sup>

679. Zuckerberg’s statements before and in the wake of the Cambridge Analytica Scandal demonstrate that Facebook had failed to secure Plaintiffs’ content and information. They also gave rise to numerous duties by Facebook.

680. On May 27, 2010, Zuckerberg alleged publicly that Facebook required App Developers to respect users’ Privacy Settings:

There’s this false rumor that’s been going around which says that we’re sharing private information with applications and it’s just not true. The way it works, is . . . if you choose to share some information with everyone on the site, that means that any person can go look up that information and any application can go look up that information as well. . . . But applications have to ask for permission for anything that you’ve set to be private.<sup>372</sup>

These statements gave rise to a duty to inform Plaintiffs about the full extent to which App Developers and other third parties including Business Partners and Whitelisted Apps were able to access their personal content notwithstanding privacy settings, and to disclose the risk that Facebook would be unable to secure content and information that was shared with third parties.

---

<sup>370</sup> *Facebook CEO Mark Zuckerberg Hearing on Data Privacy and Protection*, C-SPAN (Apr. 10, 2018), <https://www.c-span.org/video/?443543-1/facebook-ceo-mark-zuckerberg-testifies-data-protection> (complete opening statement in Senate Hearing).

<sup>371</sup> Mark Zuckerberg, Facebook (Dec. 28, 2018), <https://www.facebook.com/zuck/posts/10105865715850211>.

<sup>372</sup> Mark Memmot, *Zuckerberg: Sharing Is What Facebook Is About*, NPR All Things Considered (May 27, 2010, 3:42pm), <https://www.npr.org/sections/alltechconsidered/2010/05/27/127210855/facebook-zuckerberg-privacy>.

681. Zuckerberg went on, making statements that gave rise to an additional duty to disclose that Facebook allowed advertisers and marketers to target Plaintiffs by combining their content and information with other data:

Advertisers never get access to your information. We never sell anyone's information and we have no plans to ever do that in the future. Now, in order to run a service like this that serves more than 400 million users, it does cost money . . . so we do have to make money and the way we do that is through . . . advertising. Advertisers come to us and they say what they want to advertise and we show advertisements to people who we think are going to be most interested. . . . ***But at no part in that process is any of your information shared with advertisers.***<sup>373</sup>

**J. Facebook's CEO Drove Initiatives to Erode Privacy and Monetize Access to Content and Information.**

682. Under Zuckerberg, Facebook's guiding principle was "Move fast and break things. Unless you are breaking stuff, you are not moving fast enough."<sup>374</sup> This principle was executed through a "growth at any cost" corporate culture. In this regard, early Facebook investor and former Zuckerberg advisor Roger McNamee describes Facebook's focus on "growth hacking," the goal of which "is to generate more revenue and profits, and at Facebook those metrics blocked out all other considerations. In the world of growth hacking, users are a metric, not people. It is unlikely that civic responsibility ever came up in Facebook's internal conversations about growth hacking."<sup>375</sup>

683. Zuckerberg's trusted fellow Facebook executive, Andrew Bosworth, articulated this vision by saying that the sharing of data

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

And still we connect people.

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

---

<sup>373</sup> *Id* (emphasis added).

<sup>374</sup> Zoe Henry, *Mark Zuckerberg's 10 Best Quotes Ever*, Inc., <https://www.inc.com/zoe-henry/mark-zuckerberg-move-fast-and-break-things.html> (last visited Feb. 22, 2019)

<sup>375</sup> McNamee, *supra* note 302, at 76.

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

That's why all the work we do in growth is justified.

684. Post-Cambridge Analytica Scandal, after Bosworth's comments were published, Zuckerberg tried to walk them back, stating, "We've never believed the ends justify the means," but the culture of recklessness that Zuckerberg instilled was undeniable.<sup>376</sup>

685. Zuckerberg has taken responsibility for Facebook's privacy policy. In April 2018, Zuckerberg stated "the first line of our Terms of Service says that you control and own the information and content that you put on Facebook. . . . [Y]ou own [your data] in the sense that you chose to put it there, you could take it down anytime, and you completely control the terms under which it's used."<sup>377</sup> This statement was false at the time that it was made.

686. That was not the first time that Zuckerberg misled Facebook users about its privacy policy. In May 2010, after reporters found a privacy loophole allowing advertisers to access user identification, Zuckerberg promised: "We will add privacy controls that are much simpler to use. We will also give you an easy way to turn off all third-party services."<sup>378</sup>

687. In 2011, after Facebook settled the FTC investigation, Zuckerberg stated, "I'm the first to admit that we've made a bunch of mistakes. . . . Facebook has always been committed to being transparent about the information you have stored with us."<sup>379</sup>

---

<sup>376</sup> Ryan Mac, *Growth At Any Cost: Top Facebook Executive Defended Data Collection In 2016 Memo — And Warned That Facebook Could Get People Killed*, BuzzFeed (March 29, 2018), <https://www.buzzfeednews.com/article/ryanmac/growth-at-any-cost-top-facebook-executive-defended-data>.

<sup>377</sup> *Transcript of Mark Zuckerberg's Senate hearing*, The Washington Post (Apr. 10, 2018), [https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?utm\\_term=.eca9688c6274](https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?utm_term=.eca9688c6274).

<sup>378</sup> Geoffrey A. Fowler and Chiqui Esteban, *14 Years of Zuckerberg Saying Sorry, Not Sorry*, The Washington Post (Apr. 9, 2018), [https://www.washingtonpost.com/graphics/2018/business/facebook-zuckerbergapologies/?utm\\_term=.db1e361d79fd](https://www.washingtonpost.com/graphics/2018/business/facebook-zuckerbergapologies/?utm_term=.db1e361d79fd).

<sup>379</sup> Mark Zuckerberg, *Our Commitment to the Facebook Community*, Facebook (Nov. 19, 2011), <https://www.facebook.com/notes/facebook/our-commitment-to-the-facebookcommunity/10150378701937131/>.

688. Following the Cambridge Analytica Scandal, Zuckerberg again misled Facebook users into believing that their privacy controls had efficacy, stating, “[T]o prevent abusive apps, we announced that we were changing the entire platform to dramatically limit the data apps could access. Most importantly, apps like Kogan’s could no longer ask for data about a person’s friends unless their friends had also authorized the app.”<sup>380</sup> This statement, made in March of 2018, neglected to inform Plaintiffs of Facebook’s Business Partners and Whitelisted Apps, which were immune to privacy settings.

689. Zuckerberg is responsible for the direction of Facebook’s strategy with respect to granting access to Apps and monetizing Facebook’s platform.

690. Zuckerberg directed Facebook’s program to generate revenue from Whitelisted Apps in exchange for access to Plaintiffs’ content and information.

691. On October 7, 2012, Zuckerberg wrote an email outlining his goals for monetizing content and information by granting Whitelisted Apps access in exchange for revenue generation:

I’ve been thinking about platform business model a lot this weekend. . . . if we make it so devs can generate revenue for us in different ways, then it makes it more acceptable for us to charge them quite a bit more for using platform.

The basic idea is that any other revenue you generate for us earns you a credit towards whatever fees you owe us for using pla[t]form. For most developers this would probably cover cost completely. So instead of every paying us directly, they’d just use our payments or ads products. A basic model could be:

- Login with Facebook is always free
- Pushing content to Facebook is always free
- Reading anything, including friends, costs a lot of money. Perhaps on the order of \$0.10/user each year.

For the money that you owe, you can cover it in any of the following ways:

- Buys ads from us in neko or another system

---

<sup>380</sup> Mark Zuckerberg, Facebook (Mar. 21, 2018), [https://mobile.facebook.com/story.php?story\\_fbid=10157217558586729&id=20531316728&\\_\\_tn\\_\\_=-R](https://mobile.facebook.com/story.php?story_fbid=10157217558586729&id=20531316728&__tn__=-R).

- Run our ads in your app or website (canvas apps already do this)
- Use our payments
- Sell your items in our Karma store.
- Or if the revenue we get from those doesn't add up to more than the fees you owe us, then you just pay us the fee directly.<sup>381</sup>

692. In this context, it is evident that “Facebook had not protected user data privacy because sharing data broadly was much better for its business. Third-party applications increased usage of Facebook—time on site—a key driver of revenue and profits. The more time a user spends on Facebook, the more ads he or she will see and the more valuable that user will be. From Facebook’s perspective, anything that increases usage is good.”<sup>382</sup>

693. Zuckerberg also pushed to erode the privacy features of WhatsApp, an encrypted communication App acquired by Facebook, seeking to expose users to additional targeted ads, which resulted in the departure of WhatsApp’s founder.<sup>383</sup>

## V. PLAINTIFFS SUFFERED INJURY AND DAMAGES AS A DIRECT RESULT OF FACEBOOK’S CONDUCT

694. Facebook impermissibly collected and curated Plaintiffs’ content and information and then sold access to thousands of third parties without Plaintiffs’ knowledge or consent. Facebook’s acts enabled data brokers and others to de-anonymize users’ content and information and individually link it to Plaintiffs, targeting them with invasive and unwanted content. As a result, Plaintiffs have suffered injuries and will suffer ongoing injuries that fall into two principal categories: invasions of their privacy and economic injury.

### A. Plaintiffs Suffered Invasions of Their Privacy.

695. Facebook invaded Plaintiffs’ privacy by disseminating or causing the dissemination of

---

<sup>381</sup> *Note by Damian Collins MP, Chair of the DCMS Committee: Summary of Key Issues from the Six4Three files*, *supra* note 171.

<sup>382</sup> McNamee, *supra* note 302, at 192.

<sup>383</sup> Aaron Mak, *Another WhatsApp Founder Is Leaving Facebook—Reportedly Over How It Treats User Data*, Slate (Apr. 30, 2018) <https://slate.com/technology/2018/04/disagreements-with-facebook-over-privacy-drive-whatsapps-founder-to-leave-the-company.html>.



content and information that Plaintiffs reasonably believed was private. Plaintiffs intended those communications for limited audiences, primarily Friends. The content included photographs with geolocation data and time stamps, videos users had uploaded, accessed, or liked, also with geolocation data and time stamps, Plaintiffs' religious and political beliefs, their relationships, posts, and the pages they had liked. From this information, the thousands of third parties to whom access was granted, were able to draw inferences about Plaintiffs relating to their health, financial wherewithal and other critical issues.

696. As explained below, Plaintiffs suffered and are suffering ongoing egregious invasions of privacy as result of Facebook's conduct. For example, a user of a dating App like Tinder may have wished to keep information relating to that site private. But Facebook gave that information to thousands of third parties, which could include potential employers or others who may view such use with judgement. Other examples are even more invasive. An App for brassiere company Brayola allowed people to scroll through photos of cleavage and give it a thumbs up or down. Users whose Friends unwittingly passed on even innocuous seeming photos to them and then downloaded Brayola gave their Friends' photos to the App. The App Hot or Not, which was one of the Whitelisted Apps, allows users to rate the attractiveness of photos it has collected.<sup>384</sup> Similarly, the App Girls Around Me pulled data from Friends to tell App Users who was in the physical vicinity. These are just a few examples of unwanted, invasive and harmful uses of the content and information Facebook published to its Apps.

697. As a result, Plaintiffs experienced, and continue to experience, invasions of privacy and a loss of control of their content and information that endanger their financial, medical and emotional well-being, now and for the rest of their lives.

**1. Facebook Has Subjected Its Users to Highly Offensive, Harmful, and Invasive Forms of Psychographic Marketing.**

698. In addition to the privacy intrusions described above, Plaintiffs were harmed by psychographic marketing. Psychographic marketing targets Plaintiffs individually and attempts to

---

<sup>384</sup> *Note by Damian Collins MP, Chair of the DCMS Committee: Summary of Key Issues from the Six4Three files, supra* note 171.

manipulate them emotionally. Using the content and information that Facebook improperly disclosed to Apps, including Whitelisted Apps and Business Partners, third parties including Cambridge Analytica directly targeted specific Facebook users including Plaintiffs with advertisements that would be highly offensive to a reasonable person. Plaintiffs are and have been personally targeted with polarizing content intended to provoke them.

699. The Cambridge Analytica Scandal provides a specific example of how users are targeted, although it is not the only entity to be targeting Facebook users in this way. Cambridge Analytica “harvest[ed] the Facebook profiles of millions of people in the U.S., and to use their private and personal content and information to create sophisticated psychological and political profiles. And then target[ed] them with political ads designed to work on their particular psychological makeup.”<sup>385</sup> “Christopher Wylie, the former [Cambridge Analytica] employee who recently came forward to detail how the company improperly acquired personal data from fifty million Facebook users, has said that the company used that data to create a ‘psychological warfare mindfuck tool.’”<sup>386</sup>

700. Cambridge Analytica developed detailed voting profiles for U.S. and U.K. voters and used this information to develop psychographic models to direct messages to U.S. voters. Specifically, Cambridge Analytica used the survey responses provided by users of the This Is Your Digital Life App, in conjunction with the Personal Information of App users and their Friends that was obtained from Facebook, to “effectively take the Facebook likes of its subjects and work backwards, filling in the rest of the columns in the spreadsheet to arrive at guesses as to their personalities, political affiliations and more.”<sup>387</sup> Then, this data was used in combination with other data sets, including voter data and consumer data, to identify millions of individual Facebook users and predict their political affiliations

---

<sup>385</sup> Carole Cadwalladr, *‘I Made Steve Bannon’s Psychological Warfare Tool’: Meet the Data War Whistleblower*, The Guardian (Mar. 18, 2018), <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>.

<sup>386</sup> Sue Halpern, *Cambridge Analytica and the Perils of Psychographics*, The New Yorker (Mar. 30, 2018), <https://www.newyorker.com/news/news-desk/cambridge-analytica-and-the-perils-of-psychographics>.

<sup>387</sup> Cadwalladr, *‘I made Steve Bannon’s psychological warfare tool’*, *supra* note 385.

and personality types.<sup>388</sup> In turn, this enabled Cambridge Analytica to craft and deliver highly targeted—and highly offensive—advertisements intended to manipulate the votes of Facebook users, such as by encouraging some users to vote or by suppressing other users’ voting intentions.<sup>389</sup>

701. Alexander Nix stated that together with voter profiles, Cambridge Analytica used Plaintiffs’ content and information to “micro target” individual voters, running “4,000 different advertising campaigns—about 1.4 billion impressions.”<sup>390</sup> Much of this was on Facebook. In his recently published book *Zucked*, early Facebook investor and former Zuckerberg mentor Roger McNamee specifically identifies microtargeting as a threat to democracy: in combination with the “persuasive technologies” of platforms such as Facebook, “microtargeting becomes another tool for dividing us” and “transforms the public square of politics into the psychological mugging of every voter.”<sup>391</sup>

702. According to David Carroll, Professor at the Parsons School of Design in New York City:

[Cambridge Analytica] claim to have figured out how to project our voting behavior based on our consumer behavior. So it’s important for citizens to be able to understand this because it would affect our ability to understand how we’re being targeted by campaigns and how the messages that we’re seeing on Facebook and television are being directed at us to manipulate us. I think it is a matter of the relationship between privacy and democracy.<sup>392</sup>

703. The information provided by Facebook also helped Cambridge Analytica physically target people in the privacy of their homes. A report by Switzerland’s *Das Magazin* revealed that “Trump canvassers were provided with an App allowing them to identify the political views and personality type of a given house, and the outline conversation scripts that would work with the

---

<sup>388</sup> *Id.*

<sup>389</sup> *Id.*

<sup>390</sup> Statement of Claimant ¶ 20(h), *Carroll v. Cambridge Analytica Ltd.* [2018] EWHC (QB) (Eng.).

<sup>391</sup> *McNamee*, *supra* note 302, 238.

<sup>392</sup> Brent Bambury, *Data Mining Firm Behind Trump Election Built Psychological Profiles of Nearly Every American Voter*, CBC Radio (Mar. 20, 2018), <https://www.cbc.ca/radio/day6/episode-359-harvey-weinstein-a-stock-market-for-sneakers-trump-s-data-mining-the-curious-incident-more-1.4348278/data-mining-firm-behind-trump-election-built-psychological-profiles-of-nearly-every-american-voter-1.4348283>.

inhabitants.”<sup>393</sup>

704. Plaintiffs have suffered egregious invasions of privacy as a result of this marketing. These messages and advertisements would be highly offensive to a reasonable person.

705. The Cambridge Analytica Scandal also shows how the aggregation and ultimate deanonymization of users’ content and information, enables users’ content and information to be weaponized against them in incredibly personal ways. Cambridge Analytica sought to “exploit[] essentially mental vulnerabilities in certain types of people in the context of making them vote in a particular way.”<sup>394</sup> For instance, “a neurotic, extroverted and agreeable Democrat could be targeted with a radically different message than an emotionally stable, introverted, intellectual one, *each designed to suppress their voting intention*—even if the same messages, swapped around, would have the opposite effect.”<sup>395</sup>

706. The aggregated stolen data was used to deliver discriminatory and highly offensive advertisements to users, including Plaintiffs. For example, Cambridge Analytica sought to target African American voters with the goal of suppressing their votes: “Facebook posts were targeted at some black voters reminding them of Hillary Clinton’s 1990s description of black youths as ‘super predators,’ in the hope it would deter them from voting.”<sup>396</sup> Likewise, “[o]ne message used to boost rightwing turnout attacked same-sex marriage,” which “was targeting conscientious people. It was a picture of a dictionary and it said ‘Look up marriage and get back to me.’ For someone who is conscientious, it is a compelling message: a dictionary is a source of order, and a conscientious person

---

<sup>393</sup> Adam Lusher, *Cambridge Analytica: Who Are They, and Did They Really Help Trump Win the White House?*, Independent (Mar. 21, 2018), <https://www.independent.co.uk/news/uk/home-news/cambridge-analytica-alexander-nix-christopher-wylie-trump-brexit-election-who-data-white-house-a8267591.html>.

<sup>394</sup> Redazione, *Exclusive Interview with Christopher Wylie, the Cambridge Analytica Whistleblower*, Vogue (May 9, 2018), <https://www.vogue.it/en/news/daily-news/2018/05/09/interview-with-christopher-wylie-cambridge-analytica/>.

<sup>395</sup> Alex Hern, *Cambridge Analytica: How Did It Turn Clicks into Votes?*, Guardian (May 6, 2018), <https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie> (emphasis added).

<sup>396</sup> Olivia Solon, *Cambridge Analytica Whistleblower Says Bannon Wanted to Suppress Voters*, Guardian (May 16, 2018), <https://www.theguardian.com/uk-news/2018/may/16/steve-bannon-cambridge-analytica-whistleblower-suppress-voters-testimony>.

is more deferential to structure.”<sup>397</sup>

707. Likewise, Facebook’s advertising platform has been used to target users based on protected characteristics. For example, on July 24, 2018, the Washington State Office of Attorney General announced that Facebook signed a legally binding agreement to make changes to its “advertising platform by removing the ability of third-party advertisers to exclude ethnic and religious minorities, immigrants, LGBTQ individuals and other protected groups from seeing their ads.”<sup>398</sup> Similarly, on August 13, 2018, the Department of Housing and Urban Development (“HUD”) filed a complaint against Facebook, stating that “Facebook unlawfully discriminates by enabling advertisers to restrict which Facebook users receive housing-related ads based on race, color, religion, sex, familial status, national origin and disability.”<sup>399</sup>

708. Moreover, and perhaps most disturbingly, Facebook’s platform—including Facebook’s Custom Audiences feature—has been used by foreign nationals on behalf of the Russian Federation to compromise the integrity of a U.S. Presidential election and to polarize and destabilize the American public, threatening U.S. democracy and national security.

709. First, Facebook revealed that its platform was used to deliver advertisements by Russian actors to approximately 10 million Facebook users in the United States in conjunction with the 2016 elections.<sup>400</sup> These advertisements “touch[ed] on topics from LGBT matters to race issues to immigration to gun rights,” which mirror the subjects of advertisements placed or tested by Cambridge Analytica.<sup>401</sup> Shortly thereafter, in detailed disclosures to Congress, Facebook revealed that “Russian

---

<sup>397</sup> Hern, *Cambridge Analytica*, *supra* note 395.

<sup>398</sup> AG Ferguson Investigation Leads to Facebook Making Nationwide Changes to Prohibit Discriminatory Advertisements on its Platform, Wash. State Office of the Attorney Gen. (July 24, 2018), <https://www.atg.wa.gov/news/news-releases/ag-ferguson-investigation-leads-facebook-making-nationwide-changes-prohibit>.

<sup>399</sup> Housing Discrimination Complaint, *Assistant Sec’y for Fair Hous. & Equal Opportunity v. Facebook, Inc.* (Aug. 13, 2018), [https://www.hud.gov/sites/dfiles/PIH/documents/HUD\\_01-18-0323\\_Complaint.pdf](https://www.hud.gov/sites/dfiles/PIH/documents/HUD_01-18-0323_Complaint.pdf).

<sup>400</sup> Elliot Schrage, *Hard Questions: Russian Ads Delivered to Congress*, Facebook Newsroom (Oct. 2, 2017), <https://newsroom.fb.com/news/2017/10/hard-questions-russian-ads-delivered-to-congress/>.

<sup>401</sup> *Id.*; see also Cadwalladr, ‘I made Steve Bannon’s psychological warfare tool’, *supra* note 385.

agents intending to sow discord among American citizens disseminated inflammatory posts that ***reached 126 million users on Facebook.***<sup>402</sup> According to *The New York Times*, these revelations—published the day before Facebook was set to testify before Congress—go “far beyond” what companies including Facebook “have revealed in the past and underline the breadth of the Kremlin’s efforts to lever open divisions in the United States using American technology platforms, especially Facebook.”<sup>403</sup>

710. In *Zucked*, Roger McNamee puts a fine point on the significance of this disclosure:

Having denied any role in the Russian interference campaign for eight months, only to concede that an internal investigation had uncovered one hundred thousand dollars’ worth of Russian advertising purchases in rubles, this revelation came as a bombshell. The user number represents more than one-third of the US population, but that grossly understates its impact. The Russians did not reach a random set of 126 million people on Facebook. Their efforts were highly targeted. On the one hand they had targeted people likely to vote for Trump with motivating messages. On the other, they identified subpopulations of likely Democratic voters who might be discouraged from voting. The fact that four million people who voted for Obama in 2012 did not vote for Clinton in 2016 may reflect to some degree the effectiveness of the Russian interference. . . . In an election where only 137 million people voted, a campaign that targeted 126 million eligible votes almost certainly had an impact.<sup>404</sup>

711. Thus, “Cambridge Analytica and the Trump campaign had exploited Facebook, just as the Russians had,” and—in light of the fact that “Cambridge Analytica had been the Trump campaign’s primary advisor for digital operations and that Facebook had embedded three employees in the Trump campaign to support that effort”—“there could be little doubt that Facebook had willingly engaged with Kogan, Cambridge Analytica, and the Trump campaign.” In short, “[i]t was entirely possible that Facebook employees had played a direct role in the success of Trump’s digital strategy on Facebook.”<sup>405</sup>

712. Facebook’s invasions of user privacy—not only its unlawful disclosure of user content

---

<sup>402</sup> Mike Isaac & Daisuke Wakabayashi, *Russian Influence Reached 126 Million Through Facebook Alone*, N.Y. Times (Oct. 30, 2017), <https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html>.

<sup>403</sup> *Id.*

<sup>404</sup> *McNamee*, *supra* note 302, 130-31.

<sup>405</sup> *McNamee*, *supra* note 302, 187.

and information, but also its enabling and allowing bad actors such as Cambridge Analytica to directly target users with highly offensive advertisements designed to prey on users' psychology in order to manipulate and suppress their voting intentions—as well as Facebook's concomitant reckless and willful disregard of a clear and present threat to U.S. election integrity and national security in its relentless pursuit of revenue and growth, represents one of the most highly offensive instances of conduct by a U.S. corporation in history, and certainly constitutes an egregious violation of social norms.

713. Whistleblower and former Cambridge Analytica Director of Research, Christopher Wylie, described Cambridge Analytica's targeted political advertising as “worse than bullying,” because “people don't necessarily know it's being done to them. At least bullying respects the agency of people because they know. So it's worse, because if you do not respect the agency of people, anything that you're doing after that point is not conducive to a democracy. And fundamentally, information warfare is not conducive to democracy.”<sup>406</sup>

714. Similarly, Wylie asserted users perceived advertisements placed in a Facebook user's News Feed with less scrutiny than traditional political advertisements:

[B]ecause nobody knows that's happening—the opposition doesn't know that's happening. If it's also presented to you as a news item, you as the voter don't know there's an agenda behind it. If you don't know who the messenger is, what the agenda is, and you don't see the other side of something, and you keep seeing pieces of information that aren't true or are highly suggestive, and you start making decisions or changing your perception of something—that's deception. That information creates an imbalance of power; you haven't been given to opportunity to see the other side, or to even know why it is that you're seeing that.<sup>407</sup>

715. As such, Plaintiffs are being targeted with political messaging that they did not authorize and the messaging is not being identified as such.

716. Moreover, the fact that users are not told who is targeting them hinders Plaintiffs' ability to protect themselves. Wylie explained the power of one-way anonymity in spreading disinformation:

---

<sup>406</sup> Cadwalladr, *'I made Steve Bannon's psychological warfare tool'*, *supra* note 385.

<sup>407</sup> Redazione, *supra* note 394.



The way it works is that you set up blogs and news sites—things that don’t look like campaign material—and you find people who would be most amenable to this particular conspiracy theory, unfact, “alternative fact”. You let them start going down the rabbit hole of clicking things. The idea is that you start showing them the same material from all these different kinds of sources, so they feel like they see it everywhere, but they don’t see it on the news, on CNN or the BBC. They then question why the “establishment” doesn’t want them to know something.<sup>408</sup>

This manipulation was enabled by the aggregation of the users’ content and information that Facebook collected and gave to Kogan over a period of years.

717. Cambridge Analytica is not the only App to have engaged in such invasive behavior. AggregateIQ and 400 other Apps have been suspended by Facebook for engaging in similar activity. Likewise, Facebook’s continued to publish user content and information to 5200 Whitelisted Apps even after the FTC Consent Decree.

718. The harm is ongoing. On August 22, 2018, Facebook confirmed that it continues to allow advertisers to target Facebook users with advertisements based on data obtained from data brokers, stating that it is allowable for “data providers and agencies [to] create, upload and then share certain Custom Audiences on behalf of advertisers,” and therefore Facebook is “clarifying [its] terms to make it clear that advertisers can do this—they can independently work with partners off our platform to create Custom Audiences, as long as they have the necessary rights and permissions to do so.”<sup>409</sup> Allowing users’ content and information to be used in these intrusive ways violates Facebook’s promise not to give advertisers’ the content and information of users.

719. Facebook users, including Plaintiffs, were not aware of and did not consent to receiving advertisements targeted directly to them through Facebook’s Custom Audiences feature.

720. On July 2, 2018, Facebook for the first time started requiring advertisers who wish to target specific Facebook users with advertisements to accept responsibility for obtaining permissions

---

<sup>408</sup> *Id.*

<sup>409</sup> *Introducing New Requirements for Custom Audience Targeting*, Facebook Business (June 13, 2018), <https://www.facebook.com/business/news/introducing-new-requirements-for-custom-audience-targeting> (last updated Aug. 22, 2018).

from such users.<sup>410</sup> TechCrunch notes, “Facebook is trusting advertisers to tell the truth about consent for targeting . . . despite them having a massive financial incentive to bend or break those rules,” and, although this new requirement “will give Facebook more plausible deniability in the event of a scandal, and it might deter misuse,” the fact remains that “Facebook is stopping short of doing anything to actually prevent non-consensual ad targeting.”<sup>411</sup> Moreover, despite the Cambridge Analytica Scandal, Facebook *still* does not require that users provide affirmative consent before advertiser are allowed to directly target users with advertisements through Facebook’s Custom Audiences feature.

721. Plaintiffs also face greater economic and privacy-related harms due to the aggregation of their content and information. There is a fast-growing market for consumer data of this kind. Data is aggregated and analyzed for a host of functions, including to create “consumer scores” which predict people’s propensity to become ill or pay off debt. Or, as the World Privacy Forum notes in a lengthy report, major health insurers are looking to collect data about individuals, such as whether “a couple bought hiking boots” or “a woman did a lot of online shopping,” in order to “figure out how much to charge people [for healthcare].”<sup>412</sup> As such, the collection and dissemination of users’ content and information could have a direct effect on something as impactful as how much people pay out-of-pocket for healthcare, resulting in economic harm.

722. Finally, the harm is irreparable. Because of Facebook’s failure to limit the dissemination of users’ information to reputable companies, the information is not recoverable. As CEO Zuckerberg recently admitted to Congress he “‘can’t really say’” if the Cambridge Analytica is in the hands of

---

<sup>410</sup> Reuters, *Facebook Releases New Privacy Safeguards on How Advertisers Handle Data*, NBC News (June 13, 2018), [https://www.nbcnews.com/tech/social-media/facebook-releases-new-privacy-safeguards-how-advertisers-handle-data-n882781?cid=sm\\_npd\\_nn\\_fb\\_ma](https://www.nbcnews.com/tech/social-media/facebook-releases-new-privacy-safeguards-how-advertisers-handle-data-n882781?cid=sm_npd_nn_fb_ma).

<sup>411</sup> John Constone, *Facebook Demands Advertisers Have Consent for Email/Phone Targeting*, TechCrunch (June 13, 2018), <https://techcrunch.com/2018/06/13/facebook-custom-audiences-consent/>.

<sup>412</sup> Pam Dixon and Robert Gellman, *The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future*, World Privacy Forum (Apr. 2, 2014) [http://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF\\_Scoring\\_of\\_America\\_April2014\\_fs.pdf](http://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf).

Russian operatives.<sup>413</sup> Moreover, Christopher Wylie testified that even if user data wasn't explicitly given to the Russians, "'the scale of the data and the location of the data was made known' in a way that would have made it relatively easy for an operative to access."<sup>414</sup> Wylie added that users' content and information could be used to create an algorithm to target Facebook users with profiles similar to those that were obtained by Cambridge Analytica.<sup>415</sup>

723. Also troubling are Facebook's partnerships with Huawei, now accused by the State Department of money laundering, bank fraud, and stealing trade secrets. Similarly, Facebook partners with Yandex, Russia's largest search engine, with a "syndication feed that gathers information about updates on its Pages and profiles."<sup>416</sup> The New York Times reported that Yandex had access to unique user IDs.<sup>417</sup> User IDs enable deanonymization because you can use it to look up a person's name.

724. Plaintiffs deserve clear disclosures about how Facebook has and is partnering with third parties and what content and information it has and is sharing with them.

#### **B. Plaintiffs Suffered Economic Injury.**

725. Plaintiffs suffered economic injuries which include, but are not limited to, (i) loss of benefits in their Facebook experience; (ii) heightened risk of identity theft and fraud; (iii) out-of-pocket costs; and (iv) loss of control over, property which has marketable value.

726. *Loss of benefits.* When Plaintiffs became Facebook users, they gained access to Facebook's social networking platform in exchange for sharing certain content and information with Facebook, conditioned upon their consent to such sharing. While Plaintiffs largely knew that Facebook would generate revenue by selling advertising which would be directed to them, it was a material term

---

<sup>413</sup> Jessica Guynn, *Mark Zuckerberg Is Willing to Testify to Congress, Isn't Sure If the Russians Have Your Data. and He's Sorry*, USA Today (Mar. 21, 2018), <https://www.usatoday.com/story/tech/news/2018/03/21/mark-zuckerberg-willing-testify-congress-not-sure-if-russians-have-your-data-and-hes-sorry/448084002/>.

<sup>414</sup> Anna Edgerton, *Facebook User Data May Have Gone to Russia, Whistle-Blower Says*, Bloomberg (May 16, 2018), <https://www.bloomberg.com/news/articles/2018-05-16/facebook-user-data-may-have-gone-to-russia-whistle-blower-says>.

<sup>415</sup> *Id.*

<sup>416</sup> *Yandex and Facebook Strike a Deal*, Facebook Newsroom (Oct. 29, 2010), <https://newsroom.fb.com/news/2010/10/yandex-and-facebook-strike-a-deal/>.

<sup>417</sup> Dance, et al, *As Facebook Raised a Privacy Wall*, *supra* note 158.

to the bargain that Plaintiffs were promised control over deciding what content was shared as well as how and with whom it would be disclosed.

727. Facebook did not honor the terms of this bargain. Although Facebook told Plaintiffs they owned their own content, in practice Facebook acted as if it did. When Facebook, without notice to Plaintiffs, shared their content and information with third parties that Plaintiffs had not chosen to share, Facebook received benefits—revenues associated with increased user activity and sale of additional data generated by this increase in activity—and transferred costs and harms to Plaintiffs—loss of privacy and control over their valuable content and information.

728. As Facebook expanded the scope of access to Plaintiffs' content and information beyond that to which Plaintiffs had agreed, users were denied the benefit of a Facebook experience where they defined the terms of their content sharing. Thus, through Facebook's actions and inactions, Plaintiffs have lost benefits. In order to preserve their privacy, users were presented with the choice of: (i) reducing their participation on Facebook by limiting the content and information they provide about themselves, (ii) accepting less privacy than that which they were promised; or (iii) ceasing their participation in Facebook altogether. Each of these options resulted in lost past value for Plaintiffs.

729. Moreover, Plaintiffs are also harmed prospectively. Plaintiffs' only options now are: (i) reducing or ending their participation on Facebook by limiting the content and information they provide about themselves; or (ii) knowingly accepting less privacy than that which they were promised. Each of these options deprives Plaintiffs of the remaining benefits of the original bargain.

730. Further, Plaintiffs were denied the benefit of this information and therefore the ability to mitigate harms they incurred as a result of Facebook's impermissible disclosure and publishing of their content and information.

731. ***Risk of identity theft and fraud.*** Plaintiffs' content and information is aggregated and pooled with other data collected by data brokers, including Facebook, to create digital dossiers or profiles. Through "linking" of data from these various sources, users' content and information can be de-anonymized. The disclosure of identifying information such as names of pets, grandparents, mother's maiden name, etc. greatly heightens the risk of identity theft and fraud to Plaintiffs because

such information is often used as “challenge questions” by financial and other institutions seeking to confirm identities.

732. Facebook further harmed Plaintiffs when it failed to notify them that their content and information could be or had been misappropriated via the Cambridge Analytica Scandal and/or by partnerships with other third parties. As just one example, following the first revelations of Cambridge Analytica’s psychographic profiling in 2015, Facebook failed to take steps to confirm that Cambridge Analytica, and any other entities which had unauthorized possession of users’ content and information, had properly deleted users’ content and information.

733. Indeed, additional revelations of Facebook’s failures to keep users’ content and information safe continue unabated, including additional data breaches and other improper sharing. Facebook’s choice to forego the costs of notification, deletion and other protective action transferred and imposed upon Plaintiffs further costs from the misappropriation. Without the benefit of notification and the ability to prevent future harm, Facebook caused Plaintiffs to bear the full burden of the risk of identity theft and fraud, as well as the ongoing imposition of targeted communications, that would be highly offensive to a reasonable person, by third parties in possession of users’ content and information.

734. The economic risks to Plaintiffs that they must mitigate are real and tangible. The risks of identity theft and fraud are long term and injure users in a multiplicity of ways including: compromising their financial accounts, marring their credit ratings and history, preventing their ability to get loans, risking fraudulent tax filings, the inclusion of misinformation in their medical record leading to improper and dangerous medical treatment and/or incurring additional costs due to diminishment or loss of insurance coverage, diminishment or loss of employment opportunities, and many other potential hardships. Plaintiffs have already suffered diminished security in their personal affairs and face an expanded and imminent risk of economic harm from identity theft and fraud.

735. For example, Plaintiffs Steven Akins, Samuel Armstrong, Jason Ariciu, Anthony Bell, Bridgett Burk, Terry Fischer, Shelly Forman, Tabielle Holsinger, Tyler King, William Lloyd, Jordan O’Hara, Kimberly Robertson, Cheryl Senko, Tonya Smith, and Charnae Tutt have already experienced

additional security risks such as phishing attempts, increased phone solicitations, incidents of fraud or misuse, efforts by hackers trying to access or log in to their Facebook accounts, Friend requests from trolls or cloned or imposter accounts, and other interference with their Facebook accounts. Plaintiffs Dustin Short and Tonya Smith have been notified that their content and information is available on the dark web.

736. That Plaintiffs may not yet be aware that harm has occurred increases rather than diminishes their risk because they do not know they are at risk and cannot take specific action to prevent a known harm. As such, the remaining Plaintiffs also face security risks and are subjected to a heightened risk of such predatory conduct due to Facebook's failure to secure their personal content, including the sale of their content and information on the dark web and illicit databases. Where Plaintiffs' content and information is available on the dark web, this imposes further uncompensated costs on those individuals. The dark web permits criminals further access to users' content and information that could potentially allow more serious identity theft or fraud involving an individual's other accounts.

737. *Out-of-pocket costs.* Facebook knew that users' content and information was being collected and aggregated in ways that put Plaintiffs at heightened risk of identity theft and fraud, and failed to properly inform users of those risks, such that Plaintiffs could reasonably mitigate those potential harms. Rather, Facebook has placed the burden of mitigating the risk of identity theft and fraud on Plaintiffs. Following the Cambridge Analytica Scandal, Facebook offered no support to users who were concerned about the collection of their content and information. In fact, Facebook is still unable to confirm who has possession of Plaintiffs' content and information.

738. As a result, Plaintiffs have paid for credit monitoring and have spent time and money to protect themselves from the imminent threat of identity theft and fraud. For example, Plaintiff Dustin Short paid for credit monitoring and to remove inquiries from his credit report in the wake of the revelations about the Cambridge Analytica Scandal. Likewise, Plaintiffs Anthony Bell paid for credit monitoring services. Plaintiffs Forman, Herman, Holsinger, King, O'Hara, Senko, Smith, and Tutt use credit and bank account monitoring services from multiple providers. Plaintiff Fischer has frozen her

credit and requested fraud alerts from various credit monitoring agencies.

739. These actions were reasonable in light of the scope of content and information Facebook collected, as well as the ability of third parties, with which Facebook impermissibly shared users' content and information, allowing users' Facebook content and information to be pooled with other data sources and linked to specific Facebook users. As a result, Plaintiffs have incurred out-of-pocket costs as a result of Facebook's harmful conduct, including purchasing credit monitoring or other forms of identity theft protection services.

740. This transfer of costs from Facebook to users and benefits from users to Facebook was deliberate. Facebook engineered APIs that enabled third parties to access users' content and information without adhering to users' privacy settings. Moreover, once this data was in the hands of the third parties, Facebook took no steps to prevent its use in ways that were contrary to users' reasonable expectations of privacy.

741. In failing to mitigate, Facebook avoided costs it should have incurred as a result of its own actions—both out of pocket and loss of user engagement—and transferred those costs to Plaintiffs; warning users would have chilled user engagement as well as potential new users from joining Facebook. It would also have brought scrutiny on the Company, in the form of transaction costs such as regulatory fines, shareholder concerns, possible executive turnover, and a decline in share price. Some of these costs have, of course, materialized. Facebook and Zuckerberg were thus not only able to evade or defer these costs but to continue to accrue value for the Company and to further benefit from the delay due to the time value of money. Facebook, as of yet, still has not publicly disclosed the third parties, including App Developers, which received access to users' content and information.

742. Thus, Facebook has transferred all of the costs imposed by the unauthorized disclosure and publication of users' content and information onto Plaintiffs. Facebook increased mitigation costs by failing to notify users that their content and information had been disclosed and to alert them at the earliest time possible so that users could take steps to protect their identities. In addition, Facebook increased mitigation costs by engaging in acts that furthered both the dissemination of user information and its aggregation, as well as by its failure to audit third parties who received user information to



secure it. For example, Facebook failed to demand and enforce compliance with its policies by its own App Developers, including that user content and information not be sold and that it be deleted if improperly obtained. In failing to mitigate, Facebook avoided costs it would have incurred, both out of pocket and loss of user engagement, and transferred those costs to Plaintiffs.

743. ***Loss of control and value.*** Users also suffered diminished loss of use of their own content and information, property which has value to them.

744. Facebook cannot dispute that users' content and information is property, and Facebook has repeatedly conceded that users own it: "[y]ou own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings."<sup>418</sup> Moreover, the DCMS Report noted that Zuckerberg's testimony to Congress that users should have complete control over their data and that users own all the content they upload and can delete it at will was disingenuous and inaccurate: "the advertising profile that Facebook builds up about users ***cannot be accessed, controlled or deleted*** by those users. It is difficult to reconcile this fact with the assertion that users own all 'the content' they upload."<sup>419</sup>

745. Users' content and information also has value. ***First***, there is transactional value to user content and information. Indeed, Facebook traded use of its own platform to users in exchange for their content and information. Similarly, Facebook traded access to users' content and information with App Developers. Mr. Soltani of the FTC refers to this as "data reciprocity."<sup>420</sup> In exchange for giving App Developers access to users' content and information, App Developers increase user engagement whereby Facebook increases its audience and users generate more content and information—both resulting in greater revenue for Facebook. Facebook engages in an extensive transactional market of data reciprocity with its Business Partners, as set forth above.

---

<sup>418</sup> *Statement of Rights and Responsibilities*, Facebook (June 8, 2012), [www.facebook.com/legal/terms](http://www.facebook.com/legal/terms), [<https://web.archive.org/web/20121205191915/https://www.facebook.com/legal/terms>]; *Promises, promises: Facebook's history with privacy*, Phys.Org (Mar. 30, 2018), <https://phys.org/news/2018-03-facebook-history-privacy.html>.

<sup>419</sup> DCMS Report, *supra* note 28, ¶ 41 (emphasis added).

<sup>420</sup> *Id.* ¶ 103.

746. *Second*, there is economic value to user content and information that can be measured in dollars. Facebook calculates average revenue per user premised upon the content that users share; the current reported average revenue per user was \$34 in 2018.<sup>421</sup> Indeed, the entire foundation of Facebook's financial success is collecting users' content and information and making it available to those who wish to advertise to them. There is a legitimate business model, involving disclosure and true consent, through which user content can be collected and sold. Data brokers exist because of the high value of such information. Advertisers, App Developer, and other third parties pay Facebook billions of dollars because of the access Facebook provides to users' content and information, but Facebook does not disclose its conduct or obtain true consent.

747. There also can be no legitimate dispute that there is a market for users' content and information. One study by content marketing agency Fractl has found that an individual's online identity, including hacked financial accounts, can be sold for \$1200 on the dark web.<sup>422</sup> Facebook logins can be sold for approximately \$5.20 each. These rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other users' content, surely users can sell their own. Moreover, it was recently revealed that Facebook paid certain underage users for their content and information, evidence once again that user content has value.<sup>423</sup> In short, there is economic value to users' data that is greater than zero. The exact number will be a matter for experts to determine.

748. Users were harmed when Facebook took their property. Furthermore, users are harmed because Facebook has taken that property and exerted exclusive control over it. The fact that Facebook will not give users access to their own dossiers and the content and information Facebook has already collected prevents users from selling it. Because Facebook is selling users' content and information,

---

<sup>421</sup> *Facebook Q4 2018 Results*, Facebook (Jan. 30, 2019), [https://s21.q4cdn.com/399680738/files/doc\\_financials/2018/Q4/Q4-2018-Earnings-Presentation.pdf](https://s21.q4cdn.com/399680738/files/doc_financials/2018/Q4/Q4-2018-Earnings-Presentation.pdf).

<sup>422</sup> Maria LaMagna, *The sad truth about how much your Facebook data is worth on the dark web*, MarketWatch (June 6, 2018), <https://www.marketwatch.com/story/spooked-by-the-facebook-privacy-violations-this-is-how-much-your-personal-data-is-worth-on-the-dark-web-2018-03-20>.

<sup>423</sup> Josh Constine, *Facebook pays teens to install VPN that spies on them*, TechCrunch (Jan. 29, 2019), <https://techcrunch.com/2019/01/29/facebook-project-atlas/>.

users cannot. Finally, the first sale of users' content and information diminishes the value of the information, because there is a first seller advantage.

## **VI. PLAINTIFFS COULD NOT HAVE DISCOVERED THEIR CLAIMS UNTIL 2018**

749. Facebook has consistently denied that it is careless about user content and information.

750. Christopher Wylie testified to the U.K. Parliament that in or around July 2014, Facebook's engineers may have assisted Cambridge Analytica with its harvesting of the personal data of millions of Facebook users. Wylie testified that, according to Alexander Kogan, when the size of the transfer caused Facebook's platform to throttle the App—thereby effectively disabling the transfer of data—Cambridge Analytica reached out to Facebook for assistance.<sup>424</sup> Facebook “would have known from that moment about the project, because [Kogan would have] had a conversation with Facebook's engineers.”<sup>425</sup>

751. Even if the *Guardian*'s December 2015 article regarding Cambridge Analytica's use of information about Facebook users had obliged Plaintiffs to conduct further investigation to determine whether they were among the Facebook users whose content and information was disclosed without permission, Plaintiffs would not have been able to uncover the facts underlying their claims.

752. That is because the relevant facts were in the possession of Facebook and Cambridge Analytica, and both refused to disclose them. In the wake of the December 2015 *Guardian* article, Facebook investigated Cambridge Analytica, but never publicly released the results of its investigation and until 2018 did not confirm that Plaintiffs' content and information had been disclosed without their permission.

753. Indeed, Facebook actively concealed the facts.

754. In June 2016, it secured from Kogan and GSR a non-disclosure agreement about their collection of data, obliging them not to disclose the manner in which they obtained and used Plaintiffs'

---

<sup>424</sup> U.K. House of Commons, Digital, Culture, Media and Sport Comm., Testimony of Christopher Wylie (Mar. 27, 2018), at Q1336, <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/fake-news/oral/81022.pdf>.

<sup>425</sup> *Id.*

content and information. In exchange, Facebook waived and released any and all claims against Kogan or GSR concerning the data.

755. Moreover, when Simon Milner, Facebook's Policy Director for the United Kingdom, the Middle East, and Africa, testified to the U.K. Parliament on February 8, 2018, he denied that Cambridge Analytica or any of its associated companies had "Facebook user data," and that, in any case, Facebook had "no insight on" how Cambridge Analytica may have gathered data from users on Facebook.<sup>426</sup>

756. Then, in a February 23, 2018 letter, Cambridge Analytica CEO Alexander Nix falsely told Parliament that "Cambridge Analytica does not gather such data,"<sup>427</sup> and Facebook did not correct or clarify Nix's false statement.

757. Four days later on February 27, 2018, Nix testified before Parliament. When asked whether any of Cambridge Analytica's data came from Facebook, Nix replied, "We do not work with Facebook data and we do not have Facebook data."<sup>428</sup> Nix also claimed that Cambridge Analytica "did not use any personality modelling or 'psychographics' in the election, and that it has no access to Facebook likes."<sup>429</sup> Once again, Facebook did not correct or clarify these false statements.

758. Only in March 2018, with the publication of articles by The Guardian and The New York Times did it become clear that Plaintiffs should inquire into whether they had been injured by Facebook's misconduct. Thereafter, Facebook informed Facebook users that their content and

---

<sup>426</sup> U.K. House of Commons, Digital, Culture, Media and Sport Committee, Testimony of Juniper Downs, et al. (Feb. 8, 2018), at Q447-449, <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake-news/oral/78195.pdf>.

<sup>427</sup> Alexander Nix, Letter from Alexander Nix, Chief Executive, Cambridge Analytica to Damian Collins, Chair of the Committee (Feb. 23, 2018), <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/fake-news/written/79053.pdf>.

<sup>428</sup> U.K. House of Commons, Digital, Culture, Media and Sport Committee, Testimony of Alexander Nix (June 6, 2018), at Q3288, <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/fake-news/oral/84838.html>.

<sup>429</sup> Letter from Alexander Nix, *supra* note 427.

information had been released to Cambridge Analytica.

## VII. CHOICE OF LAW

759. Facebook’s Terms of Service (formerly known as the “Statement of Rights and Responsibilities”) contain (and have always contained) a forum selection provision that mandates the resolution of any claim—arising either out of the Terms of Service or a person’s use of Facebook—exclusively in the U.S. District Court for the Northern District of California and provides that users submit to the personal jurisdiction of those courts to litigate those claims.

760. In addition, the Terms of Service contain (and have contained since at least April 26, 2011) a California choice-of-law provision.<sup>430</sup> The provision ensures that California law applies to “any claim that might arise between” a user and Facebook.<sup>431</sup>

761. This Court has consistently enforced the California choice of law provision.

## VIII. CLASS ACTION ALLEGATIONS

762. Plaintiffs incorporate by reference all the allegations of this Complaint as though fully set forth herein.

763. Plaintiffs bring this action on behalf of themselves and all others similarly situated pursuant to Rule 23(b)(2) and 23(b)(3) of the Federal Rules of Civil Procedure.

764. Plaintiffs seek to represent the following Classes:

A. **The Class**, which is defined as all Facebook users in the United States and in the United Kingdom whose content and information, generated when they were eighteen years of age or older, was collected by Facebook and published and/or disclosed to third parties without their authorization or consent from January 1, 2007 to the present. The Class contains the following Subclasses:

i. **The Alabama Subclass**, which is defined as all members of the Class

---

<sup>430</sup> See, e.g., *Statement of Rights and Responsibilities*, Facebook (Apr. 26, 2011)

<http://www.facebook.com/legal/terms>

[<https://web.archive.org/web/20120529141325/http://www.facebook.com/legal/terms>] (“The laws of the State of California will govern this Statement, as well as any claim that might arise between you and us, without regard to conflict of law provisions).

<sup>431</sup> *Id.*

who resided in Alabama at the time the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

ii. **The Arizona Subclass**, which is defined as all members of the Class who resided in Arizona at the time the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

iii. **The Colorado Subclass**, which is defined as all members of the Class who resided in Colorado at the time the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

iv. **The Delaware Subclass**, which is defined as all members of the Class who resided in Delaware at the time the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

v. **The Florida Subclass**, which is defined as all members of the Class who resided in Florida at the time the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

vi. **The Georgia Subclass**, which is defined as all members of the Class who resided in Georgia at the time the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

vii. **The Idaho Subclass**, which is defined as all members of the Class who resided in Idaho at the time the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

viii. **The Illinois Subclass**, which is defined as all members of the Class who resided in Illinois at the time the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

ix. **The Indiana Subclass**, which is defined as all members of the Class who resided in Indiana at the time the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

x. **The Iowa Subclass**, which is defined as all members of the Class who resided in Iowa at the time the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

xi. **The Kansas Subclass**, which is defined as all members of the Class who resided in Kansas at the time the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

xii. **The Maryland Subclass**, which is defined as all members of the Class who resided in Maryland at the time the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

xiii. **The Michigan Subclass**, which is defined as all members of the Class who resided in Michigan at the time the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

xiv. **The Missouri Subclass**, which is defined as all members of the Class who resided in Missouri at the time the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or



consent.

xv. **The New Jersey Subclass**, which is defined as all members of the Class who resided in New Jersey at the time the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

xvi. **The New York Subclass**, which is defined as all members of the Class who resided in New York at the time that the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

xvii. **The Ohio Subclass**, which is defined as all members of the Class who resided in Ohio at the time the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

xviii. **The Oklahoma Subclass**, which is defined as all members of the Class who resided in Oklahoma at the time the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

xix. **The Pennsylvania Subclass**, which is defined as all members of the Class who resided in Pennsylvania at the time the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

xx. **The Tennessee Subclass**, which is defined as all members of the Class who resided in Tennessee at the time the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

xxi. **The Texas Subclass**, which is defined as all members of the Class who resided in Texas at the time the content and information they generated was collected by

Facebook and published and/or disclosed to third parties without their authorization or consent.

xxii. **The Virginia Subclass**, which is defined as all members of the Class who resided in Virginia at the time the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

xxiii. **The Washington Subclass**, which is defined as all members of the Class who resided in Washington at the time that the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

xxiv. **The West Virginia Subclass**, which is defined as all members of the Class who resided in West Virginia at the time that the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

xxv. **The Wisconsin Subclass**, which is defined as all members of the Class who resided in Wisconsin at the time the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

B. **The Minor Class**, which is defined as all Facebook users in the United States and in the United Kingdom whose content and information, generated when they were less than eighteen years, was collected by Facebook and published and/or disclosed to third parties without their authorization or consent from January 1, 2007 to the present.

765. As used in this Complaint, “Class Period” refers to the period January 1, 2007 to the present.

766. Excluded from the Classes are Defendants, their current employees, coconspirators, officers, directors, legal representatives, heirs, successors and wholly or partly owned subsidiaries or affiliated companies; the undersigned counsel for Plaintiffs and their employees; and the judge and court

staff to whom this case is assigned. Plaintiffs reserve the right to amend the definitions of the Classes if discovery or further investigation reveals that the Classes should be expanded or otherwise modified.

767. The Classes satisfy the prerequisites of Federal Rule of Civil Procedure 23(a) and the requirements of Rule 23(b)(3).

768. **Numerosity and Ascertainability:** Plaintiffs do not know the exact size of the Classes or the identities of the Class Members,<sup>432</sup> since such information is the exclusive control of Defendants. Nevertheless, the Class encompasses millions of individuals, and the Minor Class encompasses—at the least—thousands of individuals, dispersed throughout the United States and the United Kingdom. Each of the Subclasses also contains at least thousands, and almost certainly more, individuals. The number of members in each of the Classes is so numerous that joinder of all members in any of the Classes is impracticable. The names, addresses, and phone numbers of Class Members are identifiable through documents maintained by Defendants.

769. **Commonality and Predominance:** The action involves common questions of law and fact, which predominate over any question solely affecting individual Class Members. These common questions for Class Members' priority claims include:

- i. Whether Facebook gave Plaintiffs and Class Members effective notice of its program to collect their content and information;
- ii. Whether Defendants obtained authorization or consent from Plaintiffs and Class Members to collect their content and information;
- iii. Whether Defendants improperly collected Plaintiffs' and Class Members' content and information;
- iv. Whether Facebook represented that Plaintiffs' and Class Members' content and information would be protected from disclosure absent their consent;
- v. Whether Facebook owes any duty to Plaintiffs and Class Members with respect to maintaining, securing, or deleting their content and information;
- vi. To what degree Facebook has the right to use content and information pertaining to Plaintiffs and Class Members;
- vii. Whether Facebook owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, safeguarding, and/or obtaining their content and information;

---

<sup>432</sup> Here and elsewhere in the complaint, the term "Class Members" refers collectively to Members of all Classes.

- viii. Whether Facebook breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, safeguarding, and/or obtaining their content and information;
- ix. Whether the egregious breach of privacy and trust alleged in the Complaint was foreseeable by Facebook;
- x. Whether Facebook intentionally exposed Plaintiffs' and Class Members' content and information to Cambridge Analytica;
- xi. Whether Defendants violated the Stored Communications Act;
- xii. Whether Defendants violated Plaintiffs' and Class Members' privacy rights;
- xiii. Whether Facebook's conduct was an unlawful or unfair business practice under Cal. Bus. & Prof. Code §§ 17200 *et seq.* (West 2018);
- xiv. Whether Facebook is a "video tape service provider" under 18 U.S.C. § 2710;
- xv. Whether Facebook is a provider of electronic communication service to the public pursuant to 18 U.S.C. §§ 2702(a)(1) and 2510(15);
- xvi. Whether Facebook maintains a facility through which an electronic communication service is provided, pursuant to 18 U.S.C. § 2701(a);
- xvii. Whether Facebook is a provider of a remote computing service to the public, pursuant to 18 U.S.C. §§ 2702(a)(2) and 2711(2);
- xviii. Whether "Facebook content," a term defined below, constitutes electronic communications under 18 U.S.C. § 2510(12);
- xix. Whether Plaintiffs and Class Members are "users" or "subscribers" of Facebook's remote computing service, as the term "user" is defined and/or used in 18 U.S.C. § 2510(5) and (13);
- xx. Whether Plaintiffs and Class Members are "aggrieved person[s]" as that term is defined in 18 U.S.C. § 2510(11);
- xxi. Whether Plaintiffs' and the Class Members' use of Facebook's messaging systems and transfers of content and information to Facebook constitute electronic communications, pursuant to 18 U.S.C. § 2501(12);
- xxii. Whether Plaintiffs' and Class Members' electronic communications were in electronic storage, pursuant to 18 U.S.C. § 2501(17);
- xxiii. Whether Facebook knowingly divulged the contents of Plaintiffs and the Class Members' electronic communications while they were in electronic storage to unauthorized parties in violation of 18 U.S.C. § 2702(a)(1);
- xxiv. Whether Facebook knowingly divulged the contents of Plaintiffs' and Class Members' electronic communications that were carried or maintained on Facebook's remote computing service to unauthorized parties in violation of 18 U.S.C. § 2702(a)(2);
- xxv. Whether Plaintiffs and Class Members have suffered an injury as a result of Facebook's violations of the Stored Communications Act;

- xxvi. Whether Facebook profited from its acts that violate the Stored Communications Act;
- xxvii. Whether Facebook's violation of the Stored Communications Act was committed willfully and intentionally;
- xxviii. Whether Plaintiffs and Class Members are "consumers" as that term is defined in 18 U.S.C. § 2710;
- xxix. Whether Plaintiffs' and Class Members' data that Facebook possessed contained "personally identifiable information" as that term is defined in 18 U.S.C. § 2710;
- xxx. Whether Facebook knowingly allowed third parties access to Plaintiffs' and Class Members' personally identifiable information in violation of the Video Privacy Protection Act;
- xxxi. Whether Plaintiffs and the other Class Members are "aggrieved person[s]" as that term is defined by 18 U.S.C. § 2710;
- xxxii. Whether Facebook suppressed facts which it was bound to disclose to Plaintiffs and Class Members about the privacy of their user content and information;
- xxxiii. Whether Facebook gave information of facts that were likely to mislead Plaintiffs and Class Members about the privacy of their user content and information;
- xxxiv. Whether Facebook failed to disclose known risks that third-party App Developers would sell or disperse Plaintiffs' and Class Members' user content and information without their consent;
- xxxv. Whether Facebook violated the terms of an October 2012 FTC settlement by continuing to allow App Developers access to Plaintiffs and Class Members' user content and information without their consent;
- xxxvi. Whether Facebook failed to audit whether and how Plaintiffs' and Class Members' user content and information was provided to third parties;
- xxxvii. Whether Facebook failed to disclose to Plaintiffs and Class Members the risks that each faced from the disclosure of their user content and information;
- xxxviii. Whether Facebook failed to inform Plaintiffs and Class Members that their user content and information was insecure once it was shared with App Developers or other third parties;
- xxxix. Whether Facebook knew that Plaintiffs' and Class Members' user content and information was not secure;
- xl. Whether Facebook ignored warnings that audits were necessary to secure Plaintiffs' and Class Members' user content and information;
- xli. Whether Facebook intentionally failed to secure Plaintiffs' and Class Members' information and content;
- xlii. Whether Facebook had a duty to inform Plaintiffs and Class Members that Facebook had become aware that it had failed to secure Plaintiffs' and Class Members' user content and information;

- xliii. Whether Facebook intentionally concealed that Plaintiffs' and Class Members' user content and information was insecure;
- xliv. Whether Facebook failed to disclose to Plaintiffs and Class Members that it had not secured their user content and information;
- xliv. Whether Facebook failed to disclose to Plaintiffs and Class Members the risks that each faced from Facebook's failure to secure user content and information;
- xlvi. Whether Facebook intended to deceive Plaintiffs and Class Members about the security of their user content and information;
- xlvii. Whether Plaintiffs and Class Members were damaged as a result of Facebook's deceit;
- xlviii. Whether Facebook misled Plaintiffs and Class Members to believe that Facebook was protecting users' privacy;
- xliv. Whether Facebook failed to disclose to or deceived Plaintiffs and Class Members that Facebook was sharing their users' content and information with third parties;
  - i. Whether Facebook failed to disclose that, notwithstanding privacy settings that purported to provide Plaintiffs and Class Members with control over their user content and information, Facebook allowed third parties to harvest and store Plaintiffs' and Class Members' personal information;
  - ii. Whether Facebook had a duty to provide accurate information to Plaintiffs and Class Members about how their user content and information was disclosed to third parties;
  - iii. Whether Facebook encouraged Plaintiffs and Class Members to share content and information by assuring them that Facebook would respect their choices concerning privacy;
  - liii. Whether Facebook intentionally concealed how it disclosed Plaintiffs' and Class Members' user content and information and whether it did so to create a false sense of security and privacy for Plaintiffs and Class Members;
  - liv. Whether Facebook intentionally concealed how it disclosed Plaintiffs' and Class Members' user content and information in order to increase its revenues;
  - lv. Whether Plaintiffs and Class Members were damaged because their user content and information were disclosed to third party device makers and other Business Partners without their consent;
  - lvi. Whether Facebook failed to disclose to Plaintiffs and Class Members how their user content and information was being collected, shared and aggregated to develop digital profiles or dossiers of each user;
  - lvii. Whether Facebook had a duty to disclose the full extent to which it allowed Plaintiffs and Class Members to be targeted by advertisers and marketers;
  - lviii. Whether Facebook knew that advertisers and marketers were targeting Plaintiffs and Class Members with messages based upon Facebook-derived content and information;

- lix. Whether Facebook failed to disclose to Plaintiffs and Class Members that advertisers were combining data from data brokers with Facebook-derived content and information to target them with advertisements and psychographic marketing, as well as building digital dossiers of users;
- lx. Whether Facebook intended to deceive Plaintiffs and Class Members about their vulnerability to targeted advertisements;
- lxi. Whether Facebook has been unjustly enriched by virtue of its deceit concerning user content and information disclosure and aggregation for advertisers;
- lxii. Whether Facebook must disgorge its profits made from the use of Plaintiffs' and Class Members' content and information;
- lxiii. Whether Plaintiffs and Class Members had a reasonable expectation that their user content and information they entrusted to Facebook would be protected and secured against access by unauthorized parties and would not be disclosed to or obtained by unauthorized parties, or disclosed or obtained for any improper purpose;
- lxiv. Whether Facebook intentionally intruded upon the private affairs and concerns of Plaintiffs and Class Members;
- lxv. Whether Facebook intrusions upon the private affairs and concerns of Plaintiffs and Class Members were substantial, and would be highly offensive to a reasonable person;
- lxvi. Whether Plaintiffs and Class Members did not consent to Facebook's intrusions upon their private affairs and concerns;
- lxvii. Whether Plaintiffs and Class Members suffered actual and concrete injury as a result of Facebook's intrusions upon Plaintiffs' and Class Members' private affairs and concerns;
- lxviii. Whether Plaintiffs and Class Members are entitled to relief for their injuries that resulted from Facebook's intrusion upon Plaintiffs' and Class Members' private affairs and concerns;
- lxix. Whether Facebook published private content and information of Plaintiffs and Class Members to unauthorized parties and failed to take reasonable steps to prevent further dissemination of this content and information;
- lxx. Whether Facebook's publication of Plaintiffs' and Class Members' user content and information would be highly offensive to a reasonable person;
- lxxi. Whether Plaintiffs' and Class Members' content and information was private and not of legitimate public concern or substantially connected to a matter of legitimate public concern;
- lxxii. Whether Plaintiffs and Class Members suffered injury as a result of Facebook's publication of Plaintiffs' and Class Members' content and information;
- lxxiii. Whether Facebook and Plaintiffs and Class Members mutually assented to, and therefore were bound by the version of Facebook's Statement of Rights and Responsibilities or later, the Terms of Service, (collectively, the "Contracts") that was



- operative at the time each of the Plaintiffs or a member of the Classes joined Facebook;
- lxxiv. Whether the Contracts required Facebook to protect the content and information of its users, including Plaintiffs and Class Members;
  - lxxv. Whether the Contracts failed to form or obtain consent to share Plaintiffs' and Class Members' user content and information with advertisers and other third parties and/or failed to disclose that such information would be shared if users' Friends entered into an agreement which permitted third parties to collect their Friends' information;
  - lxxvi. Whether Facebook made it unreasonably difficult for Plaintiffs and Class Members to access the provisions of the Privacy and Data Use Policies, and particularly the provision of the Privacy and Data Use Policies disclosing Friend-of-user sharing;
  - lxxvii. Whether Facebook made it unreasonably difficult for Plaintiffs and Class Members to understand which privacy settings governed how third-party applications and advertisers could access users' content and information via Friend-of user sharing;
  - lxxviii. Whether Facebook failed to adequately explain to Plaintiffs and Class Members that a user's "Privacy Settings" were ineffective in controlling whether users' content and information was shared via Friend-of-user sharing;
  - lxxix. Whether, contrary to the Contracts, Facebook knowingly allowed Doe Defendants to sell the content and information regarding Plaintiffs and Class Members that they had collected via applications that used the Facebook platform;
  - lxxx. Whether Plaintiffs' and Class Members' content and information has value;
  - lxxxi. Whether Facebook breached the Contracts;
  - lxxxii. Whether Facebook owed a duty to Plaintiffs and Class Members to exercise reasonable care in the obtaining, using, and protecting of their content and information, arising from the sensitivity of their content and information and the expectation that their content and information was not going to be shared with third parties without their consent;
  - lxxxiii. Whether Facebook owed a duty to timely disclose to Plaintiffs and Class Members that Facebook had allowed their content and information to be accessed by third parties;
  - lxxxiv. Whether Facebook knew that the content and information of Plaintiffs and Class Members had value;
  - lxxxv. Whether Facebook failed to take reasonable steps to prevent harm to Plaintiffs from known threats to the security to Plaintiffs' and Class Members' user content and information;
  - lxxxvi. Whether Facebook breached the duties of care it owed to Plaintiffs and Class Members;
  - lxxxvii. Whether Plaintiffs and Class Members were foreseeable victims of Facebook's breach of its duties;

- lxxxviii. Whether, as a result of Facebook's negligent failure to safeguard Plaintiffs' and Class Members' content and information, Plaintiffs and Class Members have suffered injuries;
- lxxxix. Whether the injuries to Plaintiffs and Class Members were proximate, reasonably foreseeable results of Facebook's breaches of its duties of care;
  - xc. Whether it is reasonable for Plaintiffs and Class Members to obtain identity protection and/or credit monitoring services in light of Facebook's breach of its duties of care;
  - xc. Whether public policy would void any purported waiver of liability to which Facebook may claim;
  - xcii. Whether Facebook's conduct constitutes gross negligence;
  - xciii. Whether Plaintiffs and Class Members have a privacy right to their user content and information under Art. I, Sec. 1 of the California Constitution;
  - xciv. Whether Facebook violated Plaintiffs' and Class Members' constitutionally-protected right to privacy;
  - xcv. Whether Facebook violated the common law prohibition on the use of a person's name or likeness to its own advantage;
  - xcvi. Whether Facebook failed to obtain consent from Plaintiffs and Class Members to use their likenesses;
  - xcvii. Whether Plaintiffs and Class Members received no compensation in return for Facebook's use of their likenesses;
  - xcviii. Whether Plaintiffs and Class Members were harmed by Facebook's improper use of their likenesses;
  - xcix. Whether Facebook knowingly obtained benefits from Plaintiffs and Class Members under circumstances such that it would be inequitable and unjust for Facebook to retain them;
    - c. Whether Facebook is a "person" as defined by Ala. Code § 8-19-3(5);
    - ci. Whether Facebook's products and services are "goods" and "services" as defined by Ala. Code § 8-19-3(3), (7);
    - cii. Whether Facebook advertised, offered, or sold goods or services in Alabama and engaged in trade or commerce directly or indirectly affecting the people of Alabama as defined by Ala. Code § 8-19-3(8);
    - ciii. Whether Facebook engaged in unconscionable, false, misleading or deceptive practices in connection with its business, commerce and trade practices in violation of Ala. Code § 8-19-5(27);
    - civ. Whether Facebook acted intentionally, knowingly, and maliciously to violate Alabama's Deceptive Trade Practices Act, and recklessly disregarded the Alabama Plaintiff's and the Alabama Subclass members' rights;
    - cv. Whether Facebook is a "person" as defined by Colo. Rev. Stat. Ann. § 6-1-102(6);

- cvi. Whether the Colorado Plaintiff and Colorado Subclass members, as well as the general public, are actual or potential consumers of the services offered by Facebook to actual consumers;
- cvii. Whether Facebook engaged in deceptive trade practices in the course of its business, in violation of Colo. Rev. Stat. Ann. § 6-1-105(1)(u);
- cviii. Whether Facebook engaged in deceptive trade practices in the course of its business, in violation of Colo. Rev. Stat. Ann. § 6-1-105(3) by engaging unfair trade practices actionable at common law or under other statutes of Colorado;
- cix. Whether Facebook intended to mislead the Colorado Plaintiff and the Colorado Subclass members and induce them to rely on its misrepresentations and omissions;
- cx. Whether Facebook acted fraudulently, willfully, knowingly, or intentionally to violate Colorado’s Consumer Protection Act, and with recklessly disregarded the Colorado Plaintiff’s and the Colorado Subclass members’ rights;
- cxi. Whether Facebook is a “person” as defined by 815 Ill. Comp. Stat. Ann. § 505/1(c);
- cxii. Whether the Illinois Plaintiffs and the Illinois Subclass members are “consumer[s]” as defined by 815 Ill. Comp. Stat. Ann. § 505/1(e);
- cxiii. Whether Facebook’s conduct as described herein was in the conduct of “trade” or “commerce” as defined by 815 Ill. Comp. Stat. Ann. § 505/1(f);
- cxiv. Whether Facebook’s deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. Ann. § 505/2;
- cxv. Whether Facebook acted intentionally, knowingly, and maliciously to violate Illinois’s Consumer Fraud and Deceptive Business Practices Act, and recklessly disregarded the Illinois Plaintiffs and the Illinois Subclass members’ rights;
- cxvi. Whether Facebook is a “person” as defined by Iowa Code Ann. § 714H.2(7);
- cxvii. Whether the Iowa Plaintiff and the Iowa Subclass members are “consumer[s]” as defined by Iowa Code § 714H.2(3);
- cxviii. Whether Facebook’s conduct described herein related to or was in connection with the “sale” or “advertisement” of “merchandise” as defined by Iowa Code Ann. § 714H.2(2), (6), (8);
- cxix. Whether Facebook engaged in unfair, deceptive, and unconscionable trade practices, in violation of the Iowa Private Right of Action for Consumer Frauds Act, as described throughout and herein;
- cxx. Whether Facebook acted intentionally, knowingly, and maliciously to violate Iowa’s Private Right of Action for Consumer Frauds Act, and recklessly disregarded the Iowa Plaintiff and the Iowa Subclass members’ rights;
- cxxi. Whether the Kansas Plaintiff and the Kansas Subclass members are “consumer[s]” as defined by Kan. Stat. Ann. § 50-624(b);
- cxxii. Whether the acts and practices described herein are “consumer transaction[s],” as defined by Kan. Stat. Ann. § 50-624(c);

- cxxiii. Whether Facebook is a “supplier” as defined by Kan. Stat. Ann. § 50-624(l);
- cxxiv. Whether Facebook advertised, offered, or sold goods or services in Kansas and engaged in trade or commerce directly or indirectly affecting the people of Kansas;
- cxxv. Whether the Kansas Plaintiff and the Kansas Subclass members had unequal bargaining power with respect to their use of Facebook’s services because of Facebook’s omissions and misrepresentations;
- cxxvi. Whether Facebook acted intentionally, knowingly, and maliciously to violate Kansas’s Consumer Protection Act, and recklessly disregarded the Kansas Plaintiff and the Kansas Subclass members’ rights;
- cxxvii. Whether Facebook, the Michigan Plaintiff, and Michigan Subclass members are “person[s]” as defined by Mich. Comp. Laws Ann. § 445.902(1)(d);
- cxxviii. Whether Facebook advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.902(1)(g);
- cxxix. Whether Facebook engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1);
- cccc. Whether Facebook engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of goods or services, in violation of N.Y. Gen. Bus. Law § 349, as described herein;
- ccxxxi. Whether Facebook acted intentionally, knowingly, and maliciously to violate New York’s General Business Law, and recklessly disregarded the New York Plaintiff’s and the New York Subclass members’ rights;
- ccxxxi. Whether Facebook is a “[p]erson,” as defined by Wash. Rev. Code Ann. § 19.86.010(1);
- ccxxxi. Whether Facebook advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010(2);
- ccxxxi. Whether Facebook engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, as described herein;
- ccxxxi. Whether Facebook acted intentionally, knowingly, and maliciously to violate Washington’s Consumer Protection Act, and recklessly disregarded the Washington Plaintiff’s and Washington Subclass members’ rights;
- ccxxxi. Whether the West Virginia Subclass members are “[c]onsumer[s],” as defined by W. Va. Code Ann. § 46A-6-102(2);
- ccxxxi. Whether Facebook engaged in “consumer transaction[s],” as defined by W. Va. Code Ann. § 46A-6-102(2);

- xxxxviii. Whether Facebook advertised, offered, or sold goods or services in West Virginia and engaged in trade or commerce directly or indirectly affecting the people of West Virginia, as defined by W. Va. Code Ann. § 46A-6-102(6);
- xxxix. Whether Facebook's unfair and deceptive acts and practices violated W. Va. Code Ann. § 46A-6-102(7);
- cxl. Whether Facebook's unfair and deceptive acts and practices were unreasonable when weighed against the need to develop or preserve business, and were injurious to the public interest, under W. Va. Code Ann. § 46A-6-101;
- cxli. Whether Facebook's acts and practices were "[u]nfair" under W. Va. Code Ann. § 46A-6-104 because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition;
- cxlii. Whether Facebook's acts and practices were "deceptive" under W. Va. Code Ann. § 46A-6-104;
- cxliii. Whether Facebook's omissions were legally presumed to be equivalent to active misrepresentations because Facebook intentionally prevented the West Virginia Subclass members from discovering the truth regarding Facebook's use, sale, disclosure and abuse of private user data;
- cxliv. Whether Facebook acted intentionally, knowingly, and maliciously to violate West Virginia's Consumer Credit and Protection Act, and recklessly disregarded the West Virginia Subclass members' rights;
- cxlv. Whether Facebook's deceptive trade practices significantly impact the public;
- cxlvi. Whether Facebook's representations and omissions were material because they were likely to deceive reasonable consumers;
- cxlvii. Whether Facebook intended that the Alabama, Colorado, Illinois, Iowa, Kansas, Michigan, New York, Washington, and the various Subclass members would rely on its misrepresentations, omissions, and other unlawful conduct;
- cxlviii. Whether, as a direct and proximate result of Facebook's unfair and deceptive acts and practices, Alabama, Colorado, Illinois, Iowa, Kansas, Michigan, New York, Washington, and the various Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages;
- cxlix. Whether the Alabama, Colorado, Illinois, Iowa, Kansas, Michigan, New York, Washington, and the various Subclass members have suffered injuries in fact and lost money or property due to Facebook's business acts or practices;
- cl. Whether Plaintiffs and the Classes are entitled to equitable relief, including, but not limited to, injunctive relief, restitution, and disgorgement; and
- cli. Whether Plaintiffs and the Classes are entitled to actual, statutory, or other forms of damages, and other monetary relief.

770. Defendants engaged in a common course of conduct giving rise to the legal rights sought

to be enforced by this action and similar or identical questions of statutory and common law, as well as similar or identical injuries, are involved. Individual questions, if any, pale in comparison to the numerous common questions that predominate in this action.

771. **Typicality:** Plaintiffs' claims are typical of the other Class Members' claims because all Class Members were comparably injured through Defendants' substantially uniform misconduct as described above. The Plaintiffs representing the Classes are advancing the same claims and legal theories on behalf of themselves and all other members of the Classes that they represent, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and Class Members arise from the same operative facts and are based on the same legal theories.

772. **Adequacy:** Plaintiffs are adequate Class representatives because their interests do not conflict with the interests of the other members of the Classes they seek to represent; Plaintiffs have retained counsel competent and experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously. The Classes' interest will be fairly and adequately protected by Plaintiffs and their counsel.

773. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other detriment suffered by Plaintiffs and the other class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be virtually impossible for the Class Members to individually seek redress for Defendants' wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

774. Class certification under Rule 23(b)(2) is also warranted for purposes of injunctive and declaratory relief because Defendants have acted or refused to act on grounds generally applicable to the Classes, so that final injunctive and declaratory relief are appropriate with respect to each Class as a



whole.

## IX. CAUSES OF ACTION

775. Pursuant to 28 U.S.C. § 1407(a), this Complaint consolidates claims of all plaintiffs in this multidistrict litigation and proposes priority briefing for certain claims. In the event that Defendants seek to challenge claims asserted herein via motion pursuant to Rule 12, Plaintiffs propose that twelve of the claims asserted herein be briefed in priority. Those claims are set forth herein as Part A.

### A. Prioritized Claims

Claim I. **Violation of the Stored Communications Act (“SCA”),  
18 U.S.C. §§ 2701 *et seq.*  
(Against Prioritized Defendants Facebook and Doe Defendants;  
Non-Prioritized Defendant Kogan)  
On Behalf of All Plaintiffs and All Classes**

776. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

777. The Stored Communications Act (“SCA”) allows a private right of action against anyone who “(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system.” *See* 18 U.S.C. § 2701(a); see also 18 U.S.C. § 2707(a) (cause of action).

778. The Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.*, defines an “electronic communication” as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.” 18 U.S.C. § 2510(12). The SCA incorporates this definition of “electronic communication.”

779. To create the information transferred to Facebook such as all posts, private messages, and similar communication (collectively “Facebook content”), Facebook users transmit writing, images, or other data via the Internet from their computers or mobile devices to Facebook’s servers. This Facebook content, therefore, constitutes electronic communications for purposes of the SCA.



780. The SCA distinguishes between two types of electronic storage. The first is defined as “any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof.” 18 U.S.C. § 2510(17)(A). The second type is defined as “any storage of such communication by an electronic communication for purposes of backup protection of such communication.” 18 U.S.C. § 2510(17)(B). Because Facebook saves and archives Facebook content indefinitely, Facebook content is stored in electronic storage for purposes of the SCA.

781. Facebook allows users to select privacy settings for their Facebook content. Access can be limited to a user’s Facebook Friends, to particular groups or individuals, or to just the particular Facebook user. When users make Facebook content inaccessible to the general public, the information is considered private for purposes of the SCA.

782. As set forth herein, Plaintiffs did not authorize Defendants to share their content and information with third party Apps, including Whitelisted Apps, or with Facebook’s Business Partners such as device makers in violation of users’ personal privacy settings.

783. Plaintiffs are subscribers or customers of Facebook’s remote computing service, pursuant to 18 U.S.C. § 2702(a)(2). By virtue of Facebook’s conduct in providing the ability to send or receive wire or electronic communications, Facebook is an electronic communication service within the meaning of the SCA. Plaintiffs are users of Facebook’s electronic communication service, pursuant to 18 U.S.C. § 2510(13).

784. Plaintiffs are subscribers and persons aggrieved by violations of the SCA, pursuant to 18 U.S.C. §§ 2707(a) and 2510(11).

785. By virtue of Defendants’ conduct in providing computer storage and processing services by means of an electronic communications system, Facebook is a remote computer service within the meaning of the SCA.

786. Facebook is a provider of an electronic communication service to the public, pursuant to 18 U.S.C. §§ 2702(a)(1) and 2510(15).

787. Facebook maintains a facility through which an electronic communication service is provided, pursuant to 18 U.S.C. § 2701(a).

788. Facebook is a provider of a remote computing service to the public, pursuant to 18 U.S.C. §§ 2702(a)(2) and 2711(2).

789. Facebook and Doe Defendants are persons within the meaning of the SCA, pursuant to 18 U.S.C. § 2510(6).

790. Facebook and Doe Defendants are persons or entities within the meaning of the SCA, pursuant to 18 U.S.C. § 2707(a).

791. Plaintiffs' use of Facebook's messaging systems and transfers of content and information to Facebook constitute electronic communications, pursuant to 18 U.S.C. § 2501(12).

792. Plaintiffs' electronic communications were in electronic storage, pursuant to 18 U.S.C. § 2501(17).

793. Doe Defendants and Non-Prioritized Defendant Kogan violated the SCA by intentionally accessing without authorization or exceeding an authorization to access Facebook's facility through which an electronic communication service is provided, thereby obtaining access to Plaintiffs' electronic communications while they were in electronic storage, pursuant to 18 U.S.C. § 2701(a).

794. Facebook violated the SCA by knowingly divulging the contents, including content and information, of Plaintiffs' electronic communications while they were in electronic storage to unauthorized parties, including but not limited to Defendant Kogan, Cambridge Analytica, Doe Defendants, and Facebook's Business Partners and Apps, including Whitelisted Apps, pursuant to 18 U.S.C. § 2702(a)(1).

795. Facebook violated the SCA by knowingly divulging the contents, including content and information, of Plaintiffs' electronic communications that were carried or maintained on Facebook's remote computing service to unauthorized parties, including but not limited to Defendant Kogan, Cambridge Analytica, Doe Defendants, Apps and Facebook's Business Partners, pursuant to 18 U.S.C. § 2702(a)(2).

796. As detailed herein, the contents of Plaintiffs' electronic communications that Facebook divulged to unauthorized parties were non-public, and Plaintiffs reasonably believed that the contents of these communications would be protected against publication to unauthorized parties. In particular, the

contents of many of Plaintiffs' electronic communications through Facebook, including photos and videos, were configured to be non-public either at the time of posting or through Facebook's Privacy Settings. But that content was delivered by Facebook to third parties without identifying privacy metadata so that those limitations could not have been honored by third parties.

797. Similarly, the contents, of Plaintiffs' electronic communications through Facebook Messenger and/or Facebook instant messaging were non-public due to the inherently private and non-public nature of instant messaging communication platforms.

798. Facebook knowingly divulged the contents of Plaintiffs' electronic communications both directly to unauthorized parties including Defendant Kogan and Business Partners as well as indirectly to unauthorized parties including Cambridge Analytica and data brokers. The subsequent disclosure of user information by Apps and Business Partners to additional unauthorized parties was reasonably foreseeable, and Facebook knew or should have known about this subsequent disclosure. Facebook also failed to effectively audit, limit, or control Apps or Business Partners accessing user information so as to prevent the subsequent disclosure of user information. Further, Facebook directly profited from the subsequent disclosure of user information, through advertisements placed by unauthorized parties that received user information from Apps or Business Partners, including Cambridge Analytica.

799. As detailed herein, Plaintiffs were not aware of and did not consent to the disclosure of the contents, including content and information, of their electronic communications to unauthorized parties, including Apps used by their Facebook Friends such as the This Is Your Digital Life App and Facebook's Business Partners.

800. Users of Apps, including the This Is Your Digital Life App, and Apps generally, were not aware of and did not consent to the disclosure of the contents, including content and information, of the electronic communications of their Friends or the Friends of their Friends to unauthorized parties, including Cambridge Analytica, Business Partners, other advertisers, and data brokers. In particular, these App users did not consent to the disclosure of the contents, including content and information, of the electronic communications of their Friends or the Friends of their Friends beyond the App—either

with respect to the disclosure of this information by the App or App Developer to unauthorized parties or with respect to the use of this information for purposes beyond limited use by the App itself.

801. As a result of Defendants' violations of the SCA, Plaintiffs have suffered injury, including but not limited to the invasion of Plaintiffs' privacy rights.

802. Defendants profited through their violations of the SCA, and Plaintiffs suffered actual damages, as detailed herein, as a result of these violations, pursuant to 18 U.S.C. § 2707(c).

803. Plaintiffs are entitled to actual damages, disgorgement of profits made by Defendants as a result of their violations of the SCA, and statutory damages, in an amount not less than \$1,000 per Plaintiff.

804. Plaintiffs are also entitled to preliminary and other equitable or declaratory relief as may be appropriate, as well as reasonable attorneys' fees and litigation costs, pursuant to 18 U.S.C. § 2707(b).

805. Defendants' violations of the SCA were committed willfully and intentionally, and therefore Plaintiffs also seek punitive damages pursuant to 18 U.S.C. § 2707(c).

**Claim II. Violation of Video Privacy Protection Act, 18 U.S.C. § 2710  
(Against Prioritized Defendants Facebook and Doe Defendants;  
Non-Prioritized Defendant Kogan)  
On Behalf of All Plaintiffs and All Classes**

806. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

807. Plaintiffs assert this Claim individually and on behalf of the Class and Minor Class (for purposes of this Claim, "Plaintiffs").

808. The VPPA provides that "a video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer shall be liable to the aggrieved person for the relief provided in subsection (d)." 18 U.S. Code § 2710 (b)(1). Facebook violated this statute by knowingly disclosing personally identifiable information to third parties—including Apps used by Facebook Friends of Plaintiffs such as the This Is Your Digital Life App, Business Partners, Whitelisted Apps, and advertisers—without informed, written consent and in violation of Plaintiffs'

privacy settings.

809. Facebook is a “video tape service provider” under 18 U.S.C. § 2710 because it “engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio-visual materials.” *See* 18 U.S.C. § 2710(a)(4). In this regard, Facebook is engaged in the business of delivering video content and services to its users, including Plaintiffs, and Facebook regularly delivers and displays a variety of video content to its users. Likewise, Facebook is substantially involved in the conveyance of video content to consumers and is significantly tailored to serve that purpose. As detailed above, Facebook also enters into agreements with content providers in order to enable its users, including Plaintiffs, to access such content through Facebook.

810. Throughout the Class Period, Facebook delivered prerecorded video and visual materials to Facebook’s subscribers, including Plaintiffs, by making those materials electronically available to Plaintiffs on Facebook’s platform. For example, Facebook selects and delivers video content to Plaintiffs through its News Feed service and by making it available on Plaintiffs’ pages.

811. Facebook maintains depositories around the country that cache videos and visual materials for the purpose of delivering them to Plaintiffs and Facebook users so that Plaintiffs can obtain and view them. The visual materials include but are not limited to videos made available to subscribers through Facebook’s agreements with content providers such as Netflix and Hulu but also content available on Facebook Pages, YouTube and other websites. The materials include television programs, movies and other prerecorded visual content.

812. Plaintiffs are “consumers” under 18 U.S.C. § 2710(a)(1) because they are “subscriber[s] of goods or services” from Facebook. Plaintiffs are registered Facebook users who use the website through interaction with it. Specifically, Plaintiffs were required to provide personally identifiable information to Facebook in order to sign up, become registered users, receive Facebook User IDs, establish user profiles and engage in Facebook’s communities, including using and contributing to Facebook’s video streaming content and services.

813. Facebook itself uses the word “subscribe” to include users who participate on Facebook but who do not pay fees. By signing up for accounts with Facebook, becoming registered users,

receiving Facebook User IDs, establishing user profiles, providing Facebook with personal content and information, and spending time and attention using and contributing to Facebook’s video streaming services, Plaintiffs entered into transactions with Facebook to obtain access to Facebook’s content and services and for the purpose of subscribing to Facebook’s video streaming content and services.

814. The VPPA defines “personally identifiable information” to “include[] information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.” 18 U.S.C. § 2710(a)(1)(3). Facebook “knowingly disclose[d]” to persons—including Apps used by Facebook Friends of Plaintiffs such as the This Is Your Digital Life App, Business Partners, Whitelisted Apps, and advertisers – users’ personally identifiable information. Facebook’s unlawful disclosures of personally identifiable information were made through Facebook’s APIs, including but not limited to the following Extended Profile Properties: friends\_actions\_video, friends\_likes, friends\_photo\_video\_tags, and friends\_status, as well as the following Extended Permissions: read\_mailbox and read\_page\_mailboxes.

815. Plaintiffs’ content and information included “personally identifiable information” because the content Facebook gave to third parties identified Plaintiffs as having “requested or obtained specific video materials or services.” Specifically, Plaintiffs’ content and information included Facebook user IDs, names, addresses as well as information about Plaintiffs’ downloads, views, and comments relating to the videos that Facebook delivered was published by Facebook to App Developers. Plaintiffs’ content and information also included posts of videos, other video-related posts, Likes of videos, Page Likes for videos, tags in videos, video-related actions such as commenting on videos and sharing videos delivered by Facebook to News Feed and on users’ Timelines, and messages containing videos all revealed that users had requested or obtained video content.

816. Facebook’s unlawful disclosure of personally identifiable information concerning Plaintiffs was not incident to the “ordinary course of business” of delivering the visual content as that term is defined by the VPPA. *See* 18 U.S.C. § 2710(a)(2). The disclosure of users’ personally identifiable information to third parties not involved in the transactions as alleged herein was not necessary in order for Facebook to deliver those prerecorded visual materials to Plaintiffs.

817. The VPPA also provides that a video tape service provider may nonetheless disclose personally identifiable information concerning a consumer as long as that person has provided “informed written consent...in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer.” 18 U.S. Code § 2710(b)(2)(A)(i).

818. Facebook failed to obtain the “informed, written consent” of Plaintiffs “in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer” and “at the election of the consumer,” either “given at the time the disclosure is sought” or “given in advance for a set period of time, not to exceed 2 years or until consent is withdrawn by the consumer, whichever is sooner.” *See* 18 U.S.C. § 2710(b)(2)(B)(i)-(ii).

819. Facebook did not provide Plaintiffs with “an opportunity, in a clear and conspicuous manner, for the consumer[s] to withdraw on a case-by case basis or to withdraw from ongoing disclosures, at the consumer’s election.” *See* 18 U.S.C. § 2710(b)(2)(B)(iii).

820. The VPPA also requires that persons subject to the section “destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected.” *See* 18 U.S.C. § 2710(e). Upon information and belief, Facebook maintains rather than destroying users’ personally identifiable information under this statute, despite that it is no longer necessary for purposes of delivering the prerecorded visual materials.

821. Plaintiffs are “aggrieved person[s]” under the VPPA by Facebook’s disclosure of their personally identifiable information under 18 U.S.C. § 2710(b)(1), as alleged herein. Therefore, Plaintiffs may bring an action under § 2710(c) against Facebook.

822. Plaintiffs may be awarded actual damages, but not less than liquidated damages in an amount of \$2,500 per Plaintiff, punitive damages, attorneys’ fees and costs, and such other preliminary and equitable relief as the court determines to be appropriate.



Claim III.      **Deceit by Concealment or Omission**  
**Cal. Civ. Code §§ 1709 & 1710**  
**(Against Prioritized Defendant Facebook and Doe Defendants)**  
**On Behalf of All Plaintiffs and All Classes**

823. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

824. Under California law, a plaintiff may assert a claim for deceit by concealment based on “[t]he suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact.” Cal. Civ. Code § 1710(3).

825. These following actions are “deceit” under Cal. Civil Code § 1710 because Facebook suppressed facts that they were duty-bound to disclose, especially given Facebook’s assertions about protecting the privacy of Plaintiffs. Facebook has committed deceit by concealment in three distinct ways.

826. ***First***, Facebook did not disclose known risks that third party App Developers would sell or disperse user content and information.

827. Facebook received multiple warnings that Plaintiffs’ content and information was at risk.

- (1) In 2012, Sandy Parakilas, former Facebook operations manager, warned Facebook’s executives about the risks of App Developers gaining access to users’ personal information without their consent on Facebook’s platform. Yet, Facebook ignored Parakilas’s warnings.
- (2) In October 2012, Facebook reached a settlement with the FTC agreeing to clearly and prominently disclose its sharing of information with third parties; yet, Facebook continued to let App Developers access users’ information without their consent.
- (3) As late as 2017, Alex Stamos, Facebook’s former Chief of Security, warned Facebook executives about security risks on the platform. In an internal meeting held in 2017, Stamos warned of “intentional decisions to give access to data and systems to engineers to make them 'move fast' but that creates other issues for us.”
- (4) In 2017, Stamos states that he provided a written report concerning the circumstances leading to Cambridge Analytica obtaining users’ personal information. Facebook edited

and published a whitewashed version of this report concealing any wrongdoing.

828. Facebook did not audit what happened to content and information that was provided to third parties because it knew it would find abuse. Facebook did not disclose to Plaintiffs the risks that they faced from these warnings, and did not inform Plaintiffs that their content and information was insecure once it was shared with App Developers or other third parties.

829. Facebook knew that Plaintiffs' content and information was not secure. Facebook ignored the warnings above that audits were necessary to secure Plaintiffs' and Class Members' content and information because Defendants did not know what third parties were doing with it after it left Facebook's servers.

830. Defendants intentionally failed to secure Plaintiffs' information and content because they wanted to encourage third-party App Developers and other Business Partners to exploit that information and content. Defendants knew that appropriate security measures—such as audits—would discourage third parties. Defendants did not engage in such audits or conduct other reasonable efforts to protect Plaintiffs' content and information.

831. Defendants had a duty to inform Plaintiffs that Defendants had become aware that they had failed to secure their content and information. Facebook knew in 2015 that it had failed to secure Plaintiffs' content and information, including by making it available to Facebook's Business Partners, including but not limited to device makers, mobile carriers, software makers, security firms and chip designers.

832. Defendants intentionally concealed that Plaintiffs' information and content was insecure because they wanted Plaintiffs to continue to generate content for their Business Partners. Defendants failed to disclose the risks Plaintiffs faced with the intention to deceive them about the security of their content and information.

833. Defendants failed to disclose to Plaintiffs that it had failed to secure content and information for dozens of other third-party Apps, even after it became aware of abuse in 2015 with the Cambridge Analytica Scandal, and conducted no investigation of the extent to which it had failed to do so until March of 2018.

834. Had Plaintiffs been aware that Defendants had failed to implement adequate security measures, they would not have shared their information and content with Facebook to the extent that they did, if at all.

835. Plaintiffs were damaged because, as a result of Defendants' deceit, their content and information have been disclosed to third parties without their consent. Plaintiffs were also damaged because, as a result of Defendants' deceit, their privacy was invaded. Plaintiffs are at heightened risk of identity theft, phishing schemes, and other malicious attacks. Due to Defendants' deceit, Plaintiffs' information and content were compromised, and may be available on the dark web or in the hands of foreign nationals. Plaintiffs are therefore entitled to "any damage" that they have suffered under Civil Code Section 1709.

836. ***Second***, Defendants have committed deceit by failing to meaningfully disclose to Plaintiffs how Facebook allows other third parties—including but not limited to App Developers, "whitelisted" Apps, device makers, mobile carriers, software makers, and others—to obtain their personal information notwithstanding their privacy settings. With respect to "whitelisted" Apps, Facebook failed to disclose that Facebook would provide the Apps with users' content and information as long as the Whitelisted Apps provided Facebook with revenues that were based on how many users' content and information they accessed. Facebook failed to disclose that these users and their Friends could not control "whitelisted" Apps' access with their privacy settings.

837. Facebook allowed "whitelisted" Apps to continue to receive content and information from users and their Friends notwithstanding users' privacy settings.

838. Facebook stripped privacy settings from photos and videos that had been designated private, in violation of its own privacy policies. As a result, those Apps could not honor users' privacy settings.

839. In addition, "Apps were able to circumvent users' privacy of platform settings and access friends' information, even when the user disabled the Platform."<sup>433</sup>

840. Defendants misled users to believe that they were protecting users' privacy and failed to

---

<sup>433</sup> DCMS Report, *supra* note 28.

disclose that they were sharing users' content and information with third parties.

841. Defendants did not disclose that, notwithstanding privacy settings that purported to provide Plaintiffs with control over their content and information, Facebook allowed third -parties to harvest and store personal information.

842. Defendants had a duty to provide accurate information to Plaintiffs about how their content and information were disclosed to third parties by Facebook. Defendants knew that Plaintiffs shared personal and sometimes intimate details about their lives, personalities, and identities. Defendants encouraged Plaintiffs to share content and information by assuring them that Facebook would respect their choices concerning privacy.

843. Defendants intentionally concealed and omitted material information regarding how Facebook disclosed Plaintiffs' content and information in an effort to create a false sense of security and privacy for Plaintiffs. Defendants did this because they wanted Plaintiffs to provide more detailed content and information, whose value would be increased by that additional detail. Third parties would thereby pay a higher price for access to that content and information, increasing Facebook's revenue.

844. Had Plaintiffs been aware of the full extent of how Facebook collected and used their content and information, they would not have shared their content and information on their devices on the Facebook platform to the same degree that they did, if at all.

845. Plaintiffs were damaged because their content and information were disclosed to third-party device makers and other Business Partners without their consent. As a result of the disclosures of Plaintiffs' content and information to these third parties, Plaintiff could not take remedial measures to protect themselves from identity theft, scams, phishing, unwanted political targeting, even surveillance and other forms of harassment. Moreover, Plaintiffs would have behaved differently and shared less content and information had these acts been disclosed. Facebook deliberately withheld notice because it did not want to discourage user sharing and engagement on its platform.

846. ***Third***, Defendants failed to disclose to Plaintiffs how their content and information was being collected, shared and aggregated to develop digital profiles or dossiers of each user. Those dossiers, comprised of Facebook user content and information was combined with other sources to de-

anonymize this data such that Facebook users could be individually targeted.

847. Defendants had a duty to disclose the full extent to which it allowed Plaintiffs to be targeted by advertisers and marketers because it promised in its Contracts that it would not share users' content and information with advertisers without their consent. Defendants' duty also arose from its affirmative representations that (1) Plaintiffs could control their content and information, and (2) third parties could not access personal data absent users' consent.

848. Defendants knew that advertisers were targeting Plaintiffs with messages based upon Facebook-derived content and information, combined with content and information derived from other data brokers. Facebook was the vehicle to target Plaintiffs by drawing upon the vast amounts of content information collected by Facebook and "matched" with additional information collected about them by data brokers.

849. Defendants knew that psychographic marketing and other targeted advertising was very lucrative, and that advertisers paid a premium to combine content and information with data from data brokers.

850. Defendants did not disclose to Plaintiffs that advertisers were combining data from data brokers with Facebook-derived content and information to target them with advertisements and psychographic marketing, as well as building digital dossiers of users.

851. Defendants intended to deceive Plaintiffs about their vulnerability to targeted advertisements. Defendants intended to deceive Plaintiffs about the degree to which sharing their information and content on Facebook directly led to targeted messaging.

852. Had Plaintiffs known the extent to which Defendants shared their content and information with third parties, and how it was aggregated and made available to advertisers and political operatives, among others, Plaintiffs would have not shared their information and content on Facebook to the extent that they did, if it all.

853. Plaintiffs suffered injury as a direct result of Defendants' deceit. Plaintiffs conferred a benefit on Defendants. Their information and content were used and aggregated by advertisers and other third parties without their consent, and for nefarious—among other—uses, and Facebook received

substantial advertising revenues as a benefit. Had Plaintiffs known the extent and degree to which their content and information was provided to third parties, they would have required compensation for this use of their content and information.

854. Plaintiffs suffered economic injury as a result of Facebook's fraud. Plaintiffs have an economic interest in their content and information, which has value outside of the Facebook platform. Facebook's Business Partners, including Whitelisted Apps, would have

855. Facebook's CEO knew that it was worth at least \$0.10 for each App to view a user's profile, and Facebook orchestrated its "whitelisting" to require Apps to pay to Facebook revenues that were equivalent to the number of users and their Friends that each App had.

856. As a result, Defendants have been unjustly enriched by its deceit, and Plaintiffs and Class Members are entitled to restitution. "Restitution is a remedy that may be awarded to prevent unjust enrichment when the defendant has obtained some benefit from the plaintiff through fraud, duress, conversion or similar misconduct." *McBride v. Boughton*, 123 Cal.App.4th 379, 387–388 (2004).

857. For all types of fraudulent omissions complained of here, Plaintiffs seek disgorgement of Facebook's profits that were made with the use of Plaintiffs' content and information. Disgorgement is appropriate because Defendants profited from Plaintiffs' content and information wrongfully obtained by generating revenues from App Developers and advertisers. Disgorgement is necessary in order to deter future unauthorized use of Plaintiffs' content and information. Disgorgement is also necessary to the extent that the value of Plaintiffs' content and information cannot be assessed by ordinary tort damages. Public policy supports the use of disgorgement here to disincentivize the type of deception that Facebook used in exploiting Plaintiffs' content and information.

**Claim IV. Invasion of Privacy – Intrusion into Private Affairs  
(Against Prioritized Defendant Facebook and Doe Defendants;  
Non-Prioritized Defendants Bannon and Kogan)  
On Behalf of All Plaintiffs and All Classes**

858. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

859. Plaintiffs assert this Claim individually and on behalf of the Class and Minor Class (for purposes of this Claim, “Plaintiffs”) under California law.

860. Plaintiffs have shared private content and information, including private messages, personal information, location information, Timeline and Wall posts, and Likes, with a non-public audience such as Friends Only on Facebook or through Facebook Messenger and/or Facebook Chat. This information included personal family photographs, personal family videos, as well as personal perspectives regarding politics, religion, relationships, work, and family that Plaintiffs wanted to remain private and non-public.

861. Plaintiffs reasonably expected that the content and information that they shared on Facebook or through Facebook Messenger and/or Facebook Chat would be protected and secured against access by unauthorized parties and would not be disclosed to or obtained by unauthorized parties, or disclosed or obtained for any improper purpose.

862. Defendants intentionally intruded upon the private affairs and concerns of Plaintiffs by improperly accessing and obtaining Plaintiffs’ content and information and using it for improper purposes, including by targeting Plaintiffs with advertisements that would be highly offensive to a reasonable person, constituting an egregious breach of social norms and/or enabling the targeting of Plaintiffs with such advertisements, as detailed herein.

863. Facebook intentionally intruded upon the private affairs and concerns of Plaintiffs, by making Plaintiffs’ content and information available to unauthorized parties, including but not limited to Apps used by Facebook Friends of Plaintiffs such as the This Is Your Digital Life App, Business Partners, Whitelisted Apps, and advertisers, by disclosing this information to such unauthorized parties, and by failing to adequately protect and secure this information against access by such unauthorized parties.

864. Defendants’ intrusions upon the private affairs and concerns of Plaintiffs were substantial, and would be highly offensive to a reasonable person, constituting an egregious breach of social norms, as is evidenced by the intense public outcry and numerous, international governmental investigations in response to Defendants’ invasions of Plaintiffs’ privacy rights. Not only did Defendants



intrude upon a vast array of content and information regarding Plaintiffs, they did so in contravention of Plaintiffs' express designation of such content and information as non-public.

865. Facebook's conduct is especially offensive and egregious, in that Facebook misrepresented its practices and policies regarding data sharing to Plaintiffs, and omitted material information concerning Plaintiffs' ability to control access to their content and information through privacy settings. In this regard, Facebook not only committed privacy violations, but also affirmatively misled Plaintiffs into believing that they could control who accessed their content and information, that it would not give their personal content and information to advertisers, and that Facebook would respect and safeguard their choices regarding privacy. Facebook also omitted to tell Plaintiffs that they could not control who accessed their content and information (with respect to Business Partners and Whitelisted Apps), that it would allow advertisers to access, obtain, and de-anonymize their content and information, and that Facebook would not respect their choices regarding privacy. Moreover, Facebook intruded upon the private affairs and concerns of Plaintiffs for its own commercial benefit—to increase its growth and to attract and obtain advertising revenue.

866. Plaintiffs did not consent to Defendants' intrusions upon their private affairs and concerns.

867. Plaintiffs suffered actual and concrete injury as a result of Defendants' intrusions upon Plaintiffs' private affairs and concerns.

868. Plaintiffs and the Class seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiffs for the harm to their privacy interests, risk of future invasions of privacy, and the mental and emotional distress caused by Defendants' invasions of privacy, as well as disgorgement of profits made by Defendants as a result of their intrusions upon Plaintiffs' private affairs and/ concerns.

**Claim V. Invasion of Privacy – Public Disclosure of Private Facts  
(Against Prioritized Defendant Facebook and Doe Defendants;  
Non-Prioritized Defendants Bannon and Kogan)  
On Behalf of All Plaintiffs and All Classes**

869. Plaintiffs incorporate by reference all allegations of this complaint as though fully set

forth herein.

870. Plaintiffs assert this Claim individually and on behalf of the Class and Minor Class (for purposes of this Claim, “Plaintiffs”) under California law.

871. Plaintiffs have shared private content and information, including private messages, personal information, location information, Timeline and Wall posts, and Likes, with a non-public audience such as Friends Only on Facebook or through Facebook Messenger and/or Facebook Chat. This information included personal family photographs, personal family videos, as well as personal perspectives regarding politics, religion, relationships, work, and family that Plaintiffs wanted to remain private and non-public.

872. As detailed herein, Plaintiffs’ content and information that Facebook publicly disclosed was non-public, and Plaintiffs reasonably believed that this content and information would be protected against publication to unauthorized parties. In particular, Plaintiffs’ content and information was configured to be non-public either at the time of posting or through Facebook’s Privacy Settings, and Plaintiffs’ content and information communicated through Facebook Messenger and/or Facebook Chat was non-public, on account of the inherently private and non-public nature of instant messaging communication platforms.

873. Plaintiffs reasonably expected that the content and information that they shared on Facebook or through Facebook Messenger and/or Facebook Chat would be protected and secured against access by unauthorized parties and would not be disclosed to or obtained by unauthorized parties, or disclosed or obtained for any improper purpose.

874. As detailed herein, Facebook intentionally violated the privacy interests of Plaintiffs by publishing Plaintiffs’ content and information to unauthorized parties, including but not limited to Apps used by Facebook Friends of Plaintiffs such as the This Is Your Digital Life App, Business Partners, Whitelisted Apps, and advertisers, and by failing to take reasonable steps to prevent further publication of this content and information.

875. Facebook publicly disclosed Plaintiffs’ content and information both directly to unauthorized parties including Defendant Kogan and Business Partners as well as indirectly to

unauthorized parties including Cambridge Analytica and data brokers. The subsequent disclosure of user information by Apps and Business Partners to additional unauthorized parties was reasonably foreseeable, and Facebook knew or should have known about this subsequent disclosure. Facebook also failed to effectively audit, limit, or control Apps or Business Partners accessing user information so as to prevent the subsequent disclosure of user information. Further, Facebook directly profited from the subsequent disclosure of user information, through advertisements placed by unauthorized parties that received user information from Apps or Business Partners, including Cambridge Analytica.

876. Facebook's publication of Plaintiffs' content and information resulted in widespread disclosure of this information, constituting communication to the public in general. In particular, Facebook published Plaintiffs' content and information to approximately 53 or more Business Partners, approximately 5,200 or more Whitelisted Apps, and approximately 40,000 or more Apps used by Facebook Friends of Plaintiffs, including advertisers.

877. Facebook's publication of Plaintiffs' content and information would be highly offensive to a reasonable person, as is evidenced by the intense public outcry and numerous, international governmental investigations in response to Facebook's invasion of Plaintiffs' privacy rights, and decreased participation on the Facebook platform. Not only did Defendants publish a vast array of highly sensitive content and information regarding Plaintiffs, they did so in contravention of Plaintiffs' express designation of such content and information as non-public. In this regard, Facebook knew or acted with reckless disregard of the fact that a reasonable person would consider Facebook's publication of Plaintiffs' content and information to be highly offensive.

878. Facebook's conduct is especially offensive and egregious, in that Facebook misrepresented its practices and policies regarding data sharing to Plaintiffs, and omitted material information concerning Plaintiffs' ability to control access to their content and information through privacy settings. In this regard, Facebook not only committed privacy violations, but also affirmatively misled Plaintiffs into believing that they could control who accessed their content and information, that it would not give their personal content and information to advertisers, and that Facebook would respect and safeguard their choices regarding privacy. Facebook also omitted to tell Plaintiffs that they could not

control who accessed their content and information (with respect to Business Partners and Whitelisted Apps), that it would allow advertisers to access, obtain, and de-anonymize their content and information, and that Facebook would not respect their choices regarding privacy. Moreover, Facebook publicly disclosed Plaintiffs' content and information for its own commercial benefit—to increase its growth and to attract and obtain advertising revenue.

879. Plaintiffs' did not consent to Defendants' public disclosure of their highly sensitive content and information.

880. Plaintiffs' content and information was private and not of legitimate public concern or substantially connected to a matter of legitimate public concern.

881. Plaintiffs suffered actual and concrete injury as a result of Defendants' publication of Plaintiffs' content and information. Plaintiffs seek appropriate relief, including but not limited to damages that will reasonably compensate Plaintiffs for the public disclosure of their highly sensitive content and information and the mental and emotional distress caused by Defendants' invasions of privacy, as well as disgorgement of profits made by Facebook as a result of its publication of Plaintiffs' content and information.

**Claim VI. Breach of Contract  
(Against Prioritized Defendant Facebook)  
On Behalf of All Plaintiffs and All Classes**

882. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

883. At all relevant times, Facebook and Plaintiffs mutually assented to, and therefore were bound by the version of Facebook's Statement of Rights and Responsibilities or later, the Terms of Service, (collectively, the "Contracts") that was operative at the time each of the Plaintiffs joined Facebook.

884. Throughout the Class Period, Facebook affirmatively stated that Facebook would "not share your content and information with advertisers without your consent." None of the Contracts informed and obtained users' meaningful and lawfully-obtained consent to share their content and information with advertisers and other third parties, or disclosed that such information would be shared

if users' Friends entered into an agreement which permitted third parties to collect their Friends' information.

885. Thus, per the provision above, the Contracts did not authorize Facebook to share Plaintiffs' content and information with Facebook's Business Partners, including but not limited to mobile carriers, software makers, security firms, chip designers or device makers.

886. Further, per the provision above, the Contracts also did not authorize Facebook to make the content and information that users shared with Friends available to third party App Developers, or to sell such information to other third parties like Cambridge Analytica. The Contracts did provide that the user's content and information would be shared with a third-party application if the user *himself or herself* permitted an application to have access and agreed to its terms ("user sharing"). The Contracts did *not* provide that a user's content and information would be shared with a third-party application if a Friend of the user used such an application ("friend-of-user sharing"). At the very least, friend-of-user sharing fell outside the scope of the sharing allowed by the Contracts.

887. During the Class Period, Facebook failed to honor its promise to respect users' privacy settings. This was especially true with respect to "whitelisted" Apps, which received content and information notwithstanding users' privacy settings.

888. Additionally, Facebook breached the Contracts by stripping metadata and other information from photographs and videos that were accessed by an App. In doing so, Facebook breached its obligation to honor users' privacy settings.

889. GSR made an application available to Facebook users via Graph API v1.0. It used Graph API v1.0 to collect sensitive information regarding Plaintiffs—information that personally identified, or could easily be used to personally identify, Plaintiffs.

890. Facebook was informed that GSR then sold this information to Cambridge Analytica, which used the information to craft and target advertising on Facebook's platform to Plaintiffs. This was prohibited by the Contracts.

891. Upon information and belief, during the Class Period, certain Doe Defendants made applications available to Facebook users to collect sensitive information regarding Plaintiffs and the

Class. Upon information and belief, certain Doe Defendants also sold users' content and information to advertisers, thus causing a violation of the Contracts.

892. Contrary to the Contracts, Facebook knowingly allowed Doe Defendants who made their applications available through Graph API v1.0 to sell the content and information regarding Plaintiffs and the Class that they had collected via applications that used the Facebook platform.

893. The Contracts required Facebook to protect the content and information of its users. The Contracts affirm that users' content and information would not be shared with advertisers and other third parties without their affirmative consent. Likewise, these same terms of service informed users that their privacy setting would control who had access to their content and information, but this was untrue. Facebook did not disclose that users were required to affirmatively "opt out" of sharing their content and information with third parties in the Contracts.

894. As set forth herein, Plaintiffs' content and information is of considerable value as demonstrated by Facebook's calculation of the Average Revenue Per User that it calculates. There is an active market for the content and information generated by Facebook users, both individually and especially in the aggregate. Facebook generates billions of dollars in revenues through targeted advertising delivered to third parties, curated through the collection and aggregation of Facebook's user data. There is also an active black market for user content and information. The remedy for the breach of the Contracts is what Facebook gained through their breach.

895. The value of the content and information accumulated by Facebook about a user increases with the amount of content and information Facebook collects. Thus, over time, Facebook's benefit of the bargain has multiplied dramatically.

896. As a result of the breach, Plaintiffs have been harmed and have suffered damages by losing the value of their content and information.

**Claim VII. Negligence and Gross Negligence  
(Against Prioritized Defendant Facebook and Doe Defendants)  
On Behalf of All Plaintiffs and Classes**

897. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

898. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class.

899. Defendants owed a duty to Plaintiffs and the Class to exercise reasonable care in the obtaining, using, and protecting of their content and information, arising from the sensitivity of their content and information and the expectation that their content and information was not going to be shared with third parties without their consent. This duty included Facebook ensuring that no App Developers, device makers or other third parties, including Kogan, GSR and Cambridge Analytica, were improperly collecting, storing, obtaining and/or selling Plaintiffs' content and information.

900. Plaintiffs' willingness to entrust Defendants with their content and information was predicated on the understanding that Facebook would take appropriate measures to protect it. Facebook had a special relationship with Plaintiffs as a result of being entrusted with their content and information, which provided an independent duty of care.

901. Facebook knew that the content and information of Plaintiffs had value. Indeed, Facebook has earned billions of dollars from selling targeted advertising on its platform based on users' content and information as demonstrated by Facebook's calculation of the Average Revenue Per User. There is an active market for the content and information generated by Facebook users, both individually and especially in the aggregate. Facebook generates its billions of dollars in revenues through targeted advertising delivered to third parties, curated through the collection and aggregation of Facebook's users' content and information. There is also an active black market for user content and information.

902. Facebook received multiple warnings that Plaintiffs' content and information was at risk.

(1) In 2012, Sandy Parakilas, former Facebook operations manager, warned Facebook's executives about the risks of App Developers gaining access to users' personal information without their consent on Facebook's platform. Yet, Facebook ignored Parakilas's warnings.

(2) In October 2012, Facebook reached a settlement with the FTC agreeing to clearly and prominently disclose its sharing of information with third parties; yet, Facebook continued to let App Developers access users' information without their consent.



- (3) As late as 2017, Alex Stamos, Facebook’s former Chief of Security, warned Facebook executives about security risks on the platform. In an internal meeting held in 2017, Stamos warned of “intentional decisions to give access to data and systems to engineers to make them 'move fast' but that creates other issues for us.”
- (4) In 2017, Stamos states that he provided a written report concerning the circumstances leading to Cambridge Analytica obtaining users’ personal information. Facebook edited and published a whitewashed version of this report concealing any wrongdoing.
- (5) As reported by the *NY Times*, in 2016 Facebook exempted its Business Partner relationships, including some “whitelisted” Apps, from ongoing privacy reviews.<sup>434</sup>
- (6) Facebook knew, or was negligent in not knowing, that “whitelisted” Apps accessed users’ content and information beyond the scope of the purpose for which they had been authorized, and continued to have access to content and information even after the purpose for which they had been given access had expired.

903. Despite these warnings, Facebook failed to take reasonable steps to prevent harm to Plaintiffs:

- (1) According to Sandy Parakilas, Facebook was not conducting regular audits of App Developers using Facebook’s platform in 2012.
- (2) On April 30, 2014, Facebook announced a new “anonymous login” feature that would have allowed users to use an App without sharing any personal information. Yet, Facebook never implemented this feature.
- (3) On April 30, 2014, Facebook also announced a new “controlled login” feature to allow users to choose what information they shared with App Developers before logging in. Yet, Facebook did not implement this feature until May 2015.
- (4) As early as December 11, 2015, Facebook received notice that App Developer Aleksandr Kogan had shared users’ personal information with Cambridge Analytica; yet, Facebook waited until April 2018, more than three years later, to notify users that their personal

---

<sup>434</sup> Dance, et al, *As Facebook Raised a Privacy Wall*, *supra* note 158.

information had been improperly shared.

- (5) Facebook's failed to monitor Whitelisted Apps' access to content and information, and where third parties were granted access to support a specific function and that function was discontinued (such as Royal Bank of Canada, Netflix, and Yahoo!), Facebook failed to cut off access.

904. Facebook owed a duty to timely disclose to Plaintiffs that Facebook had allowed their content and information to be accessed by GSR, Cambridge Analytica and the Doe Defendants. Plaintiffs had a reasonable expectation that Facebook would inform them of the improper disclosure of their content and information.

905. Facebook breached its duties by, among other things: (a) failing to ensure that App Developers, "whitelisted" Apps, device makers and other third parties were not improperly collecting, storing, obtaining and/or selling Plaintiffs' content and information without users' informed consent; and (b) failing to provide adequate and timely notice that Plaintiff's content and information had been improperly obtained by Cambridge Analytica and Doe Defendants.

906. But for Facebook's breach of its duties, including its duty to use reasonable care to protect and secure Plaintiffs' content and information, Plaintiffs' content and information would not have been disclosed without their consent to third parties, which resulted in further misuse of Plaintiffs' content and information.

907. Plaintiffs were foreseeable victims of Facebook's breach of its duties. Facebook knew or should have known that allowing third parties to access Plaintiffs' and Class Members' content and information would cause damage to Plaintiffs.

908. As a result of Facebook's negligent failure to safeguard Plaintiffs' content and information, Plaintiffs have suffered injury, which includes but is not limited to impermissible disclosure of their content and information, both directly and indirectly by Facebook, and exposure to a heightened, imminent risk of misuse, fraud, identity theft, voter fraud, medical fraud, and financial and other harms.

909. The content and information shared with third parties allows this content and information

to be aggregated with other data to identify and target Plaintiffs. It is reasonable for Plaintiffs to obtain identity protection or credit monitoring services in light of the foregoing. Plaintiffs seek to recover the cost of these services from Facebook.

910. The injury to Plaintiff was a proximate, reasonably foreseeable result of Facebook's breaches of its aforementioned duties.

911. As a proximate result of Facebook's negligence in failing to take due care to monitor the use of user content and information by third parties like mobile device makers, carriers, software makers, security firms, chip designers, GSR and Doe Defendants, Plaintiffs suffered damages in an amount to be proved at trial.

912. Public policy voids any purported waiver of liability to which Facebook may claim Plaintiffs assented:

A. The contract(s) between Facebook and Plaintiffs concern a business of a type generally thought suitable for public regulation; indeed, Facebook is subject to public regulation.

B. Due to Facebook's ubiquity and importance in the daily lives of Americans, it performs a service of great importance to the public. Using Facebook is often a matter of practical necessity for the many persons who use Facebook to coordinate daily activities, network, engage in political and cultural discourse, and pursue interests and hobbies. To do these things, Facebook users must share their personal information with their Friends.

C. Facebook holds itself out as a free provider of its services to aged 13 or above.

D. Because of the network effect and the importance of Facebook's services, Facebook possesses a decisive advantage of bargaining strength against any member of the public that seeks to use its services.

E. Any purported waiver of liability occurs in a standardized adhesion contract that users must accept or reject in toto.

F. Facebook is ultimately in total control of its platform and services. The confidentiality of Plaintiffs' personal information, therefore, is under Facebook's control and subject to its carelessness.

G. Facebook violated its privacy policies by allowing “whitelisted” Apps and Business Partners to access content and information notwithstanding users’ privacy settings.

913. In addition, any purported waiver of liability is unconscionable.

914. Facebook’s conduct also constitutes gross negligence due to its extreme departure from ordinary standards of care, and its knowledge that it had failed to secure the content and information of Plaintiffs.

**Claim VIII. Violations of the California Unfair Competition Law  
Cal. Bus. & Prof. Code §§ 17200 *et seq.*  
(Against Prioritized Defendant Facebook and Doe Defendants;  
Non-Prioritized Defendants Bannon and Kogan)  
On Behalf of All Plaintiffs and Classes**

915. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

916. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class.

917. Defendants’ conduct as alleged herein constitutes unfair, unlawful, or fraudulent business acts or practices as proscribed by California’s Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.* (“UCL”).

918. As alleged above, Facebook violated Plaintiffs’ privacy by allowing their personal content to be exploited in ways that Plaintiffs could not have been anticipated. Plaintiffs interests were also violated through Defendants’ deceptive acts. Had Plaintiffs known the extent to which Facebook allowed their personal content to be collected, aggregated, pooled, and transferred for commercial purposes to companies such as Cambridge Analytica, Plaintiffs would not have shared their content and information on Facebook to the same extent they did, if at all. Facebook allowed App Developers, device makers and other third parties to harvest users’ Friends content and information on a large scale, with no effective notice to Plaintiffs, and without any opportunity for Plaintiffs to become reasonably informed about Facebook’s default privacy settings allowing App Developers, device makers and other third parties to harvest users’ Friends content and information or the risks that large-scale disclosure of their content and information would present. Facebook made assurances to Plaintiffs about respecting their privacy, and being able to own and control their content and information. Given these affirmative

statements, Facebook had a duty to disclose the nature and extent of the uses of users' content and information that Facebook allowed "whitelisted" Apps, App Developers, device makers, and other third parties to make.

919. **Defendants' conduct is "unfair."** California has a strong public policy to protect privacy interests, including in protecting the content and information shared by Plaintiff. Defendants violated this public policy by exploiting Plaintiffs' content and information without informed consent.

920. Defendants' conduct also violated the interests protected by the Video Privacy Protection Act, 18 U.S.C. § 2710; the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*; Cal. Civ. Code §§ 1709, 1710 and Article 1, § 1 of the California Constitution. To establish liability under the unfair prong, Plaintiffs need not establish that these statutes were actually violated, although the claims pleaded herein do so.

921. Facebook did not reasonably inform Plaintiffs of the uses of their content and information, and invaded Plaintiffs' privacy by subjecting their content and information to large-scale disclosure without knowledge or meaningful consent. Facebook's conduct included stripping Plaintiffs' privacy metadata from their photos and videos, and allowing "whitelisted" Apps and Business Partners to access Plaintiffs' content and information notwithstanding their privacy settings. Facebook created a false sense of privacy, defeating Plaintiffs reasonable expectations of privacy.

922. Plaintiffs could not have anticipated this degree of intrusion into their privacy, which included exposure to psychographic marketing. Defendants' conduct did not create a benefit that outweighs these strong public policy interests. Defendants' conducts narrowly benefitted Facebook and its Business Partners at the expense of the privacy of millions of people. Additionally, the effects of Facebook's conduct were comparable to or substantially the same as the conduct forbidden by the California Constitution and the common law's prohibitions against invasion of privacy, in that Facebook's conduct invaded fundamental privacy interests.

923. **Defendants' conduct is "unlawful."** Defendants' conduct violates the Video Privacy Protection Act, 18 U.S.C. § 2710; the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*; Cal. Civ. Code §§ 1709, 1710; and Article 1, § 1 of the California Constitution.

924. Facebook's conduct violated the spirit and letter of these laws, which protect privacy interests and prohibit misleading and deceptive practices. The content and information that Facebook allowed third parties to harvest exposed Plaintiffs to an increased risk of identity theft, voter fraud, tax return fraud, and allowed third parties to link their identities to other data in order to de-anonymize them.

925. **Defendants' conduct is fraudulent.** As alleged above, Defendants misled Plaintiffs concerning the use of their content and information affirmatively and through material omissions, and the privacy protection Facebook provided their content and information. Defendants did not meaningfully disclose that Plaintiffs' content and information could be obtained by "whitelisted" Apps, device makers and other Business Partners, notwithstanding Plaintiffs' privacy settings. Defendants did not disclose that privacy designations for photographs and videos were disregarded when received by Apps. Defendants did not disclose that Facebook's default privacy settings allowed third party Apps to obtain their content and information, and obfuscated how Plaintiffs could have protected their content and information from disclosure to third parties. Defendants omitted material information about how Plaintiffs' personal content was harvested, stored, searched, used and sold.

926. Plaintiffs have suffered injury in fact and lost money or property due to Defendants' business acts or practices. Plaintiffs' content and information has tangible value.

927. Restitution under the UCL is designed to return the plaintiff to the status quo ex ante.

928. Facebook told users that they owned their content and information. Additionally, because Facebook directly leveraged access to Plaintiffs' content and information in order to obtain revenues from "whitelisted" Apps and other Business Partners, Plaintiffs have a property interest in Facebook's profits. Facebook took users' property without compensation.

929. Facebook calculates an ARPU based on a user's specific circumstances and that a market exists for the content and information Plaintiffs generate.

930. There is value in Plaintiffs' content and information that Facebook disseminated to Business Partners and "whitelisted" Apps. Plaintiffs lost the opportunity to receive value from these third parties in exchange for their personal information.

931. Facebook's CEO knew that it was worth at least \$0.10 for each App to view a user's profile, and Facebook orchestrated its "whitelisting" to require Apps to pay to Facebook revenues that were equivalent to the number of users and their Friends that each App had.

932. Plaintiffs' content and information is in the possession of third parties who have used and will use it for their own advantage, including financial advantage, or have sold it or will sell it for value, making it clear that Plaintiffs' content and information has tangible value.

933. Plaintiffs are at increased risk of identity theft due to Facebook's practices concerning sharing users' content and information with third parties. Plaintiffs may be subjected to voter fraud, identity theft, medical fraud, and other harms. The content and information shared with third parties allows this content and information to be aggregated with other data to identify and target Plaintiffs. It is reasonable for Plaintiffs and Class Members to obtain identity protection or credit monitoring services in light of the foregoing. Plaintiffs seek to recover the cost of these services from Facebook.

934. Defendants invaded Plaintiffs' privacy by failing to inform Plaintiffs and Class Members that Facebook was sharing their content and information with its Business Partners, including but not limited to App Developers, mobile carriers, software makers, security firms, device makers and chip designers.

935. Defendants further failed to inform Plaintiffs about the nature of the App Developers' business, or the purposes for which App Developers were obtaining their content and information. Facebook did not disclose the nature or the extent of the exploitation of Plaintiffs' content and information. Facebook invaded Plaintiffs' privacy by subjecting them to psychographic marketing that exploited intimate aspects of their identity, including emotional and psychological manipulation.

936. Plaintiffs' content and information was exploited without informed consent. Accordingly, Plaintiffs are entitled to part of Facebook's profits that were generated by their content and information without informed consent.

937. Plaintiffs seek an order to enjoin Defendants from such unlawful, unfair, and fraudulent business acts or practices, and to restore to Plaintiffs their interest in money or property that may have been acquired by Defendants by means of unfair competition.



938. Section 17203 of the UCL authorizes a court to issue injunctive relief “as may be necessary to prevent the use or employment by any person of any practice which constitutes unfair competition.” Plaintiffs also seek the following injunctive relief: (1) an “opt in” rather than “opt out” default for sharing personal content in all of Facebook’s user settings; (2) disclosure of the purposes of which Plaintiffs’ personal content is used by Facebook, data brokers, device makers, mobile carriers, software makers, security firms, App Developers, advertisers and other third parties with whom Facebook has shared users’ content and information without their consent; (3) destruction of all personal content obtained by Defendants and all such third parties where such content is within Defendants’ control or possession; (4) a complete audit and accounting of the uses of Plaintiffs’ content and information by App Developers, device makers, and other Business Partners ; (5) a permanent injunction preventing such sharing of content and information with these third parties without Facebook users’ informed consent and affirmative authorization; and (6) a permanent ban on targeting Plaintiffs with advertisements or marketing materials based on information from data brokers.

**Claim IX. Violation of Article I, Section 1 of the California Constitution  
(Against Prioritized Defendant Facebook and Doe Defendants;  
Non-Prioritized Defendants Bannon and Kogan)  
On Behalf of All Plaintiffs and All Classes**

939. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

940. Plaintiffs assert this Claim individually and on behalf of the Class and Minor Class (for purposes of this Claim, “Plaintiffs”) under California law.

941. The California Constitution expressly provides for a right to privacy: “All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.” Cal. Const., art. I, § 1

942. Plaintiffs have shared private content and information, including personal information, location information, posts, and Likes, with a non-public audience such as Friends Only on Facebook or through Facebook Messenger and/or Facebook Chat. This information included personal family

photographs, personal family videos, as well as personal perspectives regarding politics, religion, relationships, work, and family that Plaintiffs wanted to remain private and non-public.

943. Plaintiffs reasonably expected that the content and information that they shared on Facebook or through Facebook Messenger and/or Facebook Chat would be protected and secured against access by unauthorized parties and would not be disclosed to or obtained by unauthorized parties, or disclosed or obtained for any improper purpose.

944. Plaintiffs have a privacy interest in preventing the unauthorized disclosure and misuse of their content and information and in conducting their personal activities without intrusion or interference, including the right to not to have their content and information accessed, obtained, and misused by third parties, including Apps used by Facebook Friends of Plaintiffs such as the This Is Your Digital Life App, Business Partners, Integration Partners / Whitelisted Apps, and advertisers, either for the benefit of such parties, or at the expense of their own interests.

945. Defendants intentionally violated the privacy interests of Plaintiffs by improperly accessing and obtaining Plaintiffs' content and information and using it for improper purposes, including by targeting Plaintiffs with advertisements that would be highly offensive to a reasonable person, constituting an egregious breach of social norms and/or enabling the targeting of Plaintiffs with such advertisements, as detailed herein.

946. Facebook intentionally violated the privacy interests of Plaintiffs, by making Plaintiffs' content and information available to unauthorized parties, including but not limited to Apps used by Facebook Friends of Plaintiffs such as the This Is Your Digital Life App, Business Partners, Integration Partners / Whitelisted Apps, and advertisers, by disclosing this information to such unauthorized parties, and by failing to adequately protect and secure this information against access by such unauthorized parties.

947. Defendants' violations of Plaintiffs' privacy interests were substantial, and would be highly offensive to a reasonable person, constituting an egregious breach of social norms, as is evidenced by the intense public outcry and numerous, international governmental investigations in response to Defendants' invasions of Plaintiffs' privacy rights. Not only did Defendants intrude upon

and disclose a vast array of content and information regarding Plaintiffs, they did so in contravention of Plaintiffs' express designation of such content and information as non-public.

948. Facebook's conduct is especially offensive and egregious, in that Facebook misrepresented its practices and policies regarding data sharing to Plaintiffs, and omitted material information concerning Plaintiffs' ability to control access to their content and information through privacy settings. In this regard, Facebook not only committed privacy violations, but also affirmatively misled Plaintiffs into believing that they could control who accessed their content and information, that it would not give their personal content and information to advertisers, and that Facebook would respect and safeguard their choices regarding privacy. Facebook also omitted to tell Plaintiffs that they could not control who accessed their content and information (with respect to Business Partners and Whitelisted Apps), that it would allow advertisers to access, obtain, and de-anonymize their content and information, and that Facebook would not respect their choices regarding privacy. Moreover, Facebook violated the privacy interests of Plaintiffs for its own commercial benefit—to increase its growth and to attract and obtain advertising revenue.

949. In this regard, Facebook was aware that Plaintiffs were vulnerable to having their content and information accessed, obtained, and misused, and Facebook intended for these privacy violations to occur without Plaintiffs' knowledge or consent. Had Plaintiffs known the manner and extent to which Facebook allowed their content and information to be obtained and misused by unauthorized parties, Plaintiffs would not have shared their content and information on Facebook to the same extent they did, if at all.

950. Plaintiffs did not consent to Defendants' violations of their privacy interests.

951. Plaintiffs suffered actual and concrete injury as a result of Defendants' violations of their privacy interests.

952. Plaintiffs and the Class seek appropriate relief for these injuries, including but not limited to damages that will reasonably compensate Plaintiffs for the harm to their privacy interests, risk of future invasions of privacy, and the mental and emotional distress caused by Defendants' invasions of privacy, as well as disgorgement of profits made by Defendants as a result of their privacy violations.

**Claim X. Violation of California Common Law Right of Publicity  
(Against Prioritized Defendant Facebook and Doe Defendants;  
Non-Prioritized Defendants Bannon and Kogan)  
On Behalf of All Plaintiffs and Classes**

953. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

954. Plaintiffs assert this Claim individually and on behalf of the Class and Minor Class (for purposes of this Claim, “Plaintiffs”) under California law.

955. California common law prohibits the use of a person’s name or likeness for the defendant’s advantage, commercial or otherwise, without first obtaining that person’s consent.

956. Facebook violated this section by using and publishing Plaintiffs’ names and likenesses for its advantage by allowing third parties, including but not limited to Apps used by Facebook Friends of Plaintiffs such as the This Is Your Digital Life App, Business Partners, Integration Partners / Whitelisted Apps, and advertisers, to access, obtain, and use Plaintiffs’ likenesses—including names, Likes, personal photographs, and personal videos—without first obtaining their consent.

957. On information and belief, providing access to the likenesses of Plaintiffs was integral to Facebook’s relationships with third parties, including but not limited to Apps used by Facebook Friends of Plaintiffs such as the This Is Your Digital Life App, Business Partners, Integration Partners / Whitelisted Apps, and advertisers. Facebook’s appropriation and provision of access to the likenesses of Plaintiffs was to Facebook’s advantage, resulting in growth and advertising revenue that would not have resulted without Facebook’s provision of access to this information. In this regard, the value of the services Facebook offered to App Developers was derived in substantial part from the provision of such access. Facebook thus misappropriated, gained a commercial advantage from, and capitalized on the economic value generated through the provision of access to the likenesses of Plaintiffs.

958. For example, Facebook profited from advertising purchased by Cambridge Analytica, after Facebook allowed Cambridge Analytica to obtain Plaintiffs’ personal information through the This Is Your Digital Life App. Similarly, Facebook gained a commercial advantage when it entered into contractual agreements with Business Partners and Whitelisted Apps that allowed these partners and Apps to obtain users’ information, including their names and likenesses, and were not subject to users’

privacy settings. Facebook shared this information with Business Partners and Whitelisted Apps in order to obtain growth and advertising revenues. In this regard, granting Apps, Whitelisted Apps, and Business Partners access to Plaintiffs' content and information enabled Facebook to promote and expand its platform, including across devices, service providers, and other platforms. Such relationships resulted in an exponential rate of growth and significant commercial benefit to Facebook, as evidenced by the drastic increase in Facebook's revenues as well as its average revenue per user over the Class Period.

959. Prior to using and providing access to Plaintiffs' likenesses, Facebook never obtained consent from Plaintiffs. In this regard, Facebook misrepresented and omitted material information concerning Plaintiffs' ability to control access to their content and information through privacy settings. Facebook misrepresented and failed to inform Plaintiffs that they could not control who accessed their content and information, that Facebook would allow advertisers to access, obtain, de-anonymize, share their content and information, and use and misuse this content and information for uses beyond the App, and that Facebook would not respect their choices regarding privacy. Moreover, Facebook intruded upon the private affairs and concerns of Plaintiffs for its own commercial benefit—to increase its growth and to attract and obtain advertising revenue.

960. Plaintiffs did not receive any compensation in return for Facebook's use of or provision of access to their likenesses.

961. Plaintiffs were harmed by Facebook's improper use of or provision of access to their likenesses.

962. Plaintiffs seek actual damages suffered, plus any profits attributable to Facebook's use of or provision of access to their likenesses not calculated in actual damages. Plaintiffs also seek punitive damages, costs, and reasonable attorney's fees as allowed under this statute.

**Claim XI. Breach of the Implied Covenant of Good Faith and Fair Dealing  
(Against Defendant Facebook)**

963. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

964. Under California law, there is in every contract or agreement an implied promise of good faith and fair dealing. Such a duty is read into contracts and functions as a supplement to the express contractual covenants, in order to prevent a transgressing party from engaging in conduct which (while not technically transgressing the express covenants) frustrates the other party's rights to the benefit of the contract. Thus, any claim on the part of Facebook that technically it was permitted to allow the collection and transmittal of Plaintiffs' data, must be read in the context of, and give way to, those users' rights to the benefit of the contract, including the terms strictly delimiting such activity.

965. Facebook entered into a Statement of Rights and Responsibilities with Plaintiffs.

966. A covenant of good faith and fair dealing attaches to Facebook's Statement of Rights and Responsibilities.

967. In its Statements of Rights and Responsibilities, Facebook promised Plaintiffs that "We do not give your content or information to advertisers without your consent."

968. Facebook also promised "[y]our privacy is very important to us," and that Plaintiffs could control their content and information because they "own all of the content and information [they] post on Facebook, and [they] can control how it is shared through your privacy and application settings."

969. Plaintiffs did all they were required to do under these contractual provisions.

970. Under the terms of the Statement of Rights and Responsibilities, Plaintiffs were entitled to receive the benefits promised to them by Facebook, including that Facebook would protect the privacy of their user content and information, would not disclose user content and information to third parties without the user's consent, and would keep user content and information secure.

971. Facebook was uniquely able to control the rights of its users, including Plaintiffs, concerning their privacy, ownership and control of their content and information, and whether their content and information would be provided to advertisers, device makers, and/or third parties without consent.

972. Facebook surreptitiously took measures to frustrate and undercut Plaintiffs' contractual rights concerning their privacy, ownership and control over their content and information, and whether their content and information would be provided to advertisers without consent. By doing so, Facebook

deprived Plaintiffs of the benefits under their contracts with Facebook, including the Statements of Rights and Responsibilities.

973. Facebook allowed “whitelisted” Apps to access their content and information, and that of their Friends, without regard to their privacy settings.

974. Facebook stripped privacy settings from photos and videos that had been designated private, in violation of its own privacy policies.

975. Facebook entered into business relationships with App Developers, device makers, big companies such as Amazon and Qualcomm, and other third parties that allowed Plaintiffs’ content and information to be transmitted without the user’s consent.

976. By disclosing, publishing, and providing Facebook users’ content and information to advertisers without informing Plaintiffs, Facebook breached the covenant of good faith and fair dealing. Facebook allowed its users to be targeted by advertisements, including psychographic marketing, without seeking consent of Plaintiffs, and did not allow Plaintiffs to make informed decisions about sharing their content and information on Facebook’s platform. This unfairly interfered with Plaintiffs’ rights under the Statement of Responsibilities to have their user content and information kept secure and private and not disclosed to third parties without the theirs consent.

977. Additionally, by failing to secure Plaintiffs’ content and information, and by taking measures to ensure that Plaintiffs’ privacy settings and reasonable expectations of privacy were not recognized or honored, including by disclosing and publishing user content and information through Facebook’s API streams sent to App Developers, device makers, and other third parties, Facebook deprived Plaintiffs of the benefits of their agreements.

978. Plaintiffs were damaged by Facebook’s breaches of its duty of good faith and fair dealing. Plaintiffs did not receive the benefit of the bargain for which they contracted. Plaintiffs suffered invasions of privacy and were directly targeted by advertisers without their consent, including by Cambridge Analytica. Plaintiffs content and information was released, disclosed, and published, and they are at risk of identity theft. In this regard, Facebook failed to secure Plaintiffs’ content and information and shifted the burden of doing so from Facebook to Plaintiffs.



**Claim XII. Quantum Meruit to Recover Sums Had by Unjust Enrichment  
(Against Prioritized Defendants Facebook and Doe Defendants)  
On Behalf of All Plaintiffs and All Classes**

979. Plaintiffs reallege and incorporate by reference all allegations of this complaint as though fully set forth herein. This claim is pleaded in the alternative to the claims for breach of contract.

980. Because no adequate legal remedy is available under any applicable contract, Plaintiffs bring this count in quasi contract on behalf of themselves in order to pursue restitution based on Facebook's unjust enrichment, including by way of Defendants' retention of profits that should have been expended to protect the data of Plaintiffs per its published privacy agreements and policies.

981. As alleged herein, Defendants have unjustly received and retained monetary benefits from Plaintiffs—*i.e.*, by way of its use of, and profiting from, their data under unjust circumstances, such that inequity has resulted.

982. By engaging in the conduct described in this complaint, Defendants knowingly obtained benefits from Plaintiffs as alleged herein under circumstances such that it would be inequitable and unjust for Facebook to retain them.

983. More specifically, by engaging in the acts and failures to act described in this complaint, Defendants have been knowingly enriched by revenues they received from "whitelisted" Apps in exchange for continued access to Plaintiffs' content and information. Facebook received revenues that were directly proportional to the number of users whose content and information was obtained by "whitelisted" Apps. Facebook itself estimated that the value of one App viewing one user's profile was \$0.10, and aimed to capture revenues from "whitelisted" Apps that reflected the extent to which the "whitelisted" Apps accessed content and information.

984. Facebook failed to obtain consent from Plaintiffs for the use of their content and information to "whitelisted" Apps, and other Business Partners. Indeed, Facebook falsely informed Plaintiffs and class members that they could control access to content and information through their privacy settings.

985. Also, Facebook has been enriched unjustly by the use of Plaintiffs' content and information, and has profited greatly as a result, even though it did not protect this data as it had

promised. Indeed, Defendants' failure to protect this content and information fueled Defendants' enrichment. Encouraging Plaintiffs to share their content and information allowed Defendants to collect more such information and aggregate it, to target them more precisely.

986. By engaging in the conduct described in this complaint, Defendants have knowingly obtained benefits from or by way of Plaintiffs, including by way of the use of their personal information in the course of its business, including their lucrative data broker business, under circumstances such that it would be inequitable and unjust for it to retain them.

987. Thus, Defendants will be unjustly enriched if it is permitted to retain the benefits derived from the unauthorized and impermissible gathering and sharing of Plaintiffs data.

988. Plaintiffs are therefore entitled to a restitutionary award in an amount to be determined at trial, or the imposition of a constructive trust upon the monies derived by Facebook by means of the above-described actions, or both as the circumstances may merit to provide complete relief to Plaintiffs, whether the sums of monies are those: (a) the proportional revenues that Facebook generated by providing access to Plaintiffs' content and information from "whitelisted" Apps; or (b) the money it has collected from advertisers and others that corresponds to the user data that is the subject of this lawsuit; or (c) other sums as it may be just and equitable to return to them.

## **B. Priority Consumer Protection Act Claims Alleged in the Alternative**

### **Claim XIII. Violations of the Alabama Deceptive Trade Practices Act Ala. Code §§ 8-19-1 *et seq.* (2018) (Against Facebook) (In the Alternative)**

989. Plaintiff Tonya Smith individually and on behalf of the Alabama Subclass, ("Plaintiffs," for purposes of this Claim), incorporate by reference all allegations of this complaint as though fully set forth herein.

990. Facebook is a "person" as defined by Ala. Code § 8-19-3(5).

991. Facebook's products and services are "goods" and "services" as defined by Ala. Code § 8-19-3(3), (7).

992. Facebook advertised, offered, or sold goods or services in Alabama and engaged in trade or commerce directly or indirectly affecting the people of Alabama as defined by Ala. Code § 8-19-3(8).

993. The Alabama Deceptive Trade Practices Act, Ala. Code §§ 8-19-1 *et seq.*, prohibits unfair, deceptive, false, and unconscionable trade practices.

994. Facebook engaged in unconscionable, false, misleading or deceptive practices in connection with its business, commerce and trade practices in violation of Ala. Code § 8-19-5(27).

995. Facebook's representations and omissions were material because they were likely to deceive reasonable consumers.

996. Facebook intended Plaintiffs to rely on its misrepresentations, omissions, and other unlawful conduct.

997. Had Facebook disclosed to Plaintiffs that it misrepresented and omitted material information about the nature of the privacy of user data, users' ability to control how their data was used, and access of user data to third parties, and was otherwise engaged in deceptive, common business practices, Facebook would have been unable to continue in business and it would have been forced to disclose the defects in its privacy protection. Instead, Facebook represented that its services were protecting user privacy and that users could control the use of the private data. Plaintiffs acted reasonably in relying on Facebook's misrepresentations and omissions, the truth of which they could not have discovered.

998. Facebook acted intentionally, knowingly, and maliciously to violate Alabama's Deceptive Trade Practices Act, and recklessly disregarded Plaintiffs' rights.

999. As a direct and proximate result of Facebook's unfair and deceptive acts and practices, Plaintiffs have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages.

1000. Plaintiffs have suffered injuries in fact and lost money or property due to Defendant's business acts or practices. Plaintiffs' personal content has tangible value. Their personal content is in the possession of third parties who have used and will use it for their own advantage, including financial advantage, or was and is being sold for value, making it clear that the personal content has tangible value.

1001. Plaintiffs are at increased risk of identity theft due to Facebook's practices concerning

sharing data with third parties. Plaintiffs may be subjected to voter fraud, identity theft, medical fraud, and other harms. The personal content shared with third parties allows personal content to be aggregated with other data to identify and target Plaintiffs. It is reasonable for Plaintiffs to obtain identity protection or credit monitoring services in light of the foregoing. Plaintiffs seek to recover the cost of these services from Facebook.

1002. Facebook invaded Plaintiffs' privacy by failing to keep them informed about the nature of the App Developers' business, or the purposes for which App Developers were obtaining their personal content. Facebook did not disclose the nature or the extent of the exploitation of Plaintiffs' personal content. Facebook invaded Plaintiffs' privacy by subjecting them to psychographic marketing that exploited intimate aspects of their identity, including emotional and psychological manipulation.

1003. Plaintiffs' personal content was exploited without informed consent. Accordingly, Plaintiffs are entitled to part of Facebook's profits that were generated by their personal content without informed consent.

1004. Written demand for relief has been provided as required under Ala. Code § 8-19-10(e).

1005. Plaintiffs seek all monetary and non-monetary relief allowed by law, including the greater of (a) actual damages or (b) statutory damages of \$100; treble damages; injunctive relief; attorneys' fees, costs, and any other relief that is just and proper.

**Claim XIV. Violations of the Colorado Consumer Protection Act  
Colo. Rev. Stat. Ann. §§ 6-1-101 *et seq.*  
(Against Prioritized Defendant Facebook) (In the Alternative)**

1006. Plaintiff Shelly Forman, individually and on behalf of the Colorado Subclass ("Plaintiffs," for purposes of this Claim), incorporate by reference all allegations of this complaint as though fully set forth herein.

1007. Facebook is a "person" as defined by Colo. Rev. Stat. Ann. § 6-1-102(6).

1008. Facebook provides goods and/or services.

1009. Plaintiffs, as well as the general public, are actual or potential consumers of the services offered by Facebook to actual consumers.

1010. Facebook engaged in deceptive trade practices in the course of its business, in violation

of Colo. Rev. Stat. Ann. § 6-1-105(1)(u) by failing to disclose material information concerning its services, including its improper use and lack of protection for private user data, which was known at the time of an advertisement or sale and the failure to disclose this information was intended to induce Plaintiffs to use Facebook's services.

1011. Facebook also engaged in deceptive trade practices in the course of its business, in violation of Colo. Rev. Stat. Ann. § 6-1-105(3) by engaging unfair trade practices actionable at common law or under other statutes of Colorado.

1012. Facebook's representations and omissions were material because they were likely to deceive reasonable consumers to believe their user data could be and was kept private.

1013. Facebook intended to mislead Plaintiffs and induce them to rely on its misrepresentations and omissions.

1014. Had Facebook disclosed to Plaintiffs that it misrepresented and omitted material information about the nature of the privacy of user data, users' ability to control how their data was used, and access of user data to third parties, and was otherwise engaged in deceptive, common business practices, Facebook would have been unable to continue in business and it would have been forced to disclose the defects in its privacy protection. Instead, Facebook represented that its services were protecting user privacy and that users could control the use of the private data. Plaintiffs acted reasonably in relying on Facebook's misrepresentations and omissions, the truth of which they could not have discovered.

1015. Facebook acted fraudulently, willfully, knowingly, or intentionally to violate Colorado's Consumer Protection Act, and with recklessly disregarded Plaintiffs' rights.

1016. As a direct and proximate result of Facebook's deceptive trade practices, Plaintiffs suffered injuries to their legally protected interests.

1017. Plaintiffs have suffered injuries in fact and lost money or property due to Defendant's business acts or practices. Plaintiffs personal content has tangible value. Their personal content is in the possession of third parties who have used and will use it for their own advantage, including financial advantage, or was and is being sold for value, making it clear that the personal content has tangible

value.

1018. Plaintiffs are at increased risk of identity theft due to Facebook's practices concerning sharing data with third parties. Plaintiffs may be subjected to voter fraud, identity theft, medical fraud, and other harms. The personal content shared with third parties allows personal content to be aggregated with other data to identify and target Plaintiffs. It is reasonable for Plaintiffs to obtain identity protection or credit monitoring services in light of the foregoing. Plaintiffs seek to recover the cost of these services from Facebook.

1019. Facebook invaded Plaintiffs privacy by failing to keep them informed about the nature of the App Developers' business, or the purposes for which App Developers were obtaining their personal content. Facebook did not disclose the nature or the extent of the exploitation of Plaintiffs personal content. Facebook invaded Plaintiffs privacy by subjecting them to psychographic marketing that exploited intimate aspects of their identity, including emotional and psychological manipulation.

1020. Plaintiffs personal content was exploited without informed consent. Accordingly, Plaintiffs are entitled to part of Facebook's profits that were generated by their personal content without informed consent.

1021. Facebook's deceptive trade practices significantly impact the public, because Facebook's user platform is used throughout the world, with hundreds of thousands of users who are Colorado residents and consumers.

1022. Plaintiffs seek all monetary and non-monetary relief allowed by law, including the greater of: (a) actual damages, or (b) \$500, or (c) three times actual damages (for Facebook's bad faith conduct); injunctive relief; and reasonable attorneys' fees and costs.

**Claim XV.   Violations of the Illinois Consumer Fraud and  
Deceptive Business Practices Act  
815 Ill. comp. stat. Ann. §§ 505 *et seq.*  
(Against Prioritized Defendant Facebook) (In the Alternative)**

1023. Plaintiff Kimberly Robertson, individually and on behalf of the Illinois Subclass ("Plaintiffs," for purposes of this Claim), incorporates by reference all allegations of this complaint as though fully set forth herein.

1024. Facebook is a “person” as defined by 815 Ill. Comp. Stat. Ann. § 505/1(c).

1025. Plaintiffs are “consumer[s]” as defined by 815 Ill. Comp. Stat. Ann. § 505/1(e).

1026. Facebook’s conduct as described herein was in the conduct of “trade” or “commerce” as defined by 815 Ill. Comp. Stat. Ann. § 505/1(f).

1027. Facebook’s deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. Ann. § 505/2.

1028. Facebook’s representations and omissions concerning the use of and privacy of user data were material because they were likely to deceive reasonable consumers to believe their user data could be and was kept private.

1029. Facebook intended to mislead Plaintiffs and induce them to rely on its misrepresentations and omissions. Plaintiffs and the Illinois Subclass reasonably relied on Facebook’s representations about the security of their private data.

1030. The above unfair and deceptive practices and acts by Facebook were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefit to consumers or to competition.

1031. Facebook acted intentionally, knowingly, and maliciously to violate Illinois’s Consumer Fraud and Deceptive Business Practices Act, and recklessly disregarded Plaintiffs’ rights.

1032. As a direct and proximate result of Facebook’s unfair and deceptive acts and practices, Plaintiffs have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in using Facebook’s services.

1033. Plaintiffs have suffered injuries in fact and lost money or property due to Defendant’s business acts or practices. Plaintiffs’ personal content has tangible value. Their personal content is in the possession of third parties who have used and will use it for their own advantage, including financial advantage, or was and is being sold for value, making it clear that the personal content has tangible value.

1034. Plaintiffs are at increased risk of identity theft due to Facebook’s practices concerning



sharing data with third parties. Plaintiffs may be subjected to voter fraud, identity theft, medical fraud, and other harms. The personal content shared with third parties allows personal content to be aggregated with other data to identify and target Plaintiffs. It is reasonable for Plaintiffs to obtain identity protection or credit monitoring services in light of the foregoing. Plaintiffs seek to recover the cost of these services from Facebook.

1035. Facebook invaded Plaintiffs' privacy by failing to keep them informed about the nature of the App Developers' business, or the purposes for which App Developers were obtaining their personal content. Facebook did not disclose the nature or the extent of the exploitation of Plaintiffs' personal content. Facebook invaded Plaintiffs' privacy by subjecting them to psychographic marketing that exploited intimate aspects of their identity, including emotional and psychological manipulation.

1036. Plaintiffs' personal content was exploited without informed consent. Accordingly, Plaintiffs are entitled to part of Facebook's profits that were generated by their personal content without informed consent.

1037. Plaintiffs seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

**Claim XVI. Violations of the Iowa Private Right of Action for Consumer Frauds Act  
Iowa Code Ann. § 714H  
(Against Prioritized Defendant Facebook) (In the Alternative)**

1038. On behalf of the Iowa Subclass ("Plaintiffs," for purposes of this Claim), Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

1039. Facebook is a "person" as defined by Iowa Code Ann. § 714H.2(7).

1040. Plaintiffs are "consumer[s]" as defined by Iowa Code § 714H.2(3).

1041. Facebook's conduct described herein related to or was in connection with the "sale" or "advertisement" of "merchandise" as defined by Iowa Code Ann. § 714H.2(2), (6), (8).

1042. Facebook engaged in unfair, deceptive, and unconscionable trade practices, in violation of the Iowa Private Right of Action for Consumer Frauds Act, as described throughout and herein.

1043. Facebook's representations and omissions were material because they were likely to deceive reasonable consumers to believe their user data could be and was kept private.

1044. Facebook intended to mislead Plaintiffs and induce them to rely on its misrepresentations and omissions.

1045. Facebook acted intentionally, knowingly, and maliciously to violate Iowa's Private Right of Action for Consumer Frauds Act, and recklessly disregarded Plaintiffs' rights.

1046. As a direct and proximate result of Facebook's unfair and deceptive acts and practices, Plaintiffs have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in using Facebook's services.

1047. Plaintiffs have suffered injuries in fact and lost money or property due to Defendant's business acts or practices. Plaintiffs' personal content has tangible value. Their personal content is in the possession of third parties who have used and will use it for their own advantage, including financial advantage, or was and is being sold for value, making it clear that the personal content has tangible value.

1048. Plaintiffs are at increased risk of identity theft due to Facebook's practices concerning sharing data with third parties. Plaintiffs may be subjected to voter fraud, identity theft, medical fraud, and other harms. The personal content shared with third parties allows personal content to be aggregated with other data to identify and target Plaintiffs. It is reasonable for Plaintiffs to obtain identity protection or credit monitoring services in light of the foregoing. Plaintiffs seek to recover the cost of these services from Facebook.

1049. Facebook invaded Plaintiffs' privacy by failing to keep them informed about the nature of the App Developers' business, or the purposes for which App Developers were obtaining their personal content. Facebook did not disclose the nature or the extent of the exploitation of Plaintiffs' personal content. Facebook invaded Plaintiffs' privacy by subjecting them to psychographic marketing that exploited intimate aspects of their identity, including emotional and psychological manipulation.

1050. Plaintiffs' personal content was exploited without informed consent. Accordingly, Plaintiffs are entitled to part of Facebook's profits that were generated by their personal content without informed consent.

1051. Plaintiff has provided notice to the Iowa Attorney General and has received the Attorney General's approval pursuant to Iowa Code Ann. § 714H.7.

1052. Plaintiffs seek all monetary and non-monetary relief allowed by law, including injunctive relief, damages, punitive damages, and reasonable attorneys' fees and costs.

**Claim XVII. Violations of the Kansas Consumer Protection Act  
Kan. Stat. Ann. §§ 50-623 *et seq.*  
(Against Prioritized Defendant Facebook) (In the Alternative)**

1053. Plaintiff Dustin Short, individually and on behalf of the Kansas Subclass ("Plaintiffs," for purposes of this Claim), incorporate by reference all allegations of this complaint as though fully set forth herein.

1054. Kan. Stat. Ann. §§ 50-623 *et seq.* is to be liberally construed to protect consumers from suppliers who commit deceptive and unconscionable practices.

1055. Plaintiffs are "consumer[s]" as defined by Kan. Stat. Ann. § 50-624(b).

1056. The acts and practices described herein are "consumer transaction[s]," as defined by Kan. Stat. Ann. § 50-624(c).

1057. Facebook is a "supplier" as defined by Kan. Stat. Ann. § 50-624(l).

1058. Facebook advertised, offered, or sold goods or services in Kansas and engaged in trade or commerce directly or indirectly affecting the people of Kansas.

1059. Facebook's representations and omissions were material because they were likely to deceive reasonable consumers to believe their user data could be and was kept private.

1060. Facebook intended to mislead Plaintiffs and induce them to rely on its misrepresentations and omissions.

1061. Had Facebook disclosed to Plaintiffs that it misrepresented and omitted material information about the nature of the privacy of user data, users' ability to control how their data was used, and access of user data to third parties, and was otherwise engaged in deceptive, common business practices, Facebook would have been unable to continue in business and it would have been forced to disclose the defects in its privacy protection. Instead, Facebook represented that its services were protecting user privacy and that users could control the use of the private data. Plaintiffs acted

reasonably in relying on Facebook's misrepresentations and omissions, the truth of which they could not have discovered.

1062. Facebook also engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of Kan. Stat. Ann. § 50-627, including: knowingly taking advantage of the inability of Plaintiffs to reasonably protect their privacy interests, due to their lack of knowledge (*see id.* § 50-627(b)(1)); and requiring Plaintiffs to enter into a consumer transaction on terms that Facebook knew were substantially one-sided in favor of Facebook particularly as concerned users' private data (*see id.* § 50-627(b)(5)).

1063. Plaintiffs had unequal bargaining power with respect to their use of Facebook's services because of Facebook's omissions and misrepresentations.

1064. The above unfair, deceptive, and unconscionable practices and acts by Facebook were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

1065. Facebook acted intentionally, knowingly, and maliciously to violate Kansas's Consumer Protection Act, and recklessly disregarded Plaintiffs' rights.

1066. As a direct and proximate result of Facebook's unfair, deceptive, and unconscionable trade practices, Plaintiffs have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in using Facebook's services.

1067. Plaintiffs have suffered injuries in fact and lost money or property due to Defendant's business acts or practices. Plaintiffs' personal content has tangible value. Their personal content is in the possession of third parties who have used and will use it for their own advantage, including financial advantage, or was and is being sold for value, making it clear that the personal content has tangible value.

1068. Plaintiffs are at increased risk of identity theft due to Facebook's practices concerning sharing data with third parties. Plaintiffs may be subjected to voter fraud, identity theft, medical fraud,

and other harms. The personal content shared with third parties allows personal content to be aggregated with other data to identify and target Plaintiffs. It is reasonable for Plaintiffs to obtain identity protection or credit monitoring services in light of the foregoing. Plaintiffs seek to recover the cost of these services from Facebook.

1069. Facebook invaded Plaintiffs' privacy by failing to keep them informed about the nature of the App Developers' business, or the purposes for which App Developers were obtaining their personal content. Facebook did not disclose the nature or the extent of the exploitation of Plaintiffs' personal content. Facebook invaded Plaintiffs' privacy by subjecting them to psychographic marketing that exploited intimate aspects of their identity, including emotional and psychological manipulation.

1070. Plaintiffs' personal content was exploited without informed consent. Accordingly, Plaintiffs are entitled to part of Facebook's profits that were generated by their personal content without informed consent.

1071. Plaintiffs seek all monetary and non-monetary relief allowed by law, including civil penalties or actual damages (whichever is greater), under Kan. Stat. Ann. §§ 50-634, 50-636; injunctive relief; and reasonable attorneys' fees and costs.

**Claim XVIII. Violations of the Michigan Consumer Protection Act  
Mich. Comp. Laws Ann. §§ 445.901 *et seq.*  
(Against Prioritized Defendant Facebook) (In the Alternative)**

1072. On behalf of the Michigan Subclass ("Plaintiffs," for purposes of this Claim), Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

1073. Facebook and Plaintiffs are "person[s]" as defined by Mich. Comp. Laws Ann. § 445.902(1)(d).

1074. Facebook advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.902(1)(g).

1075. Facebook engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

- a. "Making a representation of fact or statement of fact material to the transaction

such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is.” *Id.* § 445.903(1)(bb); and

- b. “Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner.” *Id.* § 445.903(1)(cc).

1076. Facebook’s representations and omissions were material because they were likely to deceive reasonable consumers to believe their user data could be and was kept private.

1077. Facebook intended to mislead Plaintiffs and induce them to rely on its misrepresentations and omissions.

1078. Facebook acted intentionally, knowingly, and maliciously to violate Michigan’s Consumer Protection Act, and recklessly disregarded Plaintiffs’ rights.

1079. As a direct and proximate result of Facebook’s unfair, deceptive, and unconscionable trade practices, Plaintiffs have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in using Facebook’s services.

1080. Plaintiffs have suffered injuries in fact and lost money or property due to Defendant’s business acts or practices. Plaintiffs personal content has tangible value. Their personal content is in the possession of third parties who have used and will use it for their own advantage, including financial advantage, or was and is being sold for value, making it clear that the personal content has tangible value.

1081. Plaintiffs are at increased risk of identity theft due to Facebook’s practices concerning sharing data with third parties. Plaintiffs may be subjected to voter fraud, identity theft, medical fraud, and other harms. The personal content shared with third parties allows personal content to be aggregated with other data to identify and target Plaintiffs. It is reasonable for Plaintiffs to obtain identity protection or credit monitoring services in light of the foregoing. Plaintiffs seek to recover the cost of these services from Facebook.

1082. Facebook invaded Plaintiffs’ privacy by failing to keep them informed about the nature of the App Developers’ business, or the purposes for which App Developers were obtaining their

personal content. Facebook did not disclose the nature or the extent of the exploitation of Plaintiffs' personal content. Facebook invaded Plaintiffs' privacy by subjecting them to psychographic marketing that exploited intimate aspects of their identity, including emotional and psychological manipulation.

1083. Plaintiffs' personal content was exploited without informed consent. Accordingly, Plaintiffs are entitled to part of Facebook's profits that were generated by their personal content without informed consent.

1084. Plaintiffs seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or \$250, injunctive relief, and any other relief that is just and proper.

**Claim XIX. Violations of the New York General Business Law  
N.Y. Gen. Bus. Law §§ 349 *et seq.*  
(Against Prioritized Defendant Facebook) (In the Alternative)**

1085. Plaintiff William Lloyd, individually and on behalf of the New York Subclass ("Plaintiffs," for purposes of this Claim), incorporate by reference all allegations of this complaint as though fully set forth herein.

1086. Facebook engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of goods or services, in violation of N.Y. Gen. Bus. Law § 349, as described herein.

1087. Facebook's representations and omissions were material because they were likely to deceive reasonable consumers to believe their user data could be and was kept private.

1088. Facebook acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiffs' rights.

1089. As a direct and proximate result of Facebook's unfair, deceptive, and unconscionable trade practices, Plaintiffs have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in using Facebook's services and keeping their data private.

1090. Facebook's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the millions of New Yorkers who use Facebook's services.



1091. The above deceptive and unlawful practices and acts by Facebook caused substantial injury to Plaintiffs that they could not reasonably avoid.

1092. As a direct and proximate result of Facebook's unfair and deceptive acts and practices, Plaintiffs have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in using Facebook's services.

1093. Plaintiffs have suffered injuries in fact and lost money or property due to Defendant's business acts or practices. Plaintiffs' personal content has tangible value. Their personal content is in the possession of third parties who have used and will use it for their own advantage, including financial advantage, or was and is being sold for value, making it clear that the personal content has tangible value.

1094. Plaintiffs are at increased risk of identity theft due to Facebook's practices concerning sharing data with third parties. Plaintiffs may be subjected to voter fraud, identity theft, medical fraud, and other harms. The personal content shared with third parties allows personal content to be aggregated with other data to identify and target Plaintiffs. It is reasonable for Plaintiffs to obtain identity protection or credit monitoring services in light of the foregoing. Plaintiffs seek to recover the cost of these services from Facebook.

1095. Facebook invaded Plaintiffs' privacy by failing to keep them informed about the nature of the App Developers' business, or the purposes for which App Developers were obtaining their personal content. Facebook did not disclose the nature or the extent of the exploitation of Plaintiffs' personal content. Facebook invaded Plaintiffs' privacy by subjecting them to psychographic marketing that exploited intimate aspects of their identity, including emotional and psychological manipulation.

1096. Plaintiffs' personal content was exploited without informed consent. Accordingly, Plaintiffs are entitled to part of Facebook's profits that were generated by their personal content without informed consent.

1097. Plaintiffs seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of \$50 (whichever is greater), treble damages, injunctive relief, and

attorney's fees and costs.

**Claim XX. Violations of the Washington Consumer Protection Act  
Wash. Rev. Code Ann. §§ 19.86.010 *et seq.*  
(Against Prioritized Defendant Facebook) (In the Alternative)**

1098. Plaintiffs Terry Fischer, individually and on behalf of the Washington Subclass ("Plaintiffs," for purposes of this Claim), incorporate by reference all allegations of this complaint as though fully set forth herein.

1099. Facebook is a "[p]erson," as defined by Wash. Rev. Code Ann. § 19.86.010(1).

1100. Facebook advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010(2).

1101. Facebook engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, as described herein.

1102. Facebook's representations and omissions were material because they were likely to deceive reasonable consumers to believe their user data could be and was kept private.

1103. Facebook acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiffs' rights. Facebook's knowledge of the improper protection and use of private user data, and release of private user data, put it on notice that the services were not as it advertised.

1104. Facebook's conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration of public interest impact, and/or injured persons and had and has the capacity to injure persons. Further, its conduct affected the public interest, including the at least hundreds of thousands of Washingtonians affected by Facebook's deceptive business practices.

1105. As a direct and proximate result of Facebook's unfair methods of competition and unfair or deceptive acts or practices, Plaintiffs have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in using Facebook's services.

1106. Plaintiffs have suffered injuries in fact and lost money or property due to Defendant's business acts or practices. Plaintiffs' personal content has tangible value. Their personal content is in the possession of third parties who have used and will use it for their own advantage, including financial advantage, or was and is being sold for value, making it clear that the personal content has tangible value.

1107. Plaintiffs are at increased risk of identity theft due to Facebook's practices concerning sharing data with third parties. Plaintiffs may be subjected to voter fraud, identity theft, medical fraud, and other harms. The personal content shared with third parties allows personal content to be aggregated with other data to identify and target Plaintiffs. It is reasonable for Plaintiffs to obtain identity protection or credit monitoring services in light of the foregoing. Plaintiffs seek to recover the cost of these services from Facebook.

1108. Facebook invaded Plaintiffs' privacy by failing to keep them informed about the nature of the App Developers' business, or the purposes for which App Developers were obtaining their personal content. Facebook did not disclose the nature or the extent of the exploitation of Plaintiffs' personal content. Facebook invaded Plaintiffs' privacy by subjecting them to psychographic marketing that exploited intimate aspects of their identity, including emotional and psychological manipulation.

1109. Plaintiffs' personal content was exploited without informed consent. Accordingly, Plaintiffs are entitled to part of Facebook's profits that were generated by their personal content without informed consent.

1110. Plaintiffs seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

**Claim XXI. Violations of the West Virginia Consumer Credit and Protection Act  
(Against Prioritized Defendant Facebook) (In the Alternative)  
W. Va. Code ann. §§ 46A-6-101 *et seq.***

1111. On behalf of the West Virginia Subclass ("Plaintiffs," for purposes of this Claim), Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

1112. Plaintiffs are "[c]onsumer[s]," as defined by W. Va. Code Ann. § 46A-6-102(2).

1113. Facebook engaged in "consumer transaction[s]," as defined by W. Va. Code Ann. § 46A-

6-102(2).

1114. Facebook advertised, offered, or sold goods or services in West Virginia and engaged in trade or commerce directly or indirectly affecting the people of West Virginia, as defined by W. Va. Code Ann. § 46A-6-102(6).

1115. Facebook has been on notice concerning its wrongful conduct as alleged herein by Plaintiffs. However, sending pre-suit notice pursuant to W. Va. Code § 46A-6-106(c) is an exercise in futility for Plaintiff, because, despite being on knowledge of the deceptive acts and practices complained of herein in this lawsuit as of the date of the first-filed lawsuit in March 2018, Facebook has not cured its unfair and deceptive acts and practices.

1116. Facebook engaged in unfair and deceptive business acts and practices in the conduct of trade or commerce, in violation of W. Va. Code Ann. § 46A-6-104, as described herein.

1117. Facebook's unfair and deceptive acts and practices also violated W. Va. Code Ann. § 46A-6-102(7), including:

- a. "Engaging in any other conduct which similarly creates a likelihood of confusion or of misunderstanding." *Id.* § 46A-6-102(7)(L); and
- b. "The act, use or employment by any person of any deception, fraud, false pretense, false promise or misrepresentation, or the concealment, suppression or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any goods or services, whether or not any person has in fact been misled, deceived or damaged thereby." *Id.* § 46A-6-102(7)(M).

1118. Facebook's unfair and deceptive acts and practices were unreasonable when weighed against the need to develop or preserve business, and were injurious to the public interest, under W. Va. Code Ann. § 46A-6-101.

1119. Facebook's acts and practices were additionally "[u]nfair" under W. Va. Code Ann. § 46A-6-104 because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to

consumers or to competition.

1120. The injury to consumers from Facebook's conduct was and is substantial because it was non-trivial and non-speculative; and involved an ascertainable injury. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

1121. Consumers could not have reasonably avoided injury because Facebook's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers, Facebook created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

1122. Facebook's business practices had no countervailing benefit to consumers or to competition.

1123. Facebook's acts and practices were additionally "deceptive" under W. Va. Code Ann. § 46A-6-104 because Facebook made representations or omissions of material facts that misled or were likely to mislead reasonable consumers, including Plaintiffs.

1124. Facebook intended to mislead Plaintiffs and induce them to rely on its misrepresentations and omissions.

1125. Facebook's representations and omissions were material because they were likely to deceive reasonable consumers to believe their user data could be and was kept private.

1126. Had Facebook disclosed to Plaintiffs that it misrepresented and omitted material information about the nature of the privacy of user data, users' ability to control how their data was used, and access of user data to third parties, and was otherwise engaged in deceptive, common business practices, Facebook would have been unable to continue in business and it would have been forced to disclose the defects in its privacy protection. Instead, Facebook represented that its services were protecting user privacy and that users could control the use of the private data. Plaintiffs acted reasonably in relying on Facebook's misrepresentations and omissions, the truth of which they could not have discovered.

1127. Facebook had a duty to disclose the above-described facts due to the circumstances of this case. Facebook's duty to disclose arose from its:

- a. Possession of exclusive knowledge regarding the defects in its services;
- b. Possession of exclusive knowledge regarding its services and inadequate protection and abuse of user data;
- c. Active concealment of the defects in its services and protection and abuse of user data; and
- d. Incomplete representations about its services and protection and abuse of user data.

1128. Facebook's omissions were legally presumed to be equivalent to active misrepresentations because Facebook intentionally prevented Plaintiffs from discovering the truth regarding Facebook's use, sale, disclosure and abuse of private user data.

1129. Facebook acted intentionally, knowingly, and maliciously to violate West Virginia's Consumer Credit and Protection Act, and recklessly disregarded Plaintiffs' rights.

1130. As a direct and proximate result of Facebook' unfair and deceptive acts or practices and Plaintiffs' purchase of goods or services, Plaintiffs have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in using Facebook's services.

1131. Plaintiffs have suffered injuries in fact and lost money or property due to Defendant's business acts or practices. Plaintiffs' personal content has tangible value. Their personal content is in the possession of third parties who have used and will use it for their own advantage, including financial advantage, or was and is being sold for value, making it clear that the personal content has tangible value.

1132. Plaintiffs are at increased risk of identity theft due to Facebook's practices concerning sharing data with third parties. Plaintiffs may be subjected to voter fraud, identity theft, medical fraud, and other harms. The personal content shared with third parties allows personal content to be aggregated with other data to identify and target Plaintiffs. It is reasonable for Plaintiffs to obtain identity protection

or credit monitoring services in light of the foregoing. Plaintiffs seek to recover the cost of these services from Facebook.

1133. Facebook invaded Plaintiffs' privacy by failing to keep them informed about the nature of the App Developers' business, or the purposes for which App Developers were obtaining their personal content. Facebook did not disclose the nature or the extent of the exploitation of Plaintiffs' personal content. Facebook invaded Plaintiffs' privacy by subjecting them to psychographic marketing that exploited intimate aspects of their identity, including emotional and psychological manipulation.

1134. Plaintiffs' personal content was exploited without informed consent. Accordingly, Plaintiffs are entitled to part of Facebook's profits that were generated by their personal content without informed consent.

1135. Facebook's violations present a continuing risk to Plaintiffs as well as to the general public.

1136. Plaintiffs seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or \$200 per violation under W. Va. Code Ann. § 46A-6-106(a), restitution, injunctive and other equitable relief, punitive damages, and reasonable attorneys' fees and costs.

### **C. Non-Prioritized Claims**

#### **Claim XXII. Racketeer Influence and Corrupt Organizations Act, 18 U.S.C. § 1962(c) (Against Prioritized Defendant Facebook and Doe Defendants; Non-Prioritized Defendants Kogan, Bannon, SCL Group, and GSR as "Co-Conspirators")**

1137. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

1138. Plaintiffs assert this Claim individually and on behalf of the Class and Minor Class (for purposes of this Claim, "Plaintiffs").

1139. Plaintiffs assert violations of 18 U.S.C. § 1962(C).

1140. Upon information and belief, the Defendants associated with GSR, Cambridge-Analytica-related-entities and other unnamed Co-Conspirator related entities, for the purpose of utilizing illicitly obtained content and information (for purposes of this claim, "User Information") for the targeting of digital political propaganda (the "Digital Political Propaganda Enterprise"). The Defendants



therefore constitute a RICO enterprise pursuant to 18 U.S.C. § 1961(4). In the alternative, these individuals and entities constitute an enterprise because they associated together for the common purpose of utilizing illicitly obtained personally identifiable information for the targeting of digital political propaganda.

1141. Upon information and belief, the Digital Political Propaganda Enterprise is an enterprise engaged in, and whose activities affect, interstate commerce. This enterprise has been in operation since at least 2014.

1142. The association-in-fact Digital Political Propaganda Enterprise consisted of the following structure: the Co-Conspirator Defendants—Aleksandr Kogan and Stephen K. Bannon—along with Non-Defendant Co-Conspirators Cambridge Analytica and other related entities, and yet unknown third parties involved in data mining and data analysis, operated an association-in-fact enterprise, which was formed for the purpose of utilizing illicitly obtained User Information for the targeting of digital political propaganda. Each of the Co-Conspirator Defendants was employed by or associated with, and conducted or participated in the affairs of the Digital Political Propaganda Enterprise:

A. Aleksandr Kogan participated in, operated and/or directed the Digital Political Propaganda Enterprise by, among other things: (i) creating a U.K. company called Global Science Research, Ltd. (“GSR”) which was part of a scheme to dupe users into providing their User Information, which was part of the broader scheme of illegally harvesting of data; (ii) through GSR, creating a Facebook App called “ThisIsYourDigitalLife” (“YDL”) which consisted of a personality quiz; (iii) utilizing Amazon Mechanical Turk’s (“MTurk”) program to recruit participants (known as “Turkers”) to complete the personality quiz; and (iv) utilizing the data gathered through the quiz to improperly harvest the data of millions of Facebook subscribers;

B. Stephen K. Bannon participated in, operated and/or directed the Digital Political Propaganda Enterprise by, among other things: (i) founded Cambridge Analytica; (ii) obtained funding for the efforts of Cambridge Analytica; (iii) acted as a Vice-President of Cambridge Analytica and (iv) oversaw the efforts of Cambridge Analytica to collect troves of Facebook

data.

1143. The actions of the Co-Conspirator Defendants were undertaken with fraud, malice, or oppression, or with a willful and conscious disregard of the rights or safety of Plaintiffs and class members. As such, Plaintiffs and each of the Class members are entitled to an award of exemplary and punitive damages against each of the Co-Conspirator Defendants in an amount according to proof at trial.

1144. The Co-Conspirator Defendants worked together to accomplish their scheme or common course of conduct. This enterprise has been in operation since at least 2014.

1145. The racketeering activity committed by each of the members of the Digital Political Propaganda Enterprise affected interstate commerce.

1146. On information and belief, the Co-Conspirator Defendants agreed to and did conduct and participate, directly and indirectly, in the conduct of the Digital Political Propaganda Enterprise's affairs in a pattern of racketeering activity targeted at intentionally defrauding Facebook users including, without limitation, via nominal payments and numerous intentionally false representations averred herein with the specific intent of inducing Facebook users to unwittingly share other users' private User Information.

1147. Pursuant to and in furtherance of their corrupt scheme, the Co-Conspirator Defendants did in fact induce Facebook users to share other Facebook users' User Information via hundreds of thousands of separate electronic monetary transfers.

1148. The Co-Conspirator Defendants willfully and knowingly devised a scheme with artifice to defraud Facebook users and to obtain, sell, and use personal User Information by false pretenses and representations, including, but not limited to, the representation that the data would only be used for academic purposes.

1149. The payments made or directed by the Co-Conspirator Defendants or any other entity to obtain Facebook data compromised in the Your Digital Life scandal were in furtherance of the fraudulent scheme. On information and belief, those payments were made by wire transfer or other electronic means through interstate or foreign commerce.

1150. The payments made from any of the Co-Conspirator Defendants or directed by any Co-Conspirator to takers of the Your Digital Life quiz were in furtherance of the fraudulent scheme. On information and belief, those payments were made by wire transfer or other electronic means through interstate or foreign commerce.

1151. The acts of wire fraud averred herein constitute a pattern of racketeering activity pursuant to 18 U.S.C. § 1961(5).

1152. The Co-Conspirator Defendants have directly and indirectly participated in the conduct of the Conspiracy's affairs through the pattern of racketeering and activity alleged herein, in violation of 18 U.S.C. § 1962(c). Facebook aided and abetted the Co-Conspirator Defendants by misleading its users to believe that their data was safe, while permitting third-party Apps like GSR's to access and use the data of non-consenting users without their permission and knowledge, and the other Co-Conspirator Defendants directly participated in the conspiracy by misleading quiz-takers that they were allowing Co-Conspirator Defendants' access to only their personal data for academic purposes, when in fact they were allowing access to their Friends' data, and by fraudulently obtaining the data, selling it in interstate and foreign commerce, and using it to influence elections.

1153. Plaintiffs and Class members were harmed by the Co-Conspirator Defendants' conduct because the private information they did not intend to become public or disclose to third parties was acquired by companies who intended to and did use it illicitly for manipulating elections and other as yet unknown purposes. Furthermore, the security breach put Plaintiffs and Class members in imminent and real danger of having their identities stolen by anyone willing to pay these unscrupulous companies for the data. In addition, Plaintiffs and class members spent time and money securing their personal information and protecting their identities, by, for instance, purchasing identity theft protection.

1154. As a direct and proximate result of the Co-Conspirator Defendants' racketeering activities and violations of 18 U.S.C. § 1962(c), Plaintiffs and the Class have been injured.

1155. Plaintiffs demand judgment in their favor and against the Co-Conspirator Defendants jointly and severally for compensatory, treble, and punitive damages with interest, the costs of suit and attorneys' fees, and other and further relief as this Court deems just and proper.

**Claim XXIII. Misappropriation of Valuable Property  
(Against Prioritized Defendant Facebook and Doe Defendants)**

1156. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

1157. Plaintiffs assert this Claim individually and on behalf of the Class and Minor Class (for purposes of this Claim, “Plaintiffs”) under California law.

1158. Defendants’ actions constitute misappropriation.

1159. Defendants used Plaintiffs’ content and information in violation of Facebook’s promises to protect their privacy.

1160. Plaintiffs and Class members did not consent to this use.

1161. Defendants’ gained a commercial benefit by using Plaintiffs’ valuable personal and private information when Defendant misappropriated, used, and/or sold for profit Plaintiffs’ content and information.

1162. Plaintiffs were harmed.

1163. Defendants’ conduct was a substantial factor in causing Plaintiffs’ and Class members’ harm.

1164. Accordingly, Plaintiffs are entitled to relief.

**Claim XXIV. Fraudulent Misrepresentation  
(Against Prioritized Defendant Facebook)**

1165. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

1166. Plaintiffs assert this Claim individually and on behalf of the Class and Minor Class (for purposes of this Claim, “Plaintiffs”) under California law.

1167. Plaintiffs are entitled to a measure of damages for common law fraud under the California Civil Code for the fraud described herein.

1168. Defendant Facebook stored the personal information of Plaintiffs in its electronic and consumer information databases. Defendant falsely and knowingly represented to Plaintiffs that their personal information would remain private, and that they could control who viewed their content and

information through their privacy settings.

1169. Defendant Facebook's statements that it would maintain the privacy of Plaintiffs' content and information was false because Defendant knowingly and intentionally provided content and information to Business Partners and Whitelisted Apps, even after representing to Plaintiffs that their privacy settings could be used to control access to their content and information.

1170. Plaintiffs suffered injury in fact and lost money or property as the proximate result of Defendant's fraudulent misrepresentation. In particular, the personal information of Plaintiffs and Class members was taken and is in the hands of those who will and did use it for their own advantage, or was and is being sold for value, making it clear that the stolen information has tangible value.

1171. Plaintiffs justifiably relied on the representations Defendant Facebook made in its publicly available privacy policy and elsewhere that it would not "share information we receive about you with others unless we have: received your permission [and] given you notice."

1172. As described with specificity above, Defendant knew the falsity of its representations, and they were made with the intent to deceive Plaintiffs into supplying Facebook with private confidential personal information. Facebook's representations regarding the maintenance of user confidentiality and privacy were material to Plaintiffs' decision to provide Facebook with the personal information Facebook subsequently disclosed to Cambridge Analytica. Plaintiffs justifiably relied upon the representations of Defendant.

1173. Plaintiffs suffered harm as a proximate result of Defendant's fraudulent acts.

1174. As a result of Defendant's fraudulent misrepresentations, Plaintiffs are entitled to general damages, special damages in an amount according to proof, punitive damages, reasonable attorneys' fees and costs, and any other relief that the Court deems proper or available for common law fraud, and injunctive relief.

**Claim XXV. Negligent Misrepresentation  
(Against Prioritized Defendant Facebook)**

1175. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

1176. Plaintiffs assert this Claim individually and on behalf of the Class and Minor Class (for purposes of this Claim, “Plaintiffs”) under California law.

1177. As alleged herein, Defendant Facebook, through its agent and Chief Executive Officer, Mark Zuckerberg, repeatedly assured Plaintiffs that their content and information could be controlled by Plaintiffs through their privacy settings, and that Facebook never provided content and information to advertisers.

1178. At the time Defendant Facebook made these representations, Defendant knew or should have known that these representations were false or made them without knowledge of their truth or veracity.

1179. At minimum, Defendant Facebook negligently misrepresented and/or negligently omitted material facts concerning its commitment to privacy and the safety of user data.

1180. The negligent misrepresentations and omissions made by Defendant, upon which Plaintiffs reasonably and justifiably relied, were intended to induce reliance.

**Claim XXVI. Trespass to Personal Property  
(Against Prioritized Defendant Facebook)**

1181. Plaintiffs adopt and incorporate all the allegations of this complaint as if stated fully herein.

1182. Plaintiffs assert this Claim individually and on behalf of the Class and Minor Class (for purposes of this Claim, “Plaintiffs”).

1183. Defendant Facebook has repeatedly represented that Plaintiffs “own all of the content and information [they] post on Facebook” and could “control” access to their content and information through their “privacy settings.”

1184. Defendant Facebook, intentionally and without consent, or exceeding any consent previously obtained from users, provided Plaintiffs’ content and information to Business Partners, including device makers, and Whitelisted Apps.

1185. Defendant Facebook’s intentional and unauthorized, or exceeding any authorization previously obtained, sharing of Plaintiffs’ property, including their content and information, interfered

with Plaintiffs' and Class members' possessory interests in that property.

1186. Defendant Facebook's conduct caused Plaintiffs damage when Plaintiffs' content and information was provided to Business Partners, including device makers, and Whitelisted Apps. Facebook unjustly profited from the sharing of Plaintiffs' content and information, which deprived Plaintiffs of any income or other form of compensation Facebook generated through its unauthorized (or exceeding any authorization previously obtained) data-sharing partnerships.

**Claim XXVII. Conversion  
(Against Prioritized Defendant Facebook and Non-Prioritized Defendants Bannon and Kogan)**

1187. Plaintiffs adopt and incorporate all the allegations of this complaint as if stated fully herein.

1188. Plaintiffs assert this Claim individually and on behalf of the Class and Minor Class (for purposes of this Claim, "Plaintiffs") under California law.

1189. Plaintiffs were the owners and possessors of their content and information. As the result of Defendants' wrongful conduct, Defendants have interfered with the Plaintiffs' rights to possess and control their content and information, to which they had a superior right of possession and control at the time of conversion.

1190. As a direct and proximate result of Defendants' conduct, Plaintiffs suffered injury, damage, loss or harm and therefore seek compensatory damages.

1191. In converting Plaintiffs' private information, Defendants have acted with malice, oppression, and in conscious disregard of the Plaintiffs' and Class members' rights. Plaintiffs, therefore, seek an award of punitive damages on behalf of the class.

**Claim XXVIII. Violation of California Consumer Record Act  
(Against Prioritized Defendant Facebook)**

1192. Plaintiffs adopt and incorporate all the allegations of this complaint as if stated fully herein.

1193. Plaintiffs assert this Claim individually and on behalf of the Class and Minor Class (for purposes of this Claim, "Plaintiffs") under California law.

1194. "[T]o ensure that personal information about California residents is protected," the



California Legislature enacted California Customer Records Act. This statute states that any business that “owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.” Civil Code § 1798.81.5.

1195. Facebook is a “business” within the meaning of Civil Code § 1798.80(a).

1196. Plaintiffs are “individual[s]” within the meaning of the Civil Code § 1798.80(d). Pursuant to Civil Code § 1798.80(e), the user information is “personal information,” which includes, but is not limited to, an individual’s name, physical characteristics or description, address, telephone number, education, employment, employment history, and medical information.

1197. The breach of the personal user information of tens of millions of Facebook customers constituted a “breach of the security system” of Facebook pursuant to Civil Code § 1798.82(g).

1198. By failing to implement reasonable measures to protect its customers’ personal information, Facebook violated Civil Code § 1798.81.5.

1199. In addition, by failing to promptly notify all affected users that their personal information had been acquired (or was reasonably believed to have been acquired) by unauthorized persons, including by the Co-Conspirator Cambridge Analytica and Co-Conspirator Defendants, Facebook violated Civil Code § 1798.82. Facebook’s failure to timely and adequately notify users of the breach leaves Plaintiffs vulnerable to continued misuse of their personal information and prevents Class members from taking adequate steps to protect their identities.

1200. By violating Civil Code §§ 1798.81.5 and 1798.82, Facebook “may be enjoined” pursuant to Civil Code § 1798.84(e).

1201. Plaintiffs further request that the Court require Facebook to (1) identify and notify all members of the Class who have not yet been informed of the breach; and (2) notify affected former and current users and employees of any future data breaches by email within 24 hours of Facebook’s discovery of a breach or possible breach and by mail within 72 hours.

1202. As a result of Facebook’s violation of Civil Code §§ 1798.81.5 and 1798.82, Plaintiffs

have and will incur economic damages relating to time and money spent remedying the breach, including, but not limited to, monitoring their online presence to ensure that their identity has not been stolen or coopted for an illicit purpose, any unauthorized charges made on financial accounts, lack of access to funds while banks issue new cards, tax fraud, as well as the costs of credit monitoring and purchasing credit reports.

1203. Plaintiffs seek all remedies available under Civil Code § 1798.84, including, but not limited to: (a) damages suffered by members of the Class; and (b) equitable relief.

1204. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law including California Code of Civil Procedure § 1021.5 and Federal Rule of Civil Procedure 23.

**Claim XXIX. Violation of California Invasion of Privacy Act (Cal. Pen. Code § 637.7)  
(Against Prioritized Defendant Facebook)**

1205. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

1206. Plaintiffs assert this Claim individually and on behalf of the Class and Minor Class (for purposes of this Claim, "Plaintiffs") under California law.

1207. Plaintiffs allege against all Defendants violations of the California Invasion of Privacy Act ("CIPA"), specifically California Penal Code § 637.7, for the unlawful acquisition of Plaintiffs' and Class members' user information without their consent.

1208. California Penal Code § 630 provides that "The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society."

1209. Defendants' acts in violation of the CIPA occurred in the State of California because those acts resulted from business decisions, practices, and operating policies that Facebook developed, implemented, and utilized in the State of California and which are unlawful and constitute criminal conduct in the state of Facebook's residence and principal business operations. Further, the data

acquired from Facebook by Cambridge Analytica was housed on Facebook’s servers in California and obtained therefrom. Facebook’s implementation of its business decisions, practices, and standard ongoing policies that violate CIPA—and Cambridge Analytica’s avilment of those business decisions, practices, and standard ongoing policies—took place and continue to take place in the State of California. Defendants profited and continue to profit in the State of California as a result of these repeated and systemic violations of CIPA. Defendants’ unlawful conduct, which occurred in the State of California, harmed and continues to harm Plaintiffs.

1210. Among the data points harvested by Facebook and provided to the remaining Defendants (as well as Business Partners, App Developers, and Whitelisted Apps) was Plaintiffs’ location.

1211. CIPA expressly prohibits the use of “an electronic tracking device to determine the location or movement of a person.” Cal. Pen. Code § 637.7(a).

1212. As defined under CIPA, “‘electronic tracking device’ means any device attached to a vehicle or other movable thing that reveals its location or movement by the transmission of electronic signals.” *Id.* § 637.7(d).

1213. Facebook acquired—and Cambridge Analytica exfiltrated and used—Plaintiffs’ location through, inter alia, location data associated with smartphones and other mobile devices running Facebook.

1214. Plaintiffs did not consent to said acquisition of location information by any Defendant.

**Claim XXX. Violation of the California Consumers Legal Remedies Act  
(Against Prioritized Defendant Facebook)**

1215. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

1216. Plaintiffs assert this Claim individually and on behalf of the Class and Minor Class (for purposes of this Claim, “Plaintiffs”) under California law.

1217. Facebook is a “person” within the meaning of CLRA in that it is a corporation.

1218. Plaintiffs are “consumers” within the meaning of CLRA in that they are individuals who seek or acquire services for personal, family, or household purposes.

1219. CLRA § 1770(a)(5) prohibits “[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have or that a person has a sponsorship, approval, status, affiliation, or connection which he or she does not have.”

1220. CLRA § 1770(a)(14) prohibits “[r]epresenting that a transaction confers or involves rights, remedies, or obligations that it does not have or involve, or that are prohibited by law.”

1221. Defendant Facebook’s conduct as alleged herein violates CLRA’s ban of proscribed practices at Cal. Civ. Code § 1770(a) subdivisions (5) and (14) in that, *inter alia*, Facebook misrepresented its services by not disclosing that it provides content and information to Business Partners, device makers, and Whitelisted Apps, when it tells Plaintiffs that they can “control” access with their “privacy settings.” The privacy and control over personal property involved with Facebook’s services were illusory. With respect to Whitelisted Apps, Facebook collected revenue for the continued access to Plaintiffs’ content and information and did not disclose that it was doing so.

1222. Plaintiffs and suffered injuries caused by Defendant’s misrepresentations and omissions because: (a) Plaintiffs suffered an invasion of their privacy as a result of Facebook exposing their content and information to Business Partners, device makers, and Whitelisted Apps, and (b) were deprived of any income Facebook generated through its unauthorized use or sale of data.

1223. Prior to the filing of this Complaint, a CLRA notice letter was sent to Defendant Facebook which complies in all respects with California Civil Code § 1782(a).

1224. Plaintiffs seek equitable relief for Facebook’s violation of CLRA, as permitted by statute. This includes injunctive relief to enjoin the wrongful practices alleged herein, and to take corrective action to remedy past conduct, including ending all data-sharing partnerships still in effect and having Facebook direct all device makers, Business Partners, and Whitelisted Apps with Plaintiffs’ data stored on their servers to delete that data.

**Claim XXXI. Violation of California’s Computer Data Access and Fraud Act  
(Against Prioritized Defendant Facebook)**

1225. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

1226. Plaintiffs assert this Claim individually and on behalf of the Class and Minor Class (for purposes of this Claim, “Plaintiffs”) under California law.

1227. Facebook knowingly accessed and without permission used Plaintiffs’ content and information in order to wrongfully control or obtain property or data in violation of California Penal Code § 502(c)(1).

1228. Facebook knowingly accessed and without permission took, copied, and/or used data from Plaintiffs’ computers, computer systems and/or computer network in violation of California Penal Code § 502(c)(2).

1229. Facebook knowingly and without permission used or caused to be used Plaintiffs’ computer services in violation of California Penal Code § 502(c)(3).

1230. Facebook knowingly and without permission accessed or caused to be accessed Plaintiffs’ computers, computer systems, and/or computer network in violation of California Penal Code § 502(c)(7).

1231. Plaintiffs suffered and continue to suffer damage as a result of Facebook’s violations of the California Penal Code § 502 identified above.

1232. Facebook’s conduct also caused irreparable and incalculable harm and injuries to Plaintiffs in the form of invading their privacy, and, unless enjoined, will cause further irreparable and incalculable injury, for which Plaintiffs have no adequate remedy at law.

1233. Facebook willfully violated California Penal Code § 502 in disregard and derogation of the rights of Plaintiffs, and Facebook’s actions as alleged above were carried out with oppression, fraud and malice.

1234. Pursuant to California Penal Code § 502(e), Plaintiffs are entitled to injunctive relief, compensatory damages, punitive or exemplary damages, attorneys’ fees, costs and other equitable relief.

**Claim XXXII. Violations of Common Law Right to Privacy in the Following States: Alabama; Arizona; Colorado; Florida; Georgia; Idaho; Indiana; Iowa; Kansas; Maryland; Michigan; Missouri; Ohio; Oklahoma; Pennsylvania; Tennessee; Texas; Washington; West Virginia; and Wisconsin  
(Against Prioritized Defendant Facebook)**

1235. Plaintiffs Akins, Ariciu, Armstrong, Burk, Fischer, Forman, Holsinger, King, Short,

Senko, Schinder, Smith, Tutt, and Wenz, individually and on behalf of the Alabama, Arizona, Colorado; Florida; Georgia; Idaho; Indiana; Iowa; Kansas; Maryland; Michigan; Missouri; Ohio; Oklahoma; Pennsylvania; Tennessee; Texas; Washington; West Virginia; and Wisconsin Sub Classes (for purposes of this claim, “Plaintiffs”) incorporate by reference all allegations of this complaint as though fully set forth herein.

1236. The common law in these states prohibits the use of a person’s name or likeness for the defendant’s advantage, commercial or otherwise, without first obtaining that person’s consent, or where appropriate the consent of that person’s parent or legal guardian.

1237. Facebook violated this section by allowing access to Plaintiffs’ likeness—including names, like history, private messages, photographs, and video—as a service to third parties without consent. On information and belief, access to the likeness of Plaintiffs was integral to the services Facebook offered App Developers like Cambridge Analytica, as well as Business Partners and Whitelisted Apps. Whitelisted Apps and other Business Partners would not have purchased services from Facebook (including advertisements) without access to Plaintiffs’ content and information.

1238. Prior to using the Plaintiffs’ likeness, Facebook never obtained consent.

1239. Plaintiffs did not receive any compensation in return for this use

1240. Plaintiffs were harmed by Facebook’s improper use.

1241. Plaintiffs seek actual damages suffered, plus any profits attributable to Facebook’s use of the unauthorized use not calculated in actual damages. Plaintiffs and class members also reserve the right to punitive damages, costs, and reasonable attorney’s fees as allowed under this statute.

Claim XXXIII. **Violations of Alabama Right of Publicity Statute,  
Ala. Code § 6-5-772  
(Against Prioritized Defendant Facebook)**

1242. Plaintiff Smith, individually and on behalf of the Alabama Subclass (“Plaintiffs,” for purposes of this Claim), incorporates by reference all allegations of this complaint as though fully set forth herein.

1243. Ala. Code § 6-5-772 prohibits the use of a person’s indicia of identity for the purposes of advertising or selling or soliciting goods or services without that persons’ consent, or where appropriate

the consent of that person's parent or legal guardian.

1244. Under Ala. Code § 6-5-771, indicia of identity include those attributes of a person that serve to identify that person to an ordinary, reasonable viewer or listener and includes "name, signature, photograph, image, likeness, voice" or similar attribute of that person.

1245. Defendant violated this section by allowing access to Plaintiffs' content and information—including names, like history, private messages, photographs, and video—as a service to third parties. On information and belief, the content and information of Plaintiffs was integral to the services Facebook offered App Developers like Cambridge Analytica and Whitelisted Apps. Whitelisted Apps would not have purchased services from Facebook (including advertisements) without access to this content and information. Indeed, the value of the services Facebook offered to Whitelisted Apps was derived from this content and information. Thus, Facebook directly benefited from this use of Plaintiffs' content and information.

1246. Prior to using the Plaintiffs' content and information, Defendant never obtained consent from the Plaintiffs.

1247. Defendant profited from the commercial use of the Plaintiffs' content and information.

1248. Plaintiffs did not receive any compensation in return for this use.

1249. According to Ala. Code § 6-5-774, Plaintiffs seek the greater of \$5,000 per incident or the actual damages suffered, plus any profits attributable to Defendants' use of the unauthorized use not calculated in actual damages. Plaintiffs also reserve the right to injunctive relief, punitive damages, costs, and reasonable attorney's fees as allowed under this statute.

**Claim XXXIV.        Violations of Florida Unauthorized Publication Statute,  
Fla. State Code § 540.08  
(Against Prioritized Defendant Facebook)**

1250. Plaintiffs Bridgett Burk, Tyler King, and Annie Wenz, individually and on behalf of the Florida Subclass ("Plaintiffs," for purposes of this Claim), incorporate by reference all allegations of this complaint as though fully set forth herein.

1251. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.



1252. Fla. Code § 540.08 prohibits the use of a person’s name, portrait, photograph, or likeness for commercial purposes without the express consent of that person, or where appropriate the consent of that person’s parent or legal guardian.

1253. Defendant Facebook violated this section by allowing access to Plaintiffs’ content and information—including names, like history, private messages, photographs, and video—as a service to third parties. On information and belief, the content and information of Plaintiffs was integral to the services Facebook offered third party App Developers like Cambridge Analytica and Whitelisted Apps. Whitelisted Apps would not have purchased services from Facebook (including advertisements) without access to this content and information. Indeed, the value of the services Facebook offered to Whitelisted Apps was derived from this content and information. Thus, Facebook directly benefited from this use of Plaintiffs’ content and information.

1254. Prior to using the Plaintiffs’ content and information, Defendant never obtained consent.

1255. Defendant profited from the commercial use of the Plaintiffs’ likenesses.

1256. Plaintiffs did not receive any compensation in return for this use.

1257. According to Fla. Code § 540.08, Plaintiffs seek the greater of \$1,000 per incident in addition to any other remedies under common law, including actual damages, punitive damages, and injunctive relief.

**Claim XXXV. Violations of Illinois Right of Publicity Statute,  
Ill. Comp. Stat. § 1075/10  
(Against Prioritized Defendant Facebook)**

1258. Plaintiff Kimberly Robertson, individually and on behalf of the Illinois Subclass (“Plaintiffs,” for purposes of this Claim), incorporates by reference all allegations of this complaint as though fully set forth herein.

1259. Ill. Comp. Stat. § 1075/5-30 prohibits the use of an individual’s likeness including their name, signature, photograph, image, likeness, or voice for or in connection with a sale of a product or services or for purposes of advertising or promoting services without written consent of that person, or where appropriate the consent of that person’s parent or legal guardian.

1260. Defendant Facebook violated this section by allowing access to Plaintiffs’ content and

information—including names, like history, private messages, photographs, and video—as a service to third parties. On information and belief, the content and information of Plaintiffs was integral to the services Facebook offered third party App Developers like Cambridge Analytica and Whitelisted Apps. Whitelisted Apps would not have purchased services from Facebook (including advertisements) without access to this content and information. Indeed, the value of the services Facebook offered to Whitelisted Apps was derived from this content and information. Thus, Facebook directly benefited from this use of Plaintiffs’ content and information.

1261. Prior to using the Plaintiffs’ content and information, Defendant never obtained consent from the Plaintiffs.

1262. Defendant profited from the commercial use of the Plaintiffs’ likenesses.

1263. Plaintiffs did not receive any compensation in return for this use.

1264. According to Ill. Comp. Stat. § 1075/40-60, Plaintiffs seek the greater of \$1,000 per incident or the actual damages suffered, plus any profits attributable to Defendants’ use of the unauthorized use not calculated in actual damages. Plaintiffs also reserve the right to punitive damages, costs, and reasonable attorney’s fees as allowed under this statute.

**Claim XXXVI. Violations of Indiana Rights of Publicity Code,  
Ind. Code § 32-36-1-8  
(Against Prioritized Defendant Facebook)**

1265. Plaintiff Samuel Armstrong, individually and on behalf of the Indiana Subclass (“Plaintiffs,” for purposes of this Claim), incorporate by reference all allegations of this complaint as though fully set forth herein.

1266. Ind. Code § 32-36-1-8 prohibits the use of a person’s name, voice, signature, photograph, image, likeness, distinctive appearance, gesture, or mannerisms in connection with a product service or commercial activity without that person’s consent, or where appropriate the consent of that person’s parent or legal guardian.

1267. Defendant Facebook violated this section by allowing access to Plaintiffs’ content and information—including names, like history, private messages, photographs, and video—as a service to third parties. On information and belief, Plaintiffs’ content and information was integral to the services

Facebook offered third party App Developers like Cambridge Analytica and Whitelisted Apps.

Whitelisted Apps would not have purchased services from Facebook (including advertisements) without access to this content and information. Indeed, the value of the services Facebook offered to Whitelisted Apps was derived from this content and information. Thus, Facebook directly benefited from this use of Plaintiffs' content and information.

1268. Prior to using the Plaintiffs' content and information, Defendant never obtained consent.

1269. Defendant profited from the commercial use of the Plaintiffs' likenesses.

1270. Plaintiffs did not receive any compensation in return for this use.

1271. According to Ind. Code § 32-36-1-10 Plaintiffs seek the greater of \$1,000 per incident or the actual damages suffered, plus any profits attributable to Defendants' use of the unauthorized use not calculated in actual damages. Plaintiffs reserve the right to injunctive relief, punitive damages, costs, and reasonable attorney's fees as allowed under this statute.

**Claim XXXVII.      Violations of New York Right to Privacy Statute,  
N.Y. Civ. Rights Law § 51  
(Against Prioritized Defendant Facebook)**

1272. Plaintiff William Lloyd, individually and on behalf of the New York Subclass ("Plaintiffs," for purposes of this Claim), incorporate by reference all allegations of this complaint as though fully set forth herein.

1273. N.Y. Civ. Rights Law § 51 prohibits the use of a person's name, portrait, picture, or voice for advertising purposes or for the purposes of trade without first obtaining that person's consent, or where appropriate the consent of that person's parent or legal guardian.

1274. Defendant Facebook violated this section by allowing access to Plaintiffs' content and information—including names, like history, private messages, photographs, and video—as a service to third parties. On information and belief, the content and information of Plaintiffs was integral to the services Facebook offered third party App Developers like Cambridge Analytica and Whitelisted Apps. Whitelisted Apps would not have purchased services from Facebook (including advertisements) without access to this content and information. Indeed, the value of the services Facebook offered to Whitelisted Apps was derived from this content and information. Thus, Facebook directly benefited from this use of

Plaintiffs' content and information.

1275. Prior to using the Plaintiffs' content and information, Defendant never obtained consent.

1276. Defendant profited from the commercial use of Plaintiffs' likenesses.

1277. Plaintiffs did not receive any compensation in return for this use.

1278. According to N.Y. Civ. Rights Law § 51, to Plaintiffs seek actual damages suffered, plus any profits attributable to Defendants' use of the unauthorized use not calculated in actual damages. Plaintiffs also reserve the right to equitable relief, punitive damages, costs, and reasonable attorney's fees as allowed under this statute.

**Claim XXXVIII.      Violations of Ohio Right of Publicity Statute,  
Ohio Code § 2741.02  
(Against Prioritized Defendant Facebook)**

1279. Plaintiff Cheryl Senko, individually and on behalf of the Ohio Subclass ("Plaintiffs," for purposes of this Claim), incorporate by reference all allegations of this complaint as though fully set forth herein.

1280. Ohio Code § 2741.02 prohibits the use of a person's name, voice, signature, photograph, image, likeness, or distinctive appearance in connection with a product, good or service with that person's written consent, or where appropriate the consent of that person's parent or legal guardian.

1281. Defendant Facebook violated this section by allowing access to Plaintiffs' content and information—including names, like history, private messages, photographs, and video—as a service to third parties. On information and belief, Plaintiffs' content and information was integral to the services Facebook offered third party App Developers like Cambridge Analytica and Whitelisted Apps. Whitelisted Apps would not have purchased services from Facebook (including advertisements) without access to this content and information. Indeed, the value of the services Facebook offered to Whitelisted Apps was derived from this content and information. Thus, Facebook directly benefited from this use of Plaintiffs' content and information.

1282. Prior to using Plaintiffs' content and information, Defendant never obtained consent.

1283. Defendant profited from the commercial use of Plaintiffs' likenesses.

1284. Plaintiffs did not receive any compensation in return for this use.

1285. According to Ohio Code § 2741.07 (a), Plaintiffs seek the greater of \$2,500 per incident or the actual damages suffered, plus any profits attributable to Defendants' use of the unauthorized use not calculated in actual damages. Plaintiffs also reserve the right to punitive damages, costs, and reasonable attorney's fees as allowed under this statute.

Claim XXXIX. **Violations of Oklahoma Rights of Publicity Statute,  
Okl. St. § 1449  
(Against Prioritized Defendant Facebook)**

1286. On behalf of the Oklahoma Subclass ("Plaintiffs," for purposes of this Claim), Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

1287. Okl. St. § 1449 prohibits the use of a person's name, voice, signature, photograph, or likeness in connection with a product, good or service with that person's written consent, or where appropriate the consent of that person's parent or legal guardian.

1288. Defendant Facebook violated this section by allowing access to Plaintiffs' content and information—including names, like history, private messages, photographs, and video—as a service to third parties. On information and belief, Plaintiffs' content and information was integral to the services Facebook offered third party App Developers like Cambridge Analytica and Whitelisted Apps. Whitelisted Apps would not have purchased services from Facebook (including advertisements) without access to this content and information. Indeed, the value of the services Facebook offered to Whitelisted Apps was derived from this content and information. Thus, Facebook directly benefited from this use of Plaintiffs' content and information.

1289. Prior to using Plaintiffs' content and information, Defendant never obtained consent.

1290. Defendant profited from the commercial use of Plaintiffs' likenesses.

1291. Plaintiffs did not receive any compensation in return for this use.

1292. According to Okl. St. § 1449, Plaintiffs seek the actual damages suffered, including any profits attributable to Defendants' use of the unauthorized use. Plaintiffs also reserve the right to punitive damages, costs, and reasonable attorney's fees as allowed under this statute.

Claim XL. **Violations of Pennsylvania Unauthorized Use Statute, 42 Pa. Stat. § 8316  
(Against Prioritized Defendant Facebook)**

1293. On behalf of the Pennsylvania Subclass (“Plaintiffs,” for purposes of this Claim), Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

1294. 42 Pa. Stat. § 8316 prohibits the use of a person’s name or likeness in connection the sale of a product, goods or services without first obtaining that person’s written consent, or where appropriate the consent of that person’s parent or legal guardian.

1295. Defendant Facebook violated this section by allowing access to Plaintiffs’ content and information—including names, like history, private messages, photographs, and video—as a service to third parties. On information and belief, Plaintiffs’ content and information was integral to the services Facebook offered third party App Developers like Cambridge Analytica and Whitelisted Apps. Whitelisted Apps would not have purchased services from Facebook (including advertisements) without access to this content and information. Indeed, the value of the services Facebook offered to Whitelisted Apps was derived from this content and information. Thus, Facebook directly benefited from this use of Plaintiffs’ content and information.

1296. Prior to using Plaintiffs’ content and information, Defendant never obtained consent.

1297. Defendant profited from the commercial use of Plaintiffs’ likenesses.

1298. Plaintiffs did not receive any compensation in return for this use.

1299. Under 42 Pa. Stat. § 8316.1, Plaintiffs seek actual damages plus any profits attributable to Defendants’ use of the unauthorized use not calculated in actual damages. Plaintiffs also reserve the right to injunctive relief as allowed under this statute.

**Claim XLI. Violations of Tennessee Protection of Personal Rights Statute  
T.C.A. § 47-25-1105  
(Against Prioritized Defendant Facebook)**

1300. Plaintiff Steve Akins, individually and on behalf of the Tennessee Subclass (“Plaintiffs,” for purposes of this Claim), incorporates by reference all allegations of this complaint as though fully set forth herein.

1301. T. C. A. § 47-25-1105 prohibits the use of a person’s name, photograph, or likeness on or in goods, merchandise, or products entered into commerce in that state without first obtaining that person’s consent, or where appropriate the consent of that person’s parent or legal guardian.

1302. Defendant Facebook violated this section by allowing access to Plaintiffs' content and information—including names, like history, private messages, photographs, and video—as a service to third parties. On information and belief, Plaintiffs' content and information was integral to the services Facebook offered third party App Developers like Cambridge Analytica and Whitelisted Apps. Whitelisted Apps would not have purchased services from Facebook (including advertisements) without access to this content and information. Indeed, the value of the services Facebook offered to Whitelisted Apps was derived from this content and information. Thus, Facebook directly benefited from this use of Plaintiffs' content and information.

1303. Prior to using Plaintiffs' content and information, Defendant never obtained consent.

1304. Defendant profited from the commercial use of Plaintiffs' likenesses.

1305. Plaintiffs did not receive any compensation in return for this use.

1306. According to T. C. A. § 47-25-1105, Plaintiffs seek the greater of \$5,000 per incident or the actual damages suffered, plus any profits attributable to Defendants' use of the unauthorized use not calculated in actual damages. Plaintiffs also reserve the right to punitive damages, costs, reasonable attorney's fees, and injunctive relief as allowed under this statute.

**Claim XLII. Violations of Virginia Unauthorized Use Statute,  
Va. Code § 8.01-40  
(Against Prioritized Defendant Facebook)**

1307. On behalf of the Virginia Subclass ("Plaintiffs," for purposes of this Claim), incorporates by reference all allegations of this complaint as though fully set forth herein.

1308. Va. Code § 8.01-40 prohibits the use of a person's name, portrait or picture for commercial purposes without first obtaining that person's consent, or where appropriate the consent of that person's parent or legal guardian.

1309. Defendant Facebook violated this section by allowing access to Plaintiffs' content and information—including names, like history, private messages, photographs, and video—as a service to third parties. On information and belief, Plaintiffs' content and information was integral to the services Facebook offered third party App Developers like Cambridge Analytica and Whitelisted Apps. Whitelisted Apps would not have purchased services from Facebook (including advertisements) without



access to this content and information. Indeed, the value of the services Facebook offered to Whitelisted Apps was derived from this content and information. Thus, Facebook directly benefited from this use of Plaintiffs' content and information.

1310. Prior to using Plaintiffs' content and information, Defendant never obtained consent.

1311. Defendant profited from the commercial use of Plaintiffs' likenesses.

1312. Plaintiffs did not receive any compensation in return for this use.

1313. According to Va. Code § 8.01-40, Plaintiffs seek actual damages suffered, plus any profits attributable to Defendants' use of the unauthorized use not calculated in actual damages.

Plaintiffs also reserve the right to punitive damages, costs, and reasonable attorney's fees as allowed under this statute.

**Claim XLIII. Violations of Washington Personality Right Statue,  
Wash. Code § 63.60.050  
(Against Prioritized Defendant Facebook)**

1314. Plaintiff Terry Fischer, individually and on behalf of the Washington Subclass ("Plaintiffs," for purposes of this Claim), incorporate by reference all allegations of this complaint as though fully set forth herein.

1315. Wash. Code § 63.60.050 prohibits the use of a person's name, voice, signature, photograph, or likeness on or in goods, merchandise, or products entered into commerce in that state without first obtaining that person's consent, or where appropriate the consent of that person's parent or legal guardian.

1316. Defendant Facebook violated this section by allowing access to Plaintiffs' content and information—including names, like history, private messages, photographs, and video—as a service to third parties. On information and belief, Plaintiffs' content and information was integral to the services Facebook offered third party App Developers like Cambridge Analytica and Whitelisted Apps. Whitelisted Apps would not have purchased services from Facebook (including advertisements) without access to this content and information. Indeed, the value of the services Facebook offered to Whitelisted Apps was derived from this content and information. Thus, Facebook directly benefited from this use of Plaintiffs' content and information.

1317. Prior to using Plaintiffs' content and information, Defendant never obtained consent.

1318. Defendant profited from the commercial use of Plaintiffs' likenesses.

1319. Plaintiffs did not receive any compensation in return for this use.

1320. According to Wash. Code § 63.60.060 Plaintiffs seek the greater of \$1,500 per incident or the actual damages suffered, plus any profits attributable to Defendants' use of the unauthorized use not calculated in actual damages. Plaintiffs also reserve the right to costs, and reasonable attorney's fees as allowed under this statute.

**Claim XLIV. Violations of Wisconsin Right of Publicity Statute,  
Wis. Stat. § 995.50  
(Against Prioritized Defendant Facebook)**

1321. On behalf of the Wisconsin Subclass ("Plaintiffs," for purposes of this Claim), Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

1322. Wis. Stat. § 995.50(b) prohibits the use of a name, portrait or picture for the purposes of trade or advertising without first obtaining that person's consent, or where appropriate the consent of that person's parent or legal guardian.

1323. Defendant Facebook violated this section by allowing access to Plaintiffs' content and information—including names, like history, private messages, photographs, and video—as a service to third parties. On information and belief, Plaintiffs' content and information was integral to the services Facebook offered third party App Developers like Cambridge Analytica and Whitelisted Apps. Whitelisted Apps would not have purchased services from Facebook (including advertisements) without access to this content and information. Indeed, the value of the services Facebook offered to Whitelisted Apps was derived from this content and information. Thus, Facebook directly benefited from this use of Plaintiffs' content and information.

1324. Prior to using Plaintiffs' content and information, Defendant never obtained consent.

1325. Defendant profited from the commercial use of Plaintiffs' likenesses.

1326. Plaintiffs did not receive any compensation in return for this use.

1327. According to Wis. Stat. § 995.50, Plaintiffs seek actual damages, plus any profits attributable to Defendants' use of the unauthorized use not calculated in actual damages. Plaintiffs and

Wisconsin Subclass members also reserve the right to costs, reasonable attorney's fees, and injunctive relief as allowed under this statute.

**Claim XLV. Violations of California Right of Publicity Statute,  
Cal. Civil Code § 3344  
(Against Prioritized Defendant Facebook; Non-Prioritized Defendants Bannon and Kogan)  
On Behalf of All Plaintiffs and Classes**

1328. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

1329. Plaintiffs assert this Claim individually and on behalf of the Class and Minor Class (for purposes of this Claim, "Plaintiffs") under California law. California Civil Code § 3344 prohibits the knowing use of a person's name, voice, signature, photograph, or likeness for a commercial gain without first obtaining that person's consent, or where appropriate the consent of that person's parent or legal guardian.

1330. Defendants violated this section by allowing access to Plaintiffs' and Class Members' content and information—including names, like history, private messages, photographs, and video—as a service to third parties. On information and belief, the content and information of Plaintiffs and Class Members was integral to the services Facebook offered App Developers like Cambridge Analytica and Whitelisted Apps. Whitelisted Apps would not have purchased services from Facebook (including advertisements) without access to this content and information. Indeed, the value of the services Facebook offered to Whitelisted Apps was derived from this content and information. Thus, Facebook directly benefited from this use of Plaintiffs' content and information.

1331. Facebooks' API feeds are "products" for purposes of Civil Code Section 3344. Additionally, Facebook used its API feeds to advertise for services Facebook offered, such as advertisements and other means of obtaining revenue from Whitelisted Apps. Facebook effectively used access to API feeds containing photographs and likenesses of Plaintiffs and Class Members to sell its advertising services.

1332. The likenesses exploited by Facebook through API feeds include photographs and videos. Facebook offered these photographs and likenesses to third party App Developers and other Business

Partners as part of the API service without regard to Plaintiffs' privacy settings, or the privacy designation attached to the photographs and videos. Facebook received substantial revenue from publishing this content and information through its API feed in the form of advertising revenue. Facebook linked the payment of advertisements with the continued access to API feeds that included photographs and likenesses of Plaintiffs and Class Members.

1333. Prior to using the Plaintiffs' content and information, the Facebook never obtained consent from the Plaintiffs.

1334. Plaintiffs received no compensation for the use of their likeness.

1335. Facebook had knowledge of the unauthorized uses of Plaintiffs' and Class Members' names, photographs, and likenesses.

1336. Plaintiffs were harmed by Facebook's improper use.

1337. According to California Civil Code § 3344(a), Plaintiffs seek the greater of \$750 per incident or the actual damages suffered, plus any profits attributable to Facebook's use of the unauthorized use not calculated in actual damages. Plaintiffs also reserve the right to punitive damages, costs, and reasonable attorney's fees as allowed under this statute.

**Claim XLVI. Violations of the Fair Credit Reporting Act**  
**15 U.S.C. §§ 1681 *et seq.***  
**(Against Prioritized Defendant Facebook)**  
**On Behalf of All Plaintiffs and Classes**

1338. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

1339. Plaintiffs assert this Claim individually and on behalf of the Class and Minor Class (for purposes of this Claim, "Plaintiffs").

1340. As individuals, Plaintiffs are consumers entitled to the protections of the FCRA. 15 U.S.C. § 1681a(c).

1341. Facebook is a "person" as defined by 15 U.S.C. § 1681a(b).

1342. Facebook is a CRA—a "consumer reporting agency" as defined in 15 U.S.C. §§ 1681a(f) which is defined as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis,

regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties . . . .” 15 U.S.C. § 1681a(f).

1343. The compromised data was a “consumer report” under the FCRA as defined under 15 U.S.C. § 1681a(d)(1).

1344. As a consumer reporting agency, Facebook may only furnish a consumer report under the limited circumstances set forth in 15 U.S.C. § 1681b, “and no other.” 15 U.S.C. § 1681b(a). None of the purposes listed under 15 U.S.C. § 1681b permit credit reporting agencies to furnish consumer reports to unauthorized or unknown entities.

1345. Facebook willfully and/or recklessly violated § 1681b and § 1681e(a) by providing impermissible access to consumer reports and by failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA.

1346. As a CRA, Facebook is required to make clear, accurate, and complete disclosures as set forth in 15 § U.S.C. 1681g.

1347. Facebook failed to make clear, accurate, and complete disclosures, violating 15 U.S.C. § 1681g.

1348. As a result of each and every willful violation of FCRA, Plaintiffs are entitled to: actual damages, pursuant to 15 U.S.C. § 1681n(a)(1); statutory damages, pursuant to 15 U.S.C. § 1681n(a)(1); punitive damages, as this Court may allow, pursuant to 15 U.S.C. § 1681n(a)(2); and reasonable attorneys’ fees and costs pursuant to 15 U.S.C. § 1681n(a)(3).

1349. As a result of each and every negligent non-compliance of the FCRA, Plaintiffs and Class members are also entitled to actual damages, pursuant to 15 U.S.C. § 1681o(a)(1); and reasonable attorney’s fees and costs pursuant to 15 U.S.C. § 1681o(a)(2) from Defendant.

**Claim XLVII. Unlawful Interception of Communications,  
11 Del. Code § 2401  
(Against Prioritized Defendant Facebook and Non-Prioritized Defendant Kogan)**

1350. Plaintiffs adopt and incorporate all the allegations of this complaint as if stated fully herein.

1351. Plaintiffs assert this Claim on behalf of the Delaware Subclass.

1352. By reason of the conduct alleged herein, Defendants violated Delaware's Criminal Code protecting persons from electronic surveillance and unlawful interception of communications.

1353. According to Chapter 24 of the Title 11 of the Delaware Criminal Code, "Electronic communication" includes "any transfer of signs, signals, writing, images, sounds, data or intelligence of any electromagnetic, photoelectronic or photooptical system." 11 Del. Code § 2401.

1354. The messages, posts, images and countless other forms of communication on Facebook user's profiles are considered electronic communications.

1355. The statute defines "Electronic communication system" as "any wire, oral, electromagnetic, photooptical, or photoelectronic facilities for the transmission of wire, oral or electronic communications and any computer facilities or related electronic equipment." *Id.*

1356. The servers Facebook uses to provide its electronic communication service which facilitate user communication are considered an "electronic communication system".

1357. Delaware prohibits the intentional interception of any wire, oral or electronic communication unless party to the communication or with prior consent by one of the parties to the communication. 11 Del. Code § 2402(a).

1358. Delaware also prohibits a person or entity providing an electronic communications service to the public from knowingly divulging to any other person or entity the contents of a communication while the communication is in electronic storage by that service. 11 Del. Code § 2422.

1359. Facebook, a "person" and "electronic communication service" pursuant to Delaware Criminal Code, unlawfully and intentionally divulged the contents of Plaintiffs' communications.

1360. Facebook intentionally divulged the contents of Plaintiffs' stored electronic communications by allowing Cambridge Analytica access to their electronic communications which also contained sensitive personal information and identifiers putting Plaintiffs and Class members at risk of being harmed.

1361. Section 2409 of the Delaware Criminal Code authorizes a private right of action for actual damages, punitive damages and reasonable attorneys' fees and other litigation costs reasonably

incurred to any person whose wire, oral or electronic communication is intercepted, disclosed or used in violation of this code.

1362. Plaintiffs have been harmed by Defendants' misconduct and are entitled to actual damages, punitive damages and reasonable attorneys' fees and costs.

**Claim XLVIII. Violation of New Jersey Consumer Fraud Act,  
N.J. Stat. Ann. §§ 56:8-1 et seq.  
(Against Prioritized Defendant Facebook)**

1363. Plaintiffs incorporate by reference the allegations in the preceding paragraphs as if fully set forth herein.

1364. Defendants and Plaintiffs are "persons" within the meaning of N.J. STAT. ANN. § 56:8-1(d). Facebook engaged in "sales" of "merchandise" within the meaning of N.J. STAT. ANN. § 56:8-1(c), (d).

1365. The New Jersey Consumer Fraud Act ("New Jersey CFA") makes unlawful "[t]he act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing concealment, suppression or omission of any material fact with the intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby..." N.J. STAT. ANN. § 56:8-2.

1366. As set forth above, Facebook, while operating in New Jersey, engaged, in unconscionable commercial practices, deception, misrepresentation, and the knowing concealment, suppression, and omission of material facts with intent that others rely on such concealment, suppression, and omission, in connection with the sale and advertisement of services, in violation of N.J. Stat. Ann. § 56:8-2. This includes:

- A. Collecting, storing, and using vast quantities of highly sensitive personal information and which Facebook failed to adequately protect from unauthorized and/or criminal access;
- B. Failing to employ technology and systems to promptly detect unauthorized access



to the personal information with which they were entrusted;

C. Unreasonably delaying giving notice to consumers after it became aware of unauthorized access to the personal information;

D. Knowingly and fraudulently failing to provide accurate, timely information to consumers about the extent to which their personal information had been compromised; and

E. Making false and deceptive representations and communications concerning the purpose of and reasons for collecting highly sensitive personal information.

1367. Facebook's breach of its duties has directly and proximately caused Plaintiffs to suffer an ascertainable loss of money and property, including the loss of their personal information and foreseeably causing them to expend time and resources investigating the extent to which their personal information has been compromised.

1368. The above unlawful and deceptive acts and practices and acts by Facebook were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs that they could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

1369. Plaintiffs seek relief under N.J. Stat. Ann. § 56:8-19, including, but not limited to, injunctive relief, other equitable actual damages (to be proven at trial), disgorgement of wrongfully obtained profits, treble damages, and attorneys' fees and costs.

**Claim XLIX. Intentional Misrepresentation  
(Against Prioritized Defendant Facebook)  
On Behalf of All Plaintiffs and Classes**

1370. Plaintiffs reallege and incorporate by reference all allegations of this complaint as though fully set forth herein.

1371. Plaintiffs assert this Claim individually and on behalf of the Class and Minor Class (for purposes of this Claim, "Plaintiffs") under California law.

1372. Facebook falsely and knowingly represented to Plaintiffs that their personal information would remain private, and that they could control who viewed their content and information through their privacy settings.

1373. Defendant Facebook's statements that it would maintain the privacy of Plaintiffs' content and information was false because Defendant knowingly and intentionally provided content and information to Business Partners and Whitelisted Apps, even after representing to Plaintiffs that their privacy settings could be used to control access to their content and information.

1374. Facebook's representations were material to Plaintiffs' decision to provide content and information to Facebook.

1375. Plaintiffs justifiably relied on the representations Facebook made concerning "control" of content and information and the efficacy of Facebook's "privacy settings" and acted in reliance on those representations by using Facebook.

1376. Facebook knew of the falsity of its representations, and its representations were made to deceive Plaintiffs.

1377. Facebook knew it did not have permission to allow Business Partners and Whitelisted Apps to use Plaintiffs' content and information.

1378. Plaintiffs suffered injury-in-fact and lost property as a proximate result of Facebook's intentional misrepresentation.

1379. As a direct and proximate result of Facebook's intentional misrepresentation, Plaintiffs suffered injuries, damages, losses or harm, including but not limited to annoyance, interference, concern, lost time, the loss of personal property, and the need for the cost of effective credit and privacy security, justifying an award of compensatory and punitive damages.

## **X. PRAYER FOR RELIEF**

1380. Plaintiffs, individually and on behalf of Class Members, request that the Court enter judgment in their favor and against Defendants, as follows:

1381. Certify the Classes and appoint Plaintiffs as Class Representatives;

1382. Enter Judgment against Defendants on Plaintiffs' and Class Members' asserted causes of action;

1383. Award Plaintiffs and Class Members appropriate relief, including actual and statutory damages, restitution, disgorgement, and punitive damages;

1384. Award equitable, injunctive, and declaratory relief as may be appropriate;

1385. Award all costs, including experts' fees and attorneys' fees, as well as the costs of prosecuting this action;

1386. Award pre-judgment and post-judgment interest as prescribed by law; and

1387. Grant additional legal and equitable relief as this Court may find just and proper.

#### **XI. DEMAND FOR JURY TRIAL**

1388. Plaintiffs, on behalf of themselves and all others similarly situated, hereby demand a trial by jury on all the issues so triable.

Dated: August 4, 2020

KELLER ROHRBACK L.L.P.

By: /s/ Derek W. Loeser  
Derek W. Loeser

Derek W. Loeser (admitted *pro hac vice*)  
Lynn Lincoln Sarko (admitted *pro hac vice*)  
Gretchen Freeman Cappio (admitted *pro hac vice*)  
Cari Campen Laufenberg (admitted *pro hac vice*)  
David Ko (admitted *pro hac vice*)  
Adele A. Daniel (admitted *pro hac vice*)  
1201 Third Avenue, Suite 3200  
Seattle, WA 98101  
Tel.: (206) 623-1900  
Fax: (206) 623-3384  
dloeser@kellerrohrback.com  
lsarko@kellerrohrback.com  
gcappio@kellerrohrback.com  
claufenberg@kellerrohrback.com  
dko@kellerrohrback.com  
adaniel@kellerrohrback.com

Christopher Springer (SBN 291180)  
801 Garden Street, Suite 301  
Santa Barbara, CA 93101  
Tel.: (805) 456-1496  
Fax: (805) 456-1497  
cspringer@kellerrohrback.com

BLEICHMAR FONTI & AULD LLP

By: /s/ Lesley E. Weaver

Lesley E. Weaver (SBN 191305)  
Anne K. Davis (SBN 267909) Matthew  
P. Montgomery (SBN 180196)  
Angelica M. Ornelas (SBN 285929)  
Joshua D. Samra (SBN 313050)  
555 12th Street, Suite 1600  
Oakland, CA 94607  
Tel.: (415) 445-4003  
Fax: (415) 445-4020  
lweaver@bfalaw.com  
adavis@bfalaw.com  
mmontgomery@bfalaw.com  
aornelas@bfalaw.com  
jsamra@bfalaw.com

*Plaintiffs' Co-Lead Counsel*

**ATTESTATION PURSUANT TO CIVIL LOCAL RULE 5-1(i)(3)**

I, Lesley E. Weaver, attest that concurrence in the filing of this document has been obtained from the other signatory. I declare under penalty of perjury that the foregoing is true and correct.

Dated: August 4, 2020

/s/ Lesley E. Weaver  
Lesley E. Weaver

**CERTIFICATE OF SERVICE**

I, Lesley E. Weaver, hereby certify that on August 4, 2020, I electronically filed the foregoing document with the Clerk of the United States District Court for the Northern District of California using the CM/ECF system, which shall send electronic notification to all counsel of record.

Dated: August 4, 2020

/s/ Lesley E. Weaver  
Lesley E. Weaver