PIERCE BAINBRIDGE BECK PRICE & HECHT LLP

YAVAR BATHAEE (CA 282388)
yavar@piercebainbridge.com
MICHAEL POMERANTZ (NY 2920932) (*pro hac vice* forthcoming)
mpomerantz@piercebainbridge.com
DAVID L. HECHT (NY 4695961) (*pro hac vice* forthcoming)
dhecht@piercebainbridge.com
ADAM C. LUDEMANN (NY 5352323) (*pro hac vice* forthcoming)
aludemann@piercebainbridge.com
277 Park Ave. 45th Floor
New York, NY 10172
(212) 484-9866

BRIAN J. DUNNE (CA 275689)
bdunne@piercebainbridge.com
355 S. Grand Ave. 44th Floor
Los Angeles, CA 90071
(213) 262-9333

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

REVEAL CHAT HOLDCO LLC, a Delaware limited liability company, USA TECHNOLOGY AND MANAGEMENT SERVICES, INC. (d/b/a Lenddo USA), a Delaware corporation, CIR.CL, INC., a dissolved Delaware corporation, and BEEHIVE BIOMETRIC, INC., a dissolved Delaware corporation, Plaintiffs, v. FACEBOOK, INC., a Delaware corporation, Defendant.	Case No. 3:20-cv-363 **CLASS ACTION COMPLAINT** Jury Trial Demanded

TABLE OF CONTENTS

TABLE OF CONTENTS
(*continued*)

1. Plaintiffs allege the following on behalf of themselves and others similarly situated on information and belief based on the review of ***only public documents and information***. All references to internal Facebook documents are ***exclusively*** to those published by news organizations and other public sources, particularly NBC News.[1] Neither Plaintiffs nor the undersigned counsel viewed or received, or even had access to, any confidential information about Facebook at the time this complaint was filed.

INTRODUCTION

2. This action seeks to halt the most brazen, willful anticompetitive scheme in a generation—a scheme that verges on final, irreparable completion as of the date of this Complaint.

3. Facebook stands today as a paragon of unbridled market power. A company with unprecedented reach, Facebook collects and monetizes the activity of more than two billion active users around the world. Facebook's advertising juggernaut produces almost $55 billion in revenue in a year, and its founder and CEO, Mark Zuckerberg, enjoys incontestable control over the company and its board. Facebook owns some of the most valuable social networks other than Facebook itself, including Instagram and WhatsApp. As 2020 begins in earnest, Facebook has no serious rival in its key markets—nor any prospect of one.

4. It was not always so. In 2010, when Facebook defeated rivals MySpace and Friendster and emerged as the winner of the social network wars, the company was caught flatfooted by a new technology that threatened its dominance—smartphones.

5. Facebook's dominance had been fortified by powerful network effects—the more data it collected on users, the more attractive its social network became to users. As a result, a social data barrier to entry ("SDBE") emerged, protecting Facebook's business. This SDBE

---

[1] As of the date of this complaint, NBC's documents were available at https://dataviz.nbcnews.com/projects/20191104-facebook-leaked-documents/as https://dataviz.nbcnews.com/projects/20191104-facebook-leaked-documents/assets/facebook-exhibits.pdfsets/facebook-sealed-exhibits.pdf; and https://dataviz.nbcnews.com/projects/20191104-facebook-leaked-documents/assets/facebook-exhibits.pdf.

allowed Facebook to fend off a frontal assault by Google's polished social network, Google+. Google, with its massive resources and user base, failed to penetrate the SDBE, and Google abandoned the project after it was clear that users were not engaging on its platform.

6. Smartphones, however, were different. Significant advances in mobile technology allowed users to access the internet from any location, on user interfaces controlled by touch, providing a distinct experience from desktop or laptop computers. Special-purpose apps designed specifically for smart phones could not only access the Internet, but also users' address books—a ready-made social network from which apps could draw.

7. These apps had become direct competitors to Facebook, providing overlapping functionality such as messaging, photo sharing, dating, check-ins, and payments. Facebook failed to create its own viable mobile app, and by 2011, found its dominance threatened. Zuckerberg told *Fortune*, "[i]t was probably one of the biggest mistakes we've ever made." Facebook's own mobile app was buggy and slow, garnering one-star ratings in the Apple App Store and crashing more often than it worked.

8. This existential threat to Facebook's monopoly in social data and social advertising came as the company was barreling towards an initial public offering ("IPO") worth billions. Facebook had successfully built a developer platform upon which third-party developers could build social applications, driving engagement on Facebook's Platform and thereby Facebook's revenue. It was clear, however, that the very same Platform was providing Facebook's competitors with access to Facebook's network of users. Third-party developers began using Facebook's Platform in more novel and creative ways than Facebook itself was doing. Facebook found itself lagging behind these third-party social applications in the mobile arena.

9. With its market dominance in imminent danger, Facebook moved to extinguish the mobile threat, to obtain a sustaining foothold in the Social Data and Social Advertising Markets,[2]

[2] Defined terms are set forth elsewhere in the body of the Complaint.

and to prevent any newcomers from building rival social networks. To do so, Zuckerberg and Facebook's most senior executives hatched an anticompetitive scheme of unprecedented scale.

10. The scheme spanned several fronts:

11. ***First***, Facebook moved to crush or co-opt competition that existed on its own Platform. Facebook identified and categorized potential market threats, then extinguished those threats by cutting them off from key application program interfaces ("APIs") in Facebook's Platform—functionality that provided social applications with user data that fueled their growth. As Facebook's own executives and engineers acknowledged, the company's decision to remove core functionality from its Platform not only lacked any legitimate or technical justification, but Facebook sacrificed massive amounts of additional social data, engagement, and advertising that it received from its Platform to do it.

12. ***Second***, Facebook collected valuable user data from competing platforms, growing its own mobile footprint and constraining the growth of rivals. Facebook accomplished this with a network of Whitelist and Data Sharing agreements with direct competitors, including rival social networks (such as Pinterest and Foursquare) and apps that generated large amounts of user data from engagement (such as Tinder). Facebook coerced these competitors into handing over their central assets—their social data—by again leveraging its Platform, threatening the apps with extinction by starving them of access to core Platform APIs if they did not join Facebook's so-called "reciprocity" scheme. Those who did join received not only access to social data, but the data of others that had joined Facebook's scheme, with Facebook acting as a hub for the exchange of user data among competitors.

13. ***Third***, Facebook moved aggressively to shut out entirely direct competitors that had built independent social networks of their own and did not rely on Facebook for their social data and user base. Facebook revoked the ability of competitors, such as WeChat and Line, to use Facebook's Platform, and even banned them from buying Facebook's social data through advertising, forgoing significant profits to do so.

14. ***Fourth***, Facebook monitored the market for nascent threats to its business, and then extinguished these threats through anticompetitive conduct or by targeted acquisition. Facebook did so using mobile surveillance technology it acquired from Onavo, a company that cloaked spyware in legitimate-looking utility apps. For example, in 2012-13, Facebook's surveillance warned it that both Instagram and WhatsApp were imminent threats to Facebook's core business, with each app having accumulated staggering user bases and levels of engagement while directly competing with Facebook. Facebook moved forcibly to acquire both companies, and with each acquisition, it dramatically increased its share of the Social Data and Social Advertising markets—not only maintaining its market power and the SDBE but, expanding and strengthening them.

15. Today, Facebook is rapidly working to integrate the backends of its acquired WhatsApp and Instagram assets in the face of regulatory concern over Facebook's unchecked market power and anticompetitive conduct. This is no coincidence. Facebook's integration efforts are deliberately intended to avoid regulatory divestiture of assets, to consolidate the geographic regions it controls through its various apps, and to finally flex the market power it acquired through those mergers. This last piece of Facebook's monopolization scheme is on the verge of completion—and once culminated, the backend integration will imbue Facebook with unrivaled global dominance of the Social Data and Social Advertising Markets.

16. The net effect of Facebook's anticompetitive scheme is one of the largest unlawful monopolies ever seen in the United States—one protected by a far-reaching and effectively impenetrable barrier to entry arising from feedback loops and powerful network effects. Facebook not only has the power to raise prices and keep them high, it can do so without suffering any decrease in demand, and without having to provide more value to users to obtain their data. This is the very definition of market power. Facebook has sought to bury the story of how it acquired, maintained and abused that market power for years, but ultimately it cannot avoid the truth.

17. This lawsuit seeks to hold Facebook accountable for its overtly anticompetitive conduct. The company, its executives, and its engineers worked together over years to execute the

anticompetitive scheme described in this Complaint. They did so with flagrant disregard for competition, for Facebook users, or for the law. Plaintiffs seek trebled damages and injunctive relief under the federal antitrust laws to remedy Facebook's brazen play for dominance—and to stop the company from further solidifying its unlawful monopoly, barrier to entry, and market power.

PARTIES

I. PLAINTIFFS

18. Plaintiff Reveal Chat HoldCo LLC ("Reveal Chat") is a Delaware limited liability company headquartered in Bainbridge Island, WA. Reveal Chat is the successor in interest to Reveal Chat, Inc. (f/k/a LikeBright, Inc. ("LikeBright")), pursuant to an April 2015 merger between Reveal Chat and Reveal Chat, Inc.

19. LikeBright was founded in 2011 and launched the dating site LikeBright.com that same year. LikeBright was designed as a platform to make dating safe and fun for women. Unlike most other matchmaking platforms during that time period, Likebright was designed to incorporate users' social media data to help facilitate better matches, drawing on second-degree friend connections and shared interests. LikeBright also featured a system in which women could vouch for their male friends. In order to facilitate these and other features essential to its business model, LikeBright was designed to incorporate—and relied heavily on—social media data made available by Facebook to developers (during the time LikeBright operated) through its Open Graph APIs. Such social data included friends, photos, likes, groups, pages and other data that facilitated pairing members to matches with similar interests and shared friends.

20. Plaintiff USA Technology and Management Services, Inc. (d/b/a Lenddo USA) (and together with its affiliates, referred to herein as "Lenddo") is a Delaware corporation with its principal place of business in New York, NY.

21. Lenddo is a market leader in alternative credit scoring and identity verification, allowing individuals and small enterprises in emerging markets to leverage their digital footprints,

including social media data, to unlock access to financial and credit services to which they might not have access through traditional means. Founded in 2011, Lenddo first began underwriting and making loans to customers in the Philippines. It then entered the Columbian market in 2012, followed shortly thereafter by its entry into the Mexican market in 2013. By 2014, Lenddo had originated over 10,000 loans using its proprietary LenddoScore algorithm and was able to provide customers the world's first Facebook-only loan origination process. Lenddo's origination algorithm was designed to incorporate and analyze social media data provided by Facebook to its developers, including through its Open Graph APIs, in order to accurately measure credit risk based on factors such as friend networks, frequency and consistency of social interactions, and the social media characteristics of applicants' friend connections. In 2015, Lenddo first made available to third parties its proprietary data scoring system and began offering identity verification services.

22. Plaintiff Cir.cl, Inc. ("Cir.cl") is a dissolved Delaware corporation formerly headquartered in New York, NY. Plaintiff Cir.cl's claims are brought by and through Carol Davidsen, who has been appointed as a receiver by the Delaware Court of Chancery pursuant to 8 Del. C. § 279 for purposes of pursing Cir.cl's claims in this action.

23. Cir.cl was founded in 2013 and designed an online platform for individuals and communities to manage peer-to-peer marketplace transactions, with the goal of allowing real-time integration of users' various online communities. This allowed them to use their digital presence and social connections to complete real-life peer-scale marketing and fulfilment goals. Cir.cl's platform was designed around and incorporated its user's social media data, including data made available by Facebook through its Open Graph APIs.

24. Plaintiff Beehive Biometric, Inc. (a/k/a Beehive ID) ("Beehive") is a dissolved Delaware corporation formerly headquartered in Austin, TX. Plaintiff Beehive's claims are brought by and through Mary Haskett, who has been appointed as a receiver by the Delaware Court of Chancery pursuant to 8 Del. C. § 279 for purposes of pursing Beehive's claims in this action.

25. Beehive was founded in 2013 and designed an identity verification system drawing heavily on social media data through a trademarked and proprietary Social Authentication Technology ("SAT"). Beehive's SAT leveraged social media data, including data made available through Facebook's Open Graph APIs, to identify fraud risks based on unique digital patterns and online social interactions.

II. DEFENDANT

26. Defendant Facebook, Inc. ("Facebook") is a publicly traded company, incorporated in Delaware. Facebook's principal place of business and headquarters is located at 1601 Willow Road in Menlo Park, California.

27. Founded in 2004 by Mark Zuckerberg, Facebook is a social media company that provides online services to two billion users around the world. In exchange for providing services, Facebook collects user data, which it uses to create and sell targeted advertising services. Facebook's principal revenue is from targeted social media advertising that it provides to advertisers as a data broker.

28. Facebook also operates as a platform for third-party applications and hardware, and owns and operates several business divisions:

- *Facebook*. Facebook's core application, which bears the Company's name, is, according to Facebook's filing with shareholders, designed to enable "people to connect, share, discover, and communicate with each other on mobile devices and personal computers." The Facebook core product contains a "News Feed" that displays an algorithmically ranked series of stories and advertisements individualized for each person.
- *Instagram*. Instagram is a photo sharing application, which allows users to share photos, videos and messages on mobile devices. Instagram was acquired in April 2012 and at present, Facebook operates Instagram as a separate application from its core Facebook product—but that is about to change, absent relief from this Court.

- *Messenger*. Facebook's Messenger application is a multimedia messaging application, allowing messages that include photos and videos to be sent from person to person across platforms and devices.
- *WhatsApp*. WhatsApp is a secure messaging application used by individuals and businesses. WhatsApp was acquired by Facebook in 2014 for $21.8 billion, and at the time had approximately 450 million users worldwide. Facebook operates WhatsApp as its own application, separate from its Messenger and Facebook products and lines of business—but that is about to change, absent relief from this Court.
- *Oculus*. Oculus is Facebook's virtual reality hardware line of business, which Facebook acquired in March 2014 for approximately $2 billion.

29. Facebook's revenue as of year-end 2018 was $55.84 billion, with net income from operations of $21.11 billion. Almost all of this revenue ($55 billion) came from advertising. As of year-end 2018, Facebook maintained $41.11 billion in cash and cash-equivalent securities. Facebook employed 35,587 people around the world at the end of 2018.

30. Across all of its lines of business, Facebook reported to investors in 2018 that it had 1.52 billion daily active users ("DAU") on average for the year. Facebook reported 2.32 billion monthly active users ("MAU") on average during the same period.

JURISDICTION AND VENUE

31. This action arises under sections 1 and 2 of the Sherman Antitrust Act (15 U.S.C. §§ 1 and 2) and sections 4, 7, and 16 of the Clayton Act (15 U.S.C. §§ 15(a), 18, and 26). The action seeks to recover treble damages, interest, costs of suit, equitable relief, and reasonable attorneys' fees for damages to Plaintiffs and members of the Class resulting from Defendant's restraints of trade and monopolization of the Social Data and/or Social Advertising Markets described herein.

32. This Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 (federal question), 1332 (class action diversity jurisdiction), and 1337(a) (antitrust); and under 15 U.S.C. § 15 (antitrust).

33. Venue is appropriate in this district under 15 U.S.C. § 15(a) (Clayton Act), 15 U.S.C. § 22 (nationwide venue for antitrust matters), and 28 U.S.C. § 1391(b) (general venue provision). Facebook transacts business within this district, and it transacts its affairs and carries out interstate trade and commerce, in substantial part, in this district.

34. The Court has personal jurisdiction over Facebook as it is subject to general jurisdiction in the State of California, where it maintains its headquarters and its principal place of business. The scheme, conspiracy, and monopolization alleged in this Complaint was targeted at individuals throughout the world and the United States, causing injury to persons not only throughout the world, but in the United States, including in this district.

FACTS

I. FACEBOOK EMERGES AS THE DOMINANT SOCIAL NETWORK

A. The Last Social Network Standing

35. Facebook's meteoric rise since its founding in 2004 is well documented. The company—started in the dorm room of its CEO Mark Zuckerberg ("Zuckerberg") as "the facebook"—rose to prominence in the face of fierce competition from several social networks. Initially an exclusive service for elite universities throughout the United States, Facebook eventually expanded its network to encompass a general audience of users throughout the United States and worldwide.

36. Between 2004 and 2010, Facebook vanquished a number of rivals to emerge as the dominant social network in the United States.

37. Facebook's first chief competitor was MySpace. Founded in 2003—a year before Facebook—MySpace targeted the same audience, provided largely the same services, and rapidly attracted an enormous number of users. By 2005, MySpace had 25 million active users, and was

acquired by NewsCorp for $580 million. In 2006, MySpace registered 100 million users, passing Google as the most visited website in the United States.

38. However, the next three years featured a steady downward spiral for MySpace—and countervailing growth by Facebook. In 2008, Facebook passed MySpace in worldwide active users, and continued to grow, reaching 307 million active users across the globe by April 2009. In May 2009, Facebook passed MySpace in United States, 70.28 million to 70.26 million monthly active users.

39. MySpace never came close to Facebook again. By 2010, MySpace had mostly exited the market, leaving the business of social media for good. MySpace's CEO capitulated in November of 2010: "MySpace is not a social network anymore. It is now a social entertainment destination." In September 2010, MySpace reported that it had lost $126 million, and in June 2011, NewsCorp sold the company for $35 million—$545 million less than it had paid for MySpace just six years earlier. By then, its user base had dwindled to just 3 million monthly visitors.

40. During the same time period, several other social networks also met their demise, including Google's Orkut, AOL's Bebo, and Friendster, which failed to scale rapidly enough to compete with MySpace and Facebook.

41. By 2009 and through 2010, Facebook emerged as the only peer-to-peer social media network to exist at scale, and no other network or company rivaled Facebook's massive user base. On March 2, 2010, *Adweek* reported that Facebook had booked revenues of up to $700 million in 2009 and was on track for $1.1 Billion in 2010—almost all from advertising to its newly won users. Facebook had been roughly doubling its revenues every year up until that point—$150 million in 2007; $280-300 million in 2008; and $700 million in 2009.

42. Time Magazine heralded Zuckerberg as its 2010 Person of the Year.

43. Time's cover story set out the stakes—the scope of the newly assembled social network was unprecedented and staggering:

> What just happened? In less than seven years, Zuckerberg wired together a twelfth of humanity into a single network, thereby creating a social entity almost twice as large as the U.S. If Facebook were a country it would be the third largest, behind only China and India. It started out as a lark, a diversion, but it has turned into something real, something that has changed the way human beings relate to one another on a species-wide scale. We are now running our social lives through a for-profit network that, on paper at least, has made Zuckerberg a billionaire six times over.

44. By 2010, Facebook was unrivaled and dominant in a way no company since Microsoft had been in post-personal-computer history. And it had done so by riding the currents of powerful network effects.

B. A New Market of Its Own Creation

45. By the beginning of the millennium's second decade, Facebook was the indisputable king of an entirely new market—a market built not on hardware or operating system dominance, but one built on a network of people, with its power and value directly derived from

their engagement with that network. The more data users fed into Facebook by communicating and interacting with each other, posting their pictures, and publishing their content, the more valuable the Facebook network became to third parties, who could advertise to Facebook's users by targeting them using the very information they provided to Facebook's network.

46. Data about what information users shared on their personal pages; the photos and profiles they viewed; their connections to others; what they shared with others; and even what they put in messages to other users all allowed targeted advertising on a scale that had never before existed. Unlike search advertising, Facebook's advertising platform allowed advertisers to target Facebook's user base by their attributes and behavior, not by a query entered into a search box. More importantly, unlike in search, user identity was not only discoverable, it was willingly provided by users—as was the identity of those users' closest friends and family members. These identities could be tracked and targeted throughout the Internet.

47. This social data created by Facebook's network of engaged users could be monetized in a number of ways. The data could be resold for targeted advertising and machine learning; Facebook's machine learning algorithms mined patterns in the data for advertisers, which allowed advertisers to reach precisely the right audience to convert into sales, user signups, or the generation of sales leads. The data also could be sold by commercializing access—for example, by providing application developers, content generators, and advertisers with direct access to the information embedded in Facebook's network, such as the interconnection between users, user attributes, and user behavior. That data then could be mined by these third parties.

48. All of the methods of monetizing social data were based on selling that data, but such data could be packaged, structured, or mined differently depending on the application for which it was being sold. For advertisers, Facebook's network presented advertisers and Facebook itself with entirely new social signals, such as relationships, events, friendships, and granular interests. Movies, music, books were inherent parts of a user's profile. The amount of information

in Facebook's network that could be mined as social data was unprecedented—and Facebook received all of that data daily from its millions of users in the United States and worldwide.

49. The data Facebook collected was uniquely social, derived from the engaged interactions and strong identity of Facebook's users. Twitter, a public-facing social network, loosely enforced identity, and never required users to disclose granular details about themselves. Facebook stood alone in this regard, with a clear product emphasis on individuals and their connections to others. In 2010, Google, Yahoo!, and the other major online advertising sources competed in an entirely different market—one based on search data. The data Facebook had at its disposal was not fungible with search data—it was actionable data about individual users, with their identities fully ascertainable.

50. By 2010, Facebook stood alone as the dominant player in the newly emergent market for social data (the "Social Data Market")—a market in which Facebook's own users provided Facebook with a constant stream of uniquely valuable information, which Facebook in turn monetized through the sale of social data (for example, through advertising, monetizing APIs, or other forms of commercializing access to Facebook's network). Advertisers, finding no substitute from any other company, paid top dollar for Facebook's powerful targeting and actionable data, and some of those advertisers—wittingly or not—even fed crucial data about themselves, their products, and the efficacy of their targeting back to Facebook's network.

51. As Facebook itself explained to third-party developers in May 2007, Facebook's core value proposition and business model was "providing access to a new kind of data—social data, which enables you to build applications that are relevant to users." With respect to that data, Facebook told developers: "You are on a level playing field with us. You can build robust apps, not just widgets. Complete integration into the Facebook site." By 2010, it was clear that Facebook's entire business was selling this new form of "social data" and that it would do so by selling access to developers and selling advertisements targeting Facebook's network of engaged and active users.

C. The Social Data Barrier to Entry

52. As Facebook's dominant position in the Social Data Market emerged in 2010, powerful network effects and feedback loops took hold and solidified that position. Data provided by users made Facebook's network more valuable, thereby attracting more users to the network. As a typical use case, a Facebook user would invite his closest friends and family, who would then invite and engage with other friends and family members who existed on the network. A familiar feedback loop—a virtuous circle—emerged, rapidly growing Facebook's user base.

53. The content generated by this user base, in turn, increased the value of the Facebook network. With each photograph, relationship status, check-in, or post by a Facebook user, the Facebook network became more valuable, not just as a means of communicating with directly connected acquaintances, but as a means of learning about more remotely connected ones.

54. As Samuel Lessin, then Facebook's VP of Product Management, explained to Mark Zuckerberg in an internal email on October 26, 2012, the data Facebook collects makes Facebook progressively more proficient at collecting and monetizing data:

> One of the things that puts us currently in a very defensible place is the relationship we have created between the people using Facebook all the time, and us having the information we need to make Facebook a better product. This is the fundamental insight in something like coefficient. ***We know more about what people want to see because people look at more stuff on our platform.*** In this respect, while there are other ways to get close, it feels viscerally correct that there is an ROS dynamic at play, ***the more people that use the system, the more information we have on how to make more people use the systems***.

(emphasis added).

55. A barrier to entry emerged from this feedback loop. To compete with Facebook, a new entrant would have to rapidly replicate both the breadth and value of the Facebook network—a task a mere clone of that network could not accomplish. Indeed, to compete with Facebook, a competitor would not only have to build its own vast network, but would have to draw active social engagement on a massive scale—which likely would require drawing a vast quantity of Facebook users away from that platform. The costs to switch would be massive: an entrant-competitor would

have to present an overall value proposition to users that not only exceeded that of Facebook's entrenched network, but one that did so handily. Moreover, to compete with Facebook's virtuous circle, the value delivered by an entrant-competitor platform would have to facilitate social data mining that would create even more value for users, developers, and advertisers. This barrier to entry is referred to throughout this Complaint as the Social Data Barrier to Entry ("SDBE").

56. The SDBE allows Facebook to control and increase prices in the Social Data and Social Advertising Markets without the pressures of price competition from existing competitors or new entrants. Because of the SDBE, Facebook has been able to consistently increase the price it charges for social data through advertising or direct access to its social data (*e.g.*, through APIs). And this is exactly what Facebook has done since it obtained its dominant position in 2010.

57. From 2011 to 2012, for example, Facebook massively increased the prices it charged for its advertisements—one of the primary sales channels for its social data. That year, costs per thousand impressions (CPM) on Facebook increased by 41%, with a 15% increase in the last quarter of 2011 alone. Cost per click, which is a measure of advertising costs paid on a by-click basis, rose 23% that same year. Facebook increased prices as it also grew the number of

Figure 1: Retail Facebook CPM, Q4 2012 – Q4 2013

advertisements it displayed on its site, indicating direct market power over social data prices, particularly through the advertising channel for selling social data.

58. Facebook maintained that power over its prices through 2013, with a 2.9x increase in CPMs year over year. The increase came as overall advertising revenues increased yet again—that year by a staggering 83% over the last.

59. These price increases would not be possible without the SDBE. If a rival network existed with comparable Social Data available for sale through advertising, Facebook's price increases would have been met with customer migration to the comparable rival. But Facebook had no such rival and was unfettered in its ability to increase prices, even while rapidly increasing its supply of data for sale through advertisement or directly through its developer platform.

60. Once Facebook had achieved dominance in the Social Data market, its position only improved—and became more entrenched. The more advertising Facebook sold, and the more social data Facebook collected and packaged for sale, the more effective Facebook became at selling advertising, targeting users, and commercializing direct access to its users' social data (*e.g.*, through APIs). This, in turn, made entry by a new rival impossible or prohibitively costly, thereby allowing Facebook to increase prices and make additional investments that deepened the SDBE moat surrounding its business.

D. Google's Failed Entry into the Social Data Market

61. In 2010, Google became desperate to enter the Social Data and Social Advertising Markets. It had tried several times to do so before, but each foray was met with failure. Google's Orkut social network, which was launched days before Facebook, was quickly overtaken. Wave, Google's social communication platform, never achieved any traction with users. And Google's Buzz social network—built on the back of its highly successful Gmail product—imploded quickly in early 2010.

62. Google's next attempt to enter the market attacked Facebook's functionality head on, which meant attempting to penetrate the powerful SDBE protecting Facebook's business. Google made a massive, unprecedented investment of resources into building a product with enough value to lure users away from Facebook's broad, highly-engaged social network.

63. In 2010, Google's Vic Gundotra became the company's Chief Architect. Gundotra pitched a new social network to Larry Page, Google's cofounder, who returned as CEO of the company in 2011. Gundotra repeated an ominous refrain, "Facebook is going to kill us. Facebook is going to kill us," which frightened Page into action.

64. Page greenlit a new product, Google+. Initially, Google+ sought to leverage Google's YouTube product to build its social network, requiring a Google+ account for access to certain key features of YouTube. In the face of significant user resistance, Google backed away from that requirement. Nonetheless, Google attempted, through Google+, to build out a "social graph" that would leverage a common user identity across Google products, including YouTube and Gmail.

65. In early 2011, Google began what insiders now refer to as "the 100-day march" toward launch of Google+. The product Google planned to deliver was, by any fair account, largely undifferentiated from what Facebook offered in terms of product features and functionality. By Summer 2011, the planned features for Google+ included a continuous scroll product called the "stream" (a clone of Facebook's "feed" product); a companion feature called "sparks," which related the "stream" to users' individual interests; and a sharing app called "Circles," a purportedly improved way to share information with one's friends, family, contacts, and the public at large.

66. Unlike Google's past products, Google+ was not designed to organically grow and scale from small beginnings. From the outset, Google invested massive amounts of resources to bring a finished, full-scale social network to market. Developed under the code name Emerald Sea, Google conscripted almost all of the company's products to help build Google+. Hundreds of engineers were involved in the effort, which remained a flagship project for Page, who had recently re-assumed the Google CEO role. Google's Gundotra was quoted explaining that the product that would become Google+ was a transformation of Google itself: "We're transforming Google itself into a social destination at a level and scale that we've never attempted—orders of magnitude more investment, in terms of people, than any previous project."

67. The amount of resources Google brought to bear stood in stark contrast to its previous attempts at penetrating the Social Data and Social Advertising Markets. Google had dedicated barely a dozen staff members to its previous failed social network product, Buzz. At its peak, Google+ involved 1000 employees from divisions across the country. Google, for example, ripped out its elaborate internal video conferencing system and forced employees to use the Google+ Hangouts video chat feature, which one internal employee described as "janky." Employee bonuses were tied to the success of Google+. And, the entire project was confined to a level of secrecy never before seen at Google.

68. Google+ was released on June 28, 2011. The product included the "stream," the "Circles" app, the "Hangout" video chat and messaging product, and a photo sharing product. The resemblance to Facebook was striking. As one internal Google employee commented: "this looks just like Facebook. What was the big deal? It's just a social network." Another Google employee was quoted as saying, "All this fanfare and then we developed something that in the end was quite ordinary." One thing was indisputable: with the release of Google+, Google had challenged Facebook head-on by effectively cloning Facebook's product.

69. Because Google's user base was already massive, the Google+ product attracted millions of users shortly after launch. But although these users signed up for Google+, Google quickly found out that they were not using the product. As one former Google employee explained:

> It was clear if you looked at the per user metrics, people weren't posting, weren't returning and weren't really engaging with the product. Six months in, there started to be a feeling that this isn't really working.

70. The problem for Google+ was the powerful network effect that reinforced the SDBE that protected Facebook. Google's clone of Facebook did not present enough new value to overcome massive network-based switching costs—the cost to Facebook users of shifting away from an existing networked product that the users had actively invested their social data in for years.

71. Paul Adams, a former Google+ user-experience team member, summed it up succinctly when asked why Google+ had failed:

> What people failed to understand was Facebook and network effects. . . . It's like you have this grungy night club and people are having a good time and you build something next door that's shiny and new, and technically better in some ways, but who wants to leave? People didn't need another version of Facebook.

72. By 2014, Google+ was declared a failure and Gundotra, its founder, eventually left Google. Within just a few years, Google—with all of its resources, developers, and existing user base—failed entirely to overcome the SDBE protecting Facebook. As long as Facebook controlled the data derived from an engaged and active user base, it could continue to keep that user base active and engaged.

73. The only way to disrupt this virtuous circle was with a rival product that provided significantly more or different value than Facebook, and that itself was propelled to scale by powerful network effects. By attempting to clone Facebook's functionality and failing to garner user engagement that could erode the SDBE protecting Facebook, Google+'s failure was virtually ensured at launch.

II. A THREAT TO FACEBOOK'S MONOPOLY: THE RISE OF SMART PHONES AND MOBILE APPS

A. The Mobile App Revolution

74. In 2009 and 2010, as Facebook emerged the undisputed winner of the newly formed Social Data and Social Advertising Markets, another new market had begun to take hold. The launch of the Apple iPhone in 2007 created a market for a new type of cellular phone—one with a user interface capable of robust Internet connectivity and messaging. No longer constrained by numeric keypads for texting—or clunky, permanent alphanumeric keyboards attached to phones, such as with the Treo or Sidekick cellular phones—the iPhone dynamically displayed a multi-touch keyboard and came equipped with a full-featured web browser that rendered complete webpages.

75. By the summer of 2008, Apple's newest iPhone, the iPhone 3G, was released with onboard GPS, as well as other hardware upgrades. Accompanying the release of the new iPhone was a new store for third-party applications that would run natively on the iPhone: the Apple App Store, which opened for business on July 10, 2008, the day before the release of the iPhone 3G.

76. Developers who launched their third-party applications via the App Store reaped huge rewards. There were approximately 500 apps available at the App Store's initial launch. Games using the iPhones accelerometer became immediate successes, some quickly earning hundreds of thousands of dollars by selling downloads for just a few dollars each. Applications that exploited the new GPS functionality in the iPhone also quickly became popular. By September 2008, the Apple App Store had racked up 100 million downloads, and by 2009, it hit 1 billion. iPhone Apps had become a new means to deliver scaled value to countless users.

77. Google also launched what became its Play Store (initially known as Android Market) in 2008. It soon thereafter overtook Apple's App Store in terms of overall volume, with 82% growth. The mobile app revolution had begun.

78. Mobile apps rapidly proliferated, with huge opportunities for further growth—as the lion's share of cell phone activity by 2010 had become something other than making phone calls. For example, a 2010 Pew Research survey showed that taking pictures and sending text messages had become the most common uses for cellular phones among adults, with more than a third of adult cell phone users accessing the Internet, playing games, emailing, recording video, or

playing music through their cell phones. At the same time, 29% of adult cell phone users had used a downloaded app.

% of adult cell phone users who do each of the following on their phone...

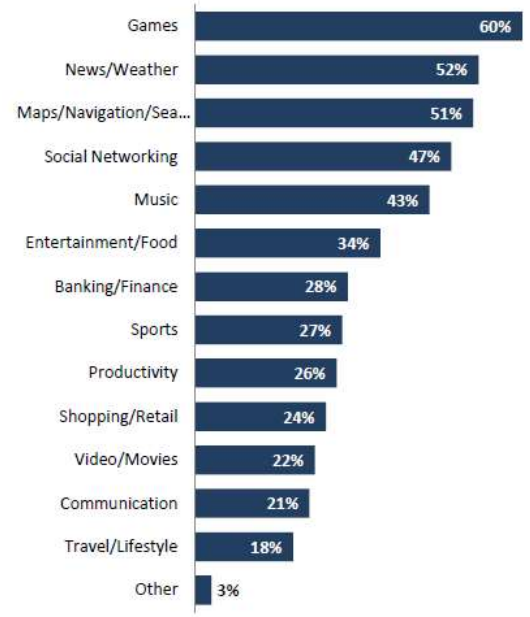
Take a picture	76%
Send or receive text messages	72
Access the internet	38
Play a game	34
Send or receive email	34
Record a video	34
Play music	33
Send or receive instant messages	30
Use an app	**29**

Source: Pew Research Center's Internet & American Life Project, April 29-May 30, 2010 Tracking Survey. N=1,917 adult cell phone users.

79. A 2010 Nielsen survey showed that games, news/weather, maps and navigation, and social networking were the most popular apps on cellular phones.

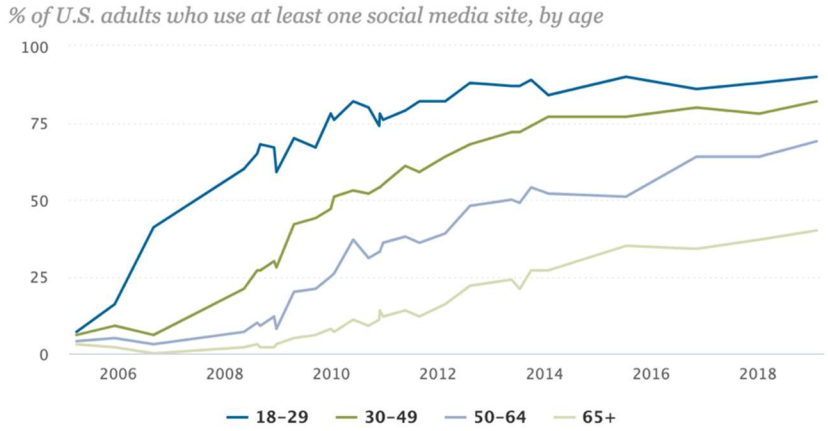
What are the most popular types of apps?

% of Nielsen recent downloaders who have used each category of apps in the past month...



Source: The Nielsen App Playbook, December 2009. N=3,962 adults who have downloaded an app in the 30 days prior to the survey.

80. Notably, mobile apps resonated most strongly with the demographics that had recently adopted social media and were providing their data to Facebook in droves. App users among cell phone owners were disproportionately younger, with 44% of app users in 2010 under the age of 20, and another 41% between the ages of 30 and 49. These were the same demographics that were rapidly adopting social media as part of their lives, and were providing Facebook with the social data that built and maintained the SDBE that protected its business.



Source: Surveys conducted 2005-2019.

PEW RESEARCH CENTER

81. Many of the mobile apps that were rapidly attracting users were doing so because they presented their own specialized value propositions. These apps had to be specialized because cellular phone screens were smaller, particularly in 2010, and mobile traffic was driven by specialty software, often designed for a single purpose. Users signed up for these apps with their e-mail addresses and personal information—and interacted directly with the apps.

82. As WIRED Magazine described in 2010, a typical user moved from app to app, each with some specialized use:

> You wake up and check your email on your bedside iPad—that's one app. During breakfast you browse Facebook, Twitter, and the New York Times—three more apps. On the way to the office you listen to a podcast on your smartphone. Another app. At work, you scroll through RSS feeds in a reader and have Skype and IM conversations. More apps. At the end of the day, you come home,

> make dinner while listening to Pandora, play some games on Xbox Live, and watch a movie on Netflix's streaming service.

83. In 2010, Morgan Stanley projected that within five years, the number of users who accessed the Internet from mobile devices would surpass the number who accessed it from PCs. The Internet was at an inflection point—the World Wide Web was no longer the dominant way to access information. Users were obtaining their information from specialized walled gardens, and Facebook's own walled garden was one app away from being superseded.

84. The years leading up to 2010 saw the rise of streaming apps, such as Netflix and Pandora, and e-book readers, such as Kindle and iBooks. Apple's 2010 list of top-grossing iPhone apps included mobile games such as Angry Birds, Doodle Jump, Skee-Ball, Bejeweled 2 + Blitz, Fruit Ninja, Cut the Rope, All-in-1 GameBox, the Moron Test, Plants vs. Zombies, and Pocket God. Facebook's mobile app topped the list of free downloads in the App Store, along with Words with Friends, Skype, and the Weather Channel App.

B. Facebook Recognizes the Looming Threat Presented by Mobile Applications

85. By 2011, Facebook realized that it had fallen behind. Facebook had just debuted its new "Timeline" product, a controversial modification of the Facebook feed that generated dynamic content for each user rather than a static series of posts visible to the user. Facebook had spent the last eight months prioritizing its desktop experience and its new Timeline product. But while it did so, mobile applications continued their meteoric rise.

86. Facebook's own mobile application was built on a technology called HTML5, which at the time was good for building web pages, but not for building mobile apps native to iOS and Android smartphones. As a result, Facebook's mobile app was buggy, prone to crashes, and painfully slow. As Zuckerberg would lament years later about HTML5, "we took a bad bet."

87. Zuckerberg reflected in 2018 that Facebook had fallen behind when mobile apps emerged:

> One of my great regrets in how we've run the company so far is I feel like we didn't get to shape the way that mobile platforms developed as much as would be good, because they were developed contemporaneously with Facebook early on. I mean, iOS and

> Android, they came out around 2007, we were a really small company at that point—so that just wasn't a thing that we were working on.

88. As mobile apps rose, Facebook's desktop product acquired users at a slower pace. All of this occurred as Facebook was planning its initial public offering ("IPO"). Facebook knew that its position was eroding and that if mobile growth continued, its IPO debut would be in the midst of material changes to its business, undermining Facebook's financial and qualitative disclosures to public investors.

89. But there was no avoiding the issue. After the IPO, when Facebook released statistics in its first major shareholder filing with the SEC in 2012, the trend was unmistakable—the transition to mobile devices from desktop web-based applications posed an existential threat to Facebook's business. Facebook disclosed this risk to shareholders as one of the factors that affected its bottom line:

> ***Growth in the use of Facebook through our mobile products as a substitute for use on personal computers may negatively affect our revenue and financial results.***
>
> We had 680 million mobile MAUs in December 2012. While most of our mobile users also access Facebook through personal computers, we anticipate that the rate of growth in mobile usage will exceed the growth in usage through personal computers for the foreseeable future and that the usage through personal computers may decline or continue to decline in certain markets, in part due to our focus on developing mobile products to encourage mobile usage of Facebook. For example, during the fourth quarter of 2012, the number of daily active users (DAUs) using personal computers declined modestly compared to the third quarter of 2012, including declines in key markets such as the United States, while mobile DAUs continued to increase. While we began showing ads in users' mobile News Feeds in early 2012, we have generated only a small portion of our revenue from the use of Facebook mobile products to date. In addition, we do not currently offer our Payments infrastructure to applications on mobile devices. If users increasingly access Facebook mobile products as a substitute for access through personal computers, and if we are unable to continue to grow mobile revenues, or if we incur excessive expenses in this effort, our financial performance and ability to grow revenue would be negatively affected.

(some emphasis added).

C. The Facebook Platform

90. Although Facebook faced a looming threat from mobile applications, it maintained an important source of leverage: its social data. Facebook possessed (and continued to receive) vast quantities of information about its massive user base, including how each user was connected to others. This information was valuable to both new and existing mobile applications, which could leverage Facebook's social data to obtain new users and to build novel social features, functions, and apps.

91. Facebook referred to its network as its "Graph," coined after a mathematical construct that models connections between individual nodes. The Facebook Graph contained user "nodes," with connections and information exchanged among nodes as "edges." Facebook coined the term "Open Graph" to describe a set of tools developers could use to traverse Facebook's network of users, including the social data that resulted from user engagement.

92. Importantly, Open Graph contained a set of Application Programming Interfaces ("APIs") that allowed those creating their own social applications to query the Facebook network for information. As Facebook explained in its 2012 10K:

> ***Open Graph.*** Our underlying Platform is a set of APIs that developers can use to build apps and websites that enable users to share their activities with friends on Facebook. As Open Graph connected apps and websites become an important part of how users express themselves, activities such as the books people are reading, the movies people want to watch and the songs they are listening to are more prominently displayed throughout Facebook's Timeline and News Feed. This enables developer apps and websites to become a key part of the Facebook experience for users and can increase growth and engagement for developers.

93. Open Graph, along with other Facebook products, such as its NEKO advertising and Payments products, comprised Facebook's Platform. The Platform was vital to Facebook's business, because it ensured that engagement continued on Facebook. Without the Platform, Facebook would be required to build applications that increased the value of its network itself—meaning that Facebook would have to try to predict what applications users wanted; design, code,

and scale those applications across its user base and network; and bear the risk and resource drain of guessing wrong and making mistakes.

94. Facebook did not have the resources to do this, so it decided instead to allow third parties to build applications for the Facebook Platform. As Mark Zuckerberg observed in a February 2008 email to Facebook's VP Engineering for Platform Michael Vernal, a senior Zuckerberg Lieutenant who was in part responsible for creating Open Graph:

> Platform is a key to our strategy because we believe that there will be a lot of different social applications . . . . And we believe we can't develop all of them ourselves. Therefore . . . . It's important for us to focus on it because the company that defines this social platform will be in the best position to offer the most good ways for people to communicate and succeed in the long term.

95. Put simply, Facebook could either speculate on new social applications by building them itself, or it could provide a platform for others to do so. For years, Facebook opted to provide a platform until it was able to develop its own social applications.

96. But Facebook also recognized that developers on Facebook's platform could potentially pose a competitive threat. In its 2012 Annual Report, Facebook disclosed the following significant risk factor to its operations:

> In addition, Platform partners may use information shared by our users through the Facebook Platform in order to develop products or features that compete with us. . . . As a result, our competitors may acquire and engage users at the expense of the growth or engagement of our user base, which may negatively affect our business and financial results.

97. Thus, Facebook knew that competition could come from its own third-party application developers. But Facebook nevertheless actively sought developers to build applications on its Platform because of the potential to extract profits from the applications these developers built and the users they attracted to, and engaged on, Facebook's Platform.

98. As Facebook explained to its investors in 2012, maintaining a Platform on which developers could build applications meant more engagement and therefore greater ad revenues for Facebook:

> Engagement with our Platform developers' apps and websites can create value for Facebook in multiple ways: our Platform supports our advertising business because apps on Facebook create engagement that enables us to show ads; our Platform developers may purchase advertising on Facebook to drive traffic to their apps and websites; Platform developers use our Payment infrastructure to facilitate transactions with users on personal computers; Platform apps share content with Facebook that makes our products more engaging; and engagement with Platform apps and websites contributes to our understanding of people's interests and preferences, improving our ability to personalize content. We continue to invest in tools and APIs that enhance the ability of Platform developers to deliver products that are more social and personalized and better engaged people on Facebook, on mobile decides and across the web.

99. Facebook's Platform was valuable to Facebook in several important ways.

100. First, the Platform meant that new applications would be built on Facebook's network, increasing the value of Facebook's network as the applications became more popular. The increased engagement with Facebook as a result of these new applications translated to better-targeted content and higher advertising revenues.

101. Second, Facebook would not need to spend significant resources to develop new applications or test new business models—third parties would do that instead. Facebook could merely wait for an application built for its Platform to gain widespread adoption, then either build a competing application or passively glean the benefits of that popular application's user engagement, including valuable new social data for Facebook and its network.

102. Third, access to Facebook's network was itself valuable to third-party developers, so Facebook could charge developers—most notably, through API access and advertising purchases—to access Facebook's Platform and the social data it collected from Facebook's massive number of engaged users.

D. The Profitable Open Graph Platform and Mobile Install Business

103. Facebook continued to struggle to catch up with the new onslaught of mobile applications, but it recognized that the new apps required aggressive user growth to be profitable. Among other things, Facebook's APIs allowed mobile app developers to query the friends of a

person's friends, which allowed mobile applications to find other users that might be interested in using their apps.

104. Mobile apps also could use Facebook to communicate across Facebook's network, either directly with a user's friends, or with others not directly connected with the user. A mobile payment application, for example, could enable two strangers to pay each other, even if they were not directly connected on Facebook—so long as both of them existed somewhere on Facebook's Platform. A user of a dating application, such as Tinder, could use Facebook's API to find a compatible date, either in the extended network of one's friends or beyond—anywhere on Facebook's platform.

105. Facebook quickly realized that it could monetize the value of its network through third-party mobile applications, and it moved aggressively to do so, beginning with games built to run on Facebook's Platform. Those games, many of which were social games that allowed users to play with and against each other, sought above all else new users to increase their adoption. Facebook's Vernal sought to obtain a beachhead with these applications, monetizing each additional game install that resulted from the use of Facebook's Platform or from Facebook's advertising product, NEKO.

106. For example, Facebook included ads as "stories" on user timelines that indicated whether the user knew other users who were playing a particular game. Facebook then monetized such advertisements when the game obtained new users from them. As Vernal explained in the same May 2012 e-mail:

> The biggest/most efficient market segment for advertising on mobile today is driving app installs. This is at least partly because it's the most measurable—if you know that you get $0.7 from every game you sell, then in theory you can afford to pay up to $0.69/install. This kind of measurability allows for maximal bidding.
>
> So, what we're trying to do is kickstart our sponsored stories business on mobile by focusing on one particular type of story (is-playing stories) and one market segment (games), make that work really well, and then expand from there.

107. Facebook thus leveraged its most valuable asset—the information it had about its users, their interests, and most importantly, their friends—to make money from the proliferation of mobile games.

108. Games like Farmville, a mobile application that allowed players to create their own simulated farms, quickly took off because of Facebook's Platform. Facebook increasingly recognized that it could obtain engagement from users through the game itself.

109. This strategy led to a broader one, in which Facebook drove app installs by allowing developers to advertise to its userbase and traverse Facebook's social network through the Facebook API. Facebook collected a fee for each app install that resulted from its network. Vernal outlined the plan in detail:

> **Roughly, the plan:**
>
> 1/ Create new iOS + Android SDKs, because the current ones are terrible. Ship Thunderhill so we get even broader adoption of our stuff.
>
> 2/ Wire them up to make sure we know when you're playing a game (so we can generate the same kind of is-playing stories we can on canvas).
>
> 3/ Generate a bunch of effective, organic distribution for these games via our existing channels (news feed, net ego on both desktop + mobile). Ship send-to-mobile, which allows us to leverage our desktop audience to drive mobile app traffic.
>
> 4/ Create an even better app store than the native app stores (our app center) and make a lot of noise about it, so developers know that they should be thinking about us to get traffic to their mobile apps.
> 5/ Introduce a paid offering, probably cost-per-install (CPI) based, where you can pay us to get installs from your mobile app. Primary channels for this paid distribution are News Feed and App Center (on desktop + mobile) as well as RHC on desktop.

(emphasis in original).

110. The strategy was clear, not just for gaming, but for mobile apps. Facebook would make money by allowing app developers to leverage its user base. Facebook would advertise social games to its users by plumbing their social data—including data about when they played games and which of their friends played them—and in exchange, Facebook would receive some amount

of money per install, which would be the app developer's cost-per-install (CPI). The same plan would work for mobile applications generally.

111. By the end of 2011 and the beginning of 2012, Facebook began discussing other ways to monetize its Platform, including its Open Graph APIs. One way was to sell API access based on usage. Zuckerberg and top executives at Facebook extensively debated a tiered approach to API access. Facebook deliberated over a pricing model for API access, and internally decided that it would be possible to sell API access to third-party developers. Facebook also decided that it could bundle API access with the ability to advertise on Facebook. However, as explained below, Facebook gave up the profits it could glean from API access for the chance to dominate the Social Data and Social Advertising Markets entirely, excluding competitors (both actual and potential) and leveraging network effects to achieve and maintain monopoly power.

III. FACEBOOK WEAPONIZES ITS PLATFORM TO DESTROY COMPETITION.

A. Facebook Makes Plans to Remove Vital Friends and News Feed APIs and Refuses to Sell Social Data to Competing Application Developers.

112. Although Facebook had made significant amounts of revenue and profit selling access to its social data through its APIs and its NEKO advertising system and had planned to expand that business, it chose not to, sacrificing those significant profits.

113. By the end of 2011 and the beginning of 2012, Zuckerberg along with Facebook's Vice President of Growth, Javier Olivan, its VP of Product Management, Samuel Lessin, and Michael Vernal internally debated a plan to prevent third-party developers from building their own competing social networks that could be capable of generating engagement and social data independent of Facebook's Platform.

114. Emerging mobile applications, such as Line, WeChat, and Instagram were creating their own vast user bases with identity and login features separate from the Facebook Platform. Their increasing ubiquity posed an existential threat to Facebook's core business, which relied heavily on engagement from its user base. These applications provided quintessentially social

applications, such as image sharing, messaging, and payments—a direct threat to Facebook's own applications, including Facebook's own fledgling Messenger application.

115. Mobile applications were rapidly eating away at Facebook's dominance, which relied heavily on its web-based desktop product. Zuckerberg openly acknowledged that its desktop applications were not the future and that native phone apps would dominate the mobile web in the future.

116. Zuckerberg therefore sought to consolidate core applications into its own centralized Facebook application, noting in a March 2012 Q&A with employees that Facebook was "building towards social Facebook versions where you can use the individual app or the Facebook version." That is, users could "replace whole parts of your phone with these Facebook apps and [they] will be a whole package for people."

117. Beginning in the fall of 2011 and well into 2012, Mark Zuckerberg and his chief lieutenants, Lessin and Vernal, planned to address the looming mobile applications threat. Their solution was a scheme to disrupt the massive growth of mobile applications by attracting third-party developers to build for Facebook's Platform and then remove their access to the APIs that were most central to their applications. They would accomplish this by leveraging Facebook's "Friends" and "Timeline" APIs, as well as other vital APIs, including those relating to messaging.

118. The Friends APIs let third-party developers traverse the Facebook Graph, searching through a user's friends, as well as their friends of friends. Zuckerberg and his executives proposed modifying the API to deny third-party developers access to information about a user's friends (and the friends of their friends) unless that developer's application was already installed by a user's friends to begin with. This ensured that new applications could not obtain new users or use Facebook's social data to increase the value of their application.

119. Facebook also foreclosed developers from continuing to extract information about a user's friends from their timeline or news feed. Thus, third-party applications that relied on the stream of information that flowed through a user's news feed, such as a post about a friend of the

user getting engaged or sharing a news article, would be abruptly left with none of the social data they needed to function.

120. Removing access to these APIs halted the growth of tens of thousands of third-party applications that relied on these essential APIs and were, in Facebook's view, threatening Facebook's dominance by eroding the SDBE that protected Facebook's business.

121. Facebook's plan prevented any competitive third-party application from buying social data from Facebook, either through its Platform APIs or through its advertising Platform. As Vernal explained to Lessin in August of 2012, Facebook would "***not allow things which are at all competitive to 'buy' this data from us.***" (emphasis added).

122. Facebook thus refused to sell its social data to any competitive third-party developer, sacrificing significant profits in exchange for a competitive advantage in the Social Data and Social Advertising markets. If not for the prospect of driving these competitors out of the markets in which Facebook competed, the decision to refuse to sell social data to third-party developers made no economic, technical, or business sense.

123. Third-party developers with successful applications increased the value of Facebook's overall network by increasing engagement and generating the very Social Data Facebook sold through its targeted advertising channels, including to developers. As Zuckerberg had observed years earlier, Facebook itself could not broadly develop new third-party apps or anticipate what apps would be successful, so it relied on third parties to do so. Refusing API and social data access to third parties meant that they could not develop the applications that were vital to Facebook's growth, engagement, and advertising revenue. Facebook decided to deliberately sacrifice the value its third-party developers provided to secure dominance in the Relevant Markets.

B. Facebook's Social-Data Heist

124. In May 2012, Zuckerberg decided to use the threat of blacklisting from its Platform to extract precious social data from some of Facebook's competitors. He instructed his executives

to quietly require "reciprocity" from major competitors that used Facebook's Platform. The reciprocity Zuckerberg demanded was the very lifeblood of these competitors' businesses—the social data harvested from user engagement on their competing networks.

125. By the middle of 2012, Facebook began to block some of its competitors from using its Platform and thereby obtaining Facebook's social data. Facebook had already blocked Google, including its competing social network Google+, from access to Facebook's APIs and advertising platform. With respect to Twitter, Instagram, Pinterest, and Foursquare, Facebook would demand "reciprocity" or blacklist them. Reciprocity, of course, meant that these competing social networks would have to hand over their most valuable asset—their social data—to their rival Facebook.

126. If rivals did not comply with Zuckerberg's demands to hand over their social data to Facebook, Facebook would simply take it. In May 2012, Vernal directed his subordinates, Douglas Purdy (Director of Engineering for Platform) and Justin Osofsky (VP of Global Operations), to build "our own hacky scraper" and a "bunch of scrapers" to crawl rival sites like Twitter and Instagram and harvest their social data—with or without their consent. If Twitter or Instagram refused to agree to Zuckerberg's "reciprocity" proposition, Facebook would use the scrapers to obtain the data instead.

127. In August 2012, Facebook considered broadening its list of companies to shake down for social data—or to block entirely from Facebook's Platform. That month, Facebook's then VP of Business and Marketing Partnerships, David Fischer identified other potential product categories and competitive companies in each category to block:

> I'd expect that a large part of the market for our network will come from current and potential competitors. Here's the list that Jud worked up of what we'd likely prohibit if we were to adopt a ban on "competitors" using a broad definition:
>
> - Social network apps (Google+, Twitter, Path, etc.)
> - Photo sharing apps (Picasa, Flickr, LiveShare, Shutterfly, etc.)
> - Messaging apps (WhatsApp, Viber, Imo, KakaoTalk, etc.)

- Local apps (Google+ local, Google Offers, Yelp, yp, etc.)
- Social search apps (HeyStaks, Wajam, etc.)
- Platforms (Google Play, Amazon, etc.)

128. Facebook thus identified its direct, horizontal competitors in the Social Data and Social Advertising Markets. These categories of competing applications, particularly on mobile platforms, threatened Facebook's business because they created social networks independent of Facebook, each capable of generating their own valuable social data. If Facebook lost control over these companies, it would lose access to the social data they generated, which meant Facebook's own product could not drive engagement and sell advertising.

129. In August 2012, Facebook gave a presentation to its Board of Directors that included various revenue models to monetize its Platform, including its APIs. The Board understood that Facebook could monetize its platform by charging per company, per application, per user, or per API call.

130. But Facebook opted to do none of those things. Instead, it decided to sacrifice those profits to obtain complete control over the growing mobile application and advertising markets, thereby maintaining and furthering its dominance of the Social Data and Social Advertising Markets.

131. Facebook's plan was to instead block competitors from using its Platform, thereby preventing them from eroding the SDBE that protected Facebook's business. In the case of a select few companies with social data that Facebook needed to maintain and grow its own business, however, Facebook would coerce them into agreements to share their most valuable social data with Facebook. If they refused, Facebook would blacklist them and take it from them anyway with its own crawling software that would scrape their public-facing site for information.

132. In September 2012, Zuckerberg formalized his order to shut down the Friends and News Feed/Timeline APIs and to coerce rivals into providing their valuable data to Facebook on pain of blacklisting. On October 30, 2012, Vernal notified his subordinates of Zuckerberg's decision:

> We are going to dramatically reduce the data we expose via the Read API . . . . We are going to change friends.get to only return friends that are also using the app . . . . Since friends.get will only returned other TOSed users' data [data from users that agreed to an application's terms of service], that means we no longer need the friends_* permissions. We are going to remove/whitelist access to the Stream APIs [the News Feed API]. We are going to limit the ability for competitive networks to use our platform without a formal deal in place . . . . We are going to require that all platform partners agree to data reciprocity.

133. This decision meant several things: (1) when a third-party application called the Friends APIs, it could not obtain information about a user's other friends unless those friends already had installed the application; (2) the News Feed APIs would no longer provide information about a user's connections; (3) access to those API could be "whitelisted" for third-party developers that were offered—and agreed to—data reciprocity; and (4) reciprocity would be required for any access to the APIs.

134. In November 2012, Osofsky, who was then head of Facebook's Platform, summarized the policy changes required by the decision:

> Policy changes: define competitive networks + require they have a deal with us, regardless of size. Maintain size-based thresholds for all other developers to force business deals. Require data reciprocity for user extended info to ensure we have richest identity.

135. Facebook knew that these changes would eliminate the "growth channel used by 23% of all Facebook apps" and that 89% of the top 1,000 iPhone apps relied on the full friends list API, with 75% of the top 1,000 iPhone apps relying on the Friends permissions APIs. Facebook determined that popular applications on its platform with millions of customers would break as a result of the decision, including FarmVille, ChefVille, CityVille, Skype, Spotify, Xobni, Texas Holdem, Yahoo!, Trip Advisor, Microsoft's Birthday Reminders, Samsung's clients, Glassdoor and dozens of others.

136. On November 19, 2012, Zuckerberg broadly announced his decision to block competitors or require full data reciprocity for continued access. Facebook's COO Sheryl Sandberg immediately ratified the decision, adding that "we are trying to maximize sharing on

Facebook, not just sharing in the world," with the note that the distinction was a "critical one" and the "heart of why."

137. Facebook began preparing its 2013 plan for its mobile advertising business, which included the launch of a new version of its Platform, version 3.0. Platform 3.0 would (according to Facebook) facilitate Facebook's transition from its desktop advertising business to a mobile advertising business. A central element of the transition plan was the implementation of Zuckerberg's decision to remove the Friends and News Feed APIs.

138. Vernal explained Zuckerberg's decision to other Facebook employees in November 2012, noting that he believed the amount of data that Facebook required from competitors was "crazy":

> [A company must share] every piece of content by that user that can be seen by another user. What Mark is saying is he wants certain partners (I assume not all) to give us news feeds on behalf of their users, which is kind of crazy.

139. Facebook continued to formalize its plan to require the right to crawl the sites of its competitors as a condition of access to its Platform. In November 2012, Facebook's Group Product Manager, Rose Yao explained the scheme:

> We also reserve the right to crawl a partner website for the user's data. Partners cannot blacklist or block Facebook from crawling your site or using the API. If they do, Facebook reserves the right to block the partner from using our APIs . . . . The theory behind Action Importers was that we needed to balance the leverage. You can call our APIs and access our data, as long as we can call your APIs (if you have them) or crawl your web site (if not) and access your data. It's one thing to drag your heels, but if we're the ones doing the work then we force you to make a decision—either you allow us access to your data, or you block us. If you block us, then it's really easy/straightforward for us to decide to block you. What's changed? ***When we first started discussing this, we were talking about doing this only for top partners. I think a lot of folks interpreted this as just a negotiation tactic—we'd just threaten to do this if they didn't cooperate. What's changed between then and now is that this is now very clearly not a negotiation tactic—this is literally the strategy for the read-side platform.***

(emphasis added).

140. Thus, what began as a negotiation strategy to extract social data from rivals became the foundation of Facebook's Platform strategy. For competitors that posed enough of a threat to create their own rival network, Facebook required them to hand over the only leverage they had—the social data they derived from their users' engagement.

141. For some rivals that directly competed, no amount of data would justify access to Facebook's Platform, and for nascent threats that relied on Facebook's platform that did not have any useful data to extract, Facebook's decision was to simply cut off their access to the Friends and Newsfeed APIs, killing their businesses almost immediately.

142. Vernal expressed concern about the strategy to Zuckerberg in November 2012, noting that he was skeptical that competitors such as Pinterest would allow Facebook to take their social data. If they, as well as others, did, Facebook would become a central exchange for data collected among competitors. That is, competitors would share the data to Facebook and Facebook would then share that data back to the competitors that participated in the scheme. ***Facebook would become a data-passthrough mechanism***.

143. In December 2012, despite recognizing that API access, particularly when bundled with Facebook's NEKO advertising platform, was profitable, Facebook decided not to charge for API access and began full implementation of Zuckerberg's decision.

144. Although Facebook had planned to announce its decision not to allow access to Friends data through its Friends and News Feed APIs in a public blog post, Zuckerberg vetoed that decision in December 2012. Instead, Zuckerberg decided to enforce the decision selectively and covertly after deliberately analyzing Facebook's competitors. Some competitors would be blocked entirely from the APIs, while some select few would be blocked only if they did not provide their own social data to Facebook.

C. Facebook Targets Its Competitors for Reciprocity or Denial of API Access.

145. Beginning in January 2013, Facebook began an internal audit of all of the applications that relied on its Platform. It immediately identified competitors to shutdown entirely

from accessing Facebook's APIs or advertising platform. Specifically, Zuckerberg ordered that WeChat, Kakao and Line be restricted from using the Friends and NewsFeed APIs and even from advertising on Facebook's NEKO and other platforms.

146. Facebook's David Fischer balked at the decision, noting that blocking competitors even from the advertising platform was irrational and unworkable:

> I continue to believe we should allow ads from competitors for several reasons: We should be secure enough in the quality of our products to enable them to compete effectively in the open marketplace . . . . It looks weak to be so defensive. This will be a challenge to enforce. We have many competitors and the list will grow in time. How will we judge retailers and e-commerce sites as we grow Gifts, since they arguably are competitors too?

147. Fischer was right. The decision made no rational economic or business sense. The sole purpose of refusing to sell social data as part of the Facebook Platform or through advertising was to shut out competition and allow Facebook to dominate the Social Data and Social Network Markets. Aside from that anticompetitive purpose, the decision to refuse to sell social data or advertisements even at full price was so facially irrational that Facebook's own employees who may not have been fully privy to the anticompetitive scheme protested at the irrationality of the decision.

148. That same month Facebook's Osofsky pleaded with Vernal to make an announcement that would send a clear signal to developers, but Vernal responded that Zuckerberg had already rejected that approach. As Vernal explained, telling developers about the decision means bearing the "very real cost" of "changing the rules," including the "PR cost" of betraying developers that Facebook had induced to build for Facebook's APIs and Platform.

149. That same month, Facebook continued to implement Zuckerberg's decision to blacklist competitors. He ordered that Facebook competitor Vine be "shut down" from Facebook's API and Platform, including from advertising. Facebook had again sacrificed the profits it would glean from increased engagement and advertising revenue as a result of Vine's use of Facebook's Platform in exchange for the exclusion of Vine from the competitive landscape.

150. Indeed, Facebook's mobile advertising platform was growing rapidly, and blocking large companies from using it made no economic sense other than to effectuate Zuckerberg's scheme to prevent rivals from competing with Facebook. In a January 20, 2013 email, Facebook's then-Director of Product Management and Platform Monetization team, Deborah Liu reported: "Neko grew another 50% this week! Hit a high of $725k Friday (see charge below). We are now 5% of total Ads revenue and 21% of mobile ads revenue."

151. Lessin responded to the news: "The neko growth is just freaking awesome. Completely exceeding my expectations re what is possible re ramping up paid products."

152. Liu was clear, however, that the increased revenues occurred notwithstanding the blacklisting of formerly large spenders, such as WeChat: "WeChat and other competitive networks are no longer advertising on Neko based on policy."

153. In February of 2013, Facebook shut down Yahoo!'s access to key APIs, resulting in direct negotiations between Yahoo!'s Marissa Mayer and Facebook's Sheryl Sandberg in order to restore Yahoo!'s access to the Facebook Platform.

154. In March 2013, Facebook's key Platform employees began to voice concern that the approach taken by Facebook of shutting down access and then coercing "data reciprocity" was problematic. They instead encouraged making an upfront announcement that the APIs would be unavailable and then negotiating a deal for access to Facebook's Platform. In an e-mail that month from Purdy to other Facebook employees and executives, he wrote:

> I have been thinking about the challenges around reciprocity and competitive enforcement (friends.get, etc.) and fact that ***it is all post facto***. The way we are structured today, you build an app on FB and then launch and then we may just shut you down, harming users and the developer. I wonder if we should move as quickly as possible to a model in product where all you get from platform is login (basic info) and sharing without approval. All other APIs are available in development, but have to be approved before the app launches to real users (basically all apps using friends.get have to have that capability approved). We are roughly on course to deliver this as part of unified review, save for the more granular approval for things like friends.get? What I love about this too is we could make our whitelists so much cleaner by making each capability an approval

> thing. Marie: I think makes your "deprecations" much easier. Thoughts?

155. Although Facebook moved towards full deprecation of the APIs with the exception of those with whitelisting agreements, it continued its campaign of quietly shutting down competitors' access to the APIs and then asking them to make a reciprocity deal. Indeed, Facebook soon thereafter shut down three competing Amazon apps, resulting in Amazon protesting that the decision "will break 3 of our live integrations."

156. That same March in 2013, Facebook used API and Platform access as leverage to acquire rival Refresh.io. Facebook internally decided that it would threaten Refresh.io with denial of access to the APIs unless it sold its business to Facebook. That same form of leverage would be used to acquire other rivals—either they sold to Facebook or they saw their business ejected from Facebook's Platform.

157. In 2013, Facebook also began using mobile spyware company Onavo to secretly track application usage on customers' phones. Onavo, through deceptive terms of service, tracked app usage in real time, and Facebook used that data to target specific competitors. By April 2013, Olivan was using Onavo to track Snapchat, Pinterest, WhatsApp, Tumblr, Foursquare, Google, Path, vine, Kik, Voxer, MessageMe, Viber, GroupMe, Skype, Line, and Tango. One internal Olivan presentation contained detailed usage data for these applications from August 2012 to March 2013.

158. By July 2013, Onavo data was providing detailed intelligence to Facebook on 30 million Onavo users. Among all of the apps, the data showed the meteoric rise of WhatsApp, a direct competitor to Facebook's own fledgling product, Messenger.

159. Armed with detailed intelligence about its competitors—both on and off the Facebook Platform—Facebook ordered a detailed audit of Facebook applications that relied on the Friends and News Feed APIs.

160. Facebook's Director of Developer Platforms & Programs, Konstantinos Papamiltiadis, reported back that there were 40,000 apps using the APIs that were to be restricted, with 7% of them being photo or video sharing apps.

161. Facebook then began to categorize these third-party applications into three general categories: (1) developers that "may cause negative press" if their access to APIs were shut down; (2) applications that "provide strategic value"; and (3) applications that were "competitive" or "not useful to FB. Application developers that would experience "a Major Business Disruption/Kill" as a result of the restriction of API access received a "PR flag."

162. In response to the categorization, Lessin immediately ordered his subordinates to "shut down access to friends on lifestyle apps . . . because ***we are ultimately competitive with all of them***." (emphasis added).

163. As Facebook continued its analysis of the applications that relied on the Friends and Newsfeed APIs, it became clear that Facebook's plan would result in the deprecation of the "majority of the API surface"—namely, the APIs that were the most essential parts of the Facebook Platform.

D. The Decision to Remove Developer Access to the Friends, News Feed and Other Crucial APIs Lacked Any Legitimate Justification.

164. The engineers tasked with implementing Zuckerberg's decision to restrict access to the APIs were baffled. The decision made no technical sense whatsoever. Indeed, there was no justification for it other than to squelch competitors who threatened Facebook's dominant position and SDBE.

165. As Facebook engineer, David Poll, had written to all Platform Engineers earlier in 2011, the decision would mean gutting the Facebook Platform of functionality used—and needed—by some of the most important mobile apps built on Facebook's Platform:

> I was thinking about the Platform 3.0 friend list change a bit as I was using my Android phone tonight and realized that two for the apps that most impact my day-to-day mobile experience will be completely, irrevocably broken by this change . . . . In both of these cases, the apps are adding real value to my experience, and in both

> of those cases, I have zero expectation that any of my friends will be using the app. The fundamental problem I'm having with this change is that my friend list is my information—it's part of who I am, and for Facebook to shut down this access primarily comes across to me as FB intruding upon and shutting down my own access to my own information.

166. Poll concluded, "No matter how you slice it, this change is going to have a significant negative impact on my day-to-day smartphone experience."

167. Poll was correct. The change meant breaking applications that added significant value to Facebook's network and increased valuable user engagement on Facebook's core product. The decision to deliberately break these applications had only one plausible purpose—to strengthen the SDBE and to ensure that competitors could not create rival social networks that could compete with Facebook.

168. That proposition was entirely obvious to those responsible for Facebook's Platform. In an August 2013 e-mail, senior Platform engineer Bryan Klimt wrote to Ilya Sukhar, Facebook's Head of Developer Products and Senior Engineer working on its APIs, and others working on Facebook's Platform, stating that the reason for the decision to block access to the Friends and News Feed APIs was to exclude competitors and that all other reasons were simply false and pretextual. To begin with, Klimt was clear that the removal of the APIs was "ridiculous" because they were so essential to the Facebook Platform:

> I'm trying to write a post about how bad an idea it would be to remove the api that lets you get a list of user's friends from Facebook Platform. In order to illustrate my point, I'd like to satirically suggest removing some API that is so core to the developer experience and that removing it would be ridiculous on its face. For example, removing the Windows API method that lets you create a new window. Or removing the Twilio API method that lets you send a text message. Both suggestions are utterly insane. The problem is, for Facebook Platform, removing the method to let you get a list of friends literally is already that ridiculous. I can't think of an example more ridiculous to parody it with.

169. Klimt then dispelled any notion that the APIs were being removed for any technical or functionality-driven reason:

> Before we discuss in more detail, I'd like to clear up some misconceptions about the deprecations. I've heard some rumors

> floating around about why we are doing this. But many of them are clearly pablum designed to make engineers think this decision has solid technical reasons. It does not. 1/ This API can be abused so we can remove it. False. That is a non-sequitur. Lots of APIs can be abused. Our whole product can be abused. That's why we have one of the best teams in the industry at detecting and stemming abuse. That team, plus Unified Review, is more than sufficient to deal with any theoretical abuse coming from this API. Even if this were true, who wants to be in that classroom where the whole class is punished for transgressions of a few?

170. Klimt also was clear that the APIs were not being removed in favor of new or different APIs providing the same features:

> 2/ It's okay to remove because we've provided alternatives for common uses. False. If you think that's true, then I don't think you realize why developer platforms exist. If we wanted to limit Facebook to the set of use cases we've already imagined, we could just do that ourselves, and not even have a Platform. The purpose of a Platform is to let people build new things on top of it. It's to enable the whole universe of ideas that anyone in the world could think of. Developers out there will have all sorts of crazy ideas. We want them to build those crazy ideas on top of Facebook. Do you know why Facebook was originally built for the WWW instead of being part of CompuServe or AOL's proprietary networks? It's because the web is an open and extensible platform. It lets developers make their craziest become reality.

171. Klimt then explained that the real reason was to hurt Facebook's competitors and prevent them from competing with Facebook:

> So, if neither of those reasons explains why we are doing this, what's driving it? The only reason I've heard that makes sense is that we are worried about people "stealing the graph", ***we are doing this as a protectionist grab to make sure no one else can make a competing social network by bootstrapping with our social graph***. Okay, so let's assume for a minute that the social graph does belong to us, and not to our users. And let's even go so far as to assume that this is a real problem, although, I'm not convinced it is. I mean, concerns that other companies will steal our friend graph may just be paranoia. But for the sake of argument, let's say it's not. Then what? ***We're removing the core API in our developer platform. Out of concerns that someone will steal our social network product.*** That sends a clear message to developers: Facebook Platform comes second to Facebook the Social Network Product. This has been a criticism all along with our Platform. When you go read the blog posts critical of our Platform, they all hit on this same point. When our APIs are subjugated to the whims of our other products, they can't be stable. And an unstable platform isn't really a platform at all. So then you are left with 2 big problems. 1/ How do you convince external developers to build on a platform where the most

> basic core APIs may be removed at any time? I mean, the only big value we bring to the table right now is in distribution and discovery, and that's going to encourage developers to do only the most superficial integration with Facebook. Basically, they're going to do just enough to be able to use Neko ads. 2/ How do you convince internal developers to work on Platform knowing it's only ever going to play second fiddle to the rest of the company? I mean why should any of us work on a product that could be crippled at any time to benefit another team? If I worked on Platform, I would be seriously reconsidering my options if this API gets deprecated.

(emphasis added).

172. Klimt was clear—the decision to remove the APIs lacked any technical or business justification other than to prevent a competitor from creating a competing social network, eroding the SDBE protecting Facebook's business. Any proffered justification by anyone at Facebook to the contrary was entirely pretextual.

173. Moreover, the decision to remove the APIs permanently destroyed the value of Facebook's Platform. If developers could not trust Facebook to maintain the APIs as stable parts of its Platform, they would not risk writing apps for the Platform in the future. The decision meant scuttling Facebook's valuable Platform for the ability to prevent a rival social network from taking hold.

174. Sukhar responded to Klimt, noting that he agreed and that he "talks about this every single meeting." His pleas to Vernal, Purdy and Zuckerberg to reverse their decision fell on deaf ears. The decision had been made and Klimt and Sukhar would have to implement it.

175. Facebook continued its audit of apps that relied on the APIs. Most of the Apps were important to the Facebook ecosystem. Indeed, Facebook acknowledged they "are not spammy or crap, but apps users like a lot." Nonetheless, Facebook's Papamiltiadis concluded that, among others, apps like Sunrise, Yahoo!, IFTT, Friendcaster, MyLife, Sync.me, YouTube, Contacts+, and Bitly "overlap with Facebook products" and "could compromise our success in those areas."

176. Facebook's careful monitoring of competitive apps continued well into 2013, and given its heavy reliance on data secretly collected by Onavo, Facebook purchased Onavo on October 14, 2013. Facebook used that data to determine which apps competed with its social

network and thus posed a threat to the SDBE. It then targeted those companies for withdrawal of API access and coerced data reciprocity agreements.

177. In October 2013, Facebook's Purdy reported that Facebook was dividing apps into "three buckets: existing competitors, possible future competitors, developers that we have alignment with on business model." Facebook's Eddie O'Neil believed that the "separation between those categories doesn't feel clean" and that the overlap was problematic. As O'Neil observed, "apps can transition from aligned to competitive and will ultimately make us sad that we leaked a bunch of data to them when they were aligned."

178. Sukhar objected to the entire exercise, noting that he had been speaking to many dozens of developers "who will get totally fucked by this and it won't even be for the right reason." Sukhar explained that his "engineers think ***this plan is insane*** and I'm not going to support an all hands [meeting] to convince them otherwise." (emphasis added).

179. As Sukhar noted, the decision to withdraw the Friends and News Feed APIs from the Platform made no technical sense whatsoever, and Sukhar could not bring himself to tell his engineers—who saw through the ruse—otherwise. It was obvious that Facebook was seeking to squelch potential competition—namely, by preventing user growth and engagement for competitive apps. As one Facebook engineer commented about the obvious purpose of the plan to remove the APIs: "I understand we want to make it hard for a developer to grow a new app."

180. The review of apps continued and specific decisions with respect to certain highly sensitive competitors were escalated to Mark Zuckerberg. As one internal Facebook e-mail explained:

> We maintain a small list of strategic competitors that Mark personally reviewed. Apps produced by the companies on the list are subject to a number of restrictions outlined below. Any usage beyond that specified is not permitted without Mark level signoff.

181. In December 2013, Klimt complained to Sukhar about the audit and categorization process:

> So we are literally going to group apps into buckets based on how scared we are of them and give them different APIs? How do we ever hope to document this? Put a link at the top of the page that says "Going to be building a messenger app? Click here to filter out the APIs we won't let you use!"
>
> And what if an app adds a feature that moves them from 2 to 1. Shit just breaks? And messaging app can't use Facebook login? So the message is, "if you're going to compete with us at all, make sure you don't integrate with us at all."? I am just dumbfounded.

182. As Poll recognized in response to Klimt's complaint, the changes to Facebook's Platform were "more than complicated, it's sort of unethical." Klimt agreed with the assessment, noting that the API removal "feels unethical somehow . . . . It just makes me feel like a bad person."

E. Facebook Prepares to Announce Removal of the APIs.

183. Zuckerberg decided to announce the API removal under the cover of a major change to the Facebook Platform, codenamed PS12N, which would be announced at the next Facebook F8 Developer Conference. Facebook's engineers were accordingly instructed in September 2013 to bury the changes to the API and announce them quietly along with the changes that would be announced at the conference.

184. In the run-up to its API withdrawal announcement, Facebook continued its audit of applications on its platform that were using the APIs. During that process Facebook continued to classify potential competitors, including LinkedIn and AirBnB, as companies that would be denied access with no whitelist exception.

185. Although Facebook knew that the APIs were going to be removed by the next F8 conference, it continued to tell developers to rely on them. As a Facebook Platform evangelist noted about one particular document frequently shared with developers, "the language in here around friend permissions is very counter to our upcoming platform simplification efforts" and "feels against the spirit of where we are headed."

186. That was, however, precisely what Facebook wanted—to continue to entice developers to build their software and their businesses on APIs that made them dependent on

Facebook. The use of the APIs meant that competitors could be abruptly shut out of the market, useful apps could be extorted for valuable social data, and the rest could simply be destroyed.

187. By October 2013, Facebook required certain application developers it chose to whitelist to sign Private Extended API Agreements, which obligated them to purchase certain amounts of social data through advertising or to provide their own valuable social data to Facebook in exchange for continued access. That month, for example, Facebook whitelisted Royal Bank of Canada's application in exchange for the purchase of social data through Facebook's NEKO advertising platform.

188. Facebook catalogued and tracked developers on its platform that would likely complain about the decision, creating negative press. Facebook's internal employees tasked with crafting a PR message explained the undertaking in a December 2013 e-mail:

> In prep for Platform Simplification, we're putting together a list of developers who we think could be noisy and negative in press about the changes we're making: Primarily we think it will be a list of the usual suspects from past policy enforcements. We'd love to pull from your historic knowledge on the topic. Is there anybody you'd add to the list below? We're going to build plans around how we manage and communicate with each of these developers. There are also comms plans in the works for working with developers who are high ad spenders and friends of Mark/Sheryl."

189. Facebook planned to manage its message carefully, as its decision likely would alienate even those developers who were making large purchases of social data from Facebook through ads and/or who were friends of Facebook's two most senior executives, Zuckerberg and Sandberg. Those developers were identified and the message to them was carefully crafted to avoid a PR disaster. For most application developers, however, the decision would result in the complete exclusion of their applications from Facebook's ecosystem—which would likely be fatal to their businesses.

190. Facebook targeted potentially "noisy" or "negative" developers individually, including, but not limited to, the following applications and developers: iLike, Rock You, Zynga, Path, Flipboard, Slide, Social, Fixer, SocialCam, Viddy, BranchOut, Vince, Voxer, Message Me,

Lulu, Anil Dash, Super Cell, Kabam, Washington Post, Guardian, The Wall Street Journal, Jason Calacanis, Cir.cl, Bang with Friends, Tinder, Social Roulette, App Wonder, Ark, Vintage Camera, and Girls Around Me.

191. Facebook also used call-log data secretly collected by Android users to target developers and applications to be shut down.

192. The entire process led Facebook engineer George Lee to lament:

> We sold developers a bill of goods around implicit OG [Open Graph] 2 years ago and have been telling them ever since that one of the best things they could do is to a/b/ test and optimize the content and creative. Now that we have successes. . . . We're talking about taking it away . . . . [Developers] have invested a lot of time to establish that traffic in our system . . . . The more I think about this, the more concern I have over the pile of asks were [sic] making of our developers this year. PS12N is going to require them to alter how they deal with APIs (and for limited value).

193. Thus, as Facebook continued to prepare its API withdrawal announcement, Facebook's own executives recognized that Platform developers had been conned into relying on Facebook's APIs. Facebook knew full well that it intended to remove the APIs, but it allowed and encouraged developers to build entire businesses on and around them. As Lee put it, they were sold a "bill of goods."

194. By 2014, it was clear that with the exception of a few apps and developers, most would be denied access entirely to the Friend and News Feed APIs.

195. In January 2014, Zuckerberg debated denying API access to dating apps. Facebook decided that it would whitelist Tinder and other anointed dating apps and shut down the rest, clearing the way for the selected apps to dominate the dating market. Zuckerberg reasoned that although Facebook would ultimately create its own dating app, it would let Tinder and a select few others to survive until Facebook's competing app was ready:

> I've been thinking a lot about Tinder and other people recommendation apps since about 10% of people in many countries are using a Tinder now. People recommendations seems like something that should be right up our alley, but it's currently something we're not very good at. Tinder's growth is especially alarming to me because their product is built completely on

> Facebook data, and it's much better than anything we've built for recommendations using the same corpus . . . . I think this is a big and important space and it's something we should have a team working on—probably to develop people recommendation Hunch sections for now.

196. Zuckerberg became increasingly involved in assessing whether individual apps would be whitelisted when the APIs were removed. Facebook's senior-most executives accordingly prepared recommendations for his consideration. In a January 2014 presentation entitled, "Slides for Mark," for example, Facebook employees summarized the results of the ongoing app audit. The presentation observed that the changes would make it "impossible to build" an app without a whitelist agreement with Facebook. The presentation made special recommendations for apps that purchased large amounts of social data through Facebook's NEKO platform or whose developers were friends with Zuckerberg or Sandberg. The bulk of the 41,191 apps that relied on the Friends or News Feed APIs, however, would be shut out and, as a result, completely destroyed.

197. Although the effect on these apps was clear, Facebook continued to evangelize the APIs to developers. In January 2014, Facebook's George Lee sounded the alarm to Purdy and Vernal, which fell on willfully deaf ears:

> [P]artner managers are still selling products that we ask them to sell, so when it comes to feed integration, we're still telling people to use [Open Graph]. The last f8 was all about implicit [Open Graph], so while we may have decided amongst ourselves that this is no longer the future without an alternative we don't have anything to tell current [developers] (so partners continue to tell them to use [Open Graph] and they continue to integrate it).

198. The plan to quietly take away the APIs in favor of a new crippled developer platform was called the "switcharoo plan" by Facebook's engineers. It was clear to all involved that the announcement of the changes to the platform at the upcoming F8 conference was cover for the radical changes Facebook planned to make to its platform—namely, the removal of the Friends and News Feed APIs.

199. During March 2014, Facebook's engineers and employees continued to be baffled by the upcoming decision. As one employee noted:

> It seems a bit odd that we block other developers from doing things on our platform that we're ok with doing ourselves. Do we consider ourselves exempted? That seems a little unfair especially when our stance on some of these policies is that they're about ensuring trusts and a great experience. My mental model on how platform is a level playing field could be way off though.

200. The decision made no sense to Facebook's own employees, particularly because Facebook itself needed the APIs to make their own competing applications, including Facebook's Messenger application. Facebook's executives ignored all of the concerns raised by their employees, including their API engineers, and continued to drive towards the announcement of the removal of the APIs at F8.

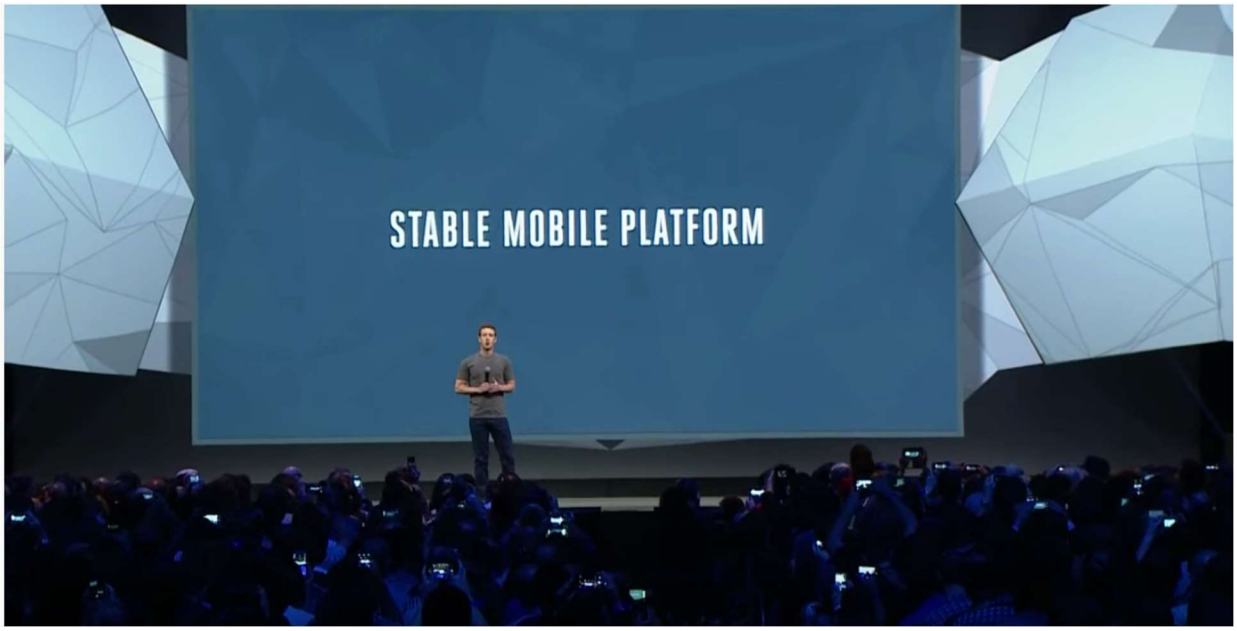
201. The real reason for the removal of the APIs was kept tightly under wraps. In April 2014, right before the announcement, Vernal warned Sukhar that if any mention was made of the competitive reasons for the removal of the APIs (as Sukhar wanted), there would be a "high likelihood of breaking into jail."

F. The Announcement at F8

202. On April 30, 2014, Facebook announced "The New Facebook Login and Graph API 2.0" on Facebook's website. Facebook heralded changes to its new Login system for several pages. Buried in the announcement was a quiet statement about the Platform's most important APIs—the Friend and News Feed APIs: "In addition to the above, we are removing several rarely used API endpoints; visit our changelog for details."

203. These APIs were not ***rarely used*** at all. Tens of thousands of third-party apps were actively using and building on the APIs. Internal Facebook engineers likened them to essential APIs in Microsoft's Windows and were outraged at the removal. Five of the top ten Facebook Apps surveyed in December 2012 relied heavily on them. The announcement was entirely false and was deliberately buried beneath other API announcements to avoid drawing attention to the competition-crippling effect of the decision. In fact, today, the changelog referred to in the announcement is no longer accessible on Facebook's page even though years of other changes are.

204. When Mark Zuckerberg took the stage at F8 days later for his keynote speech, there was no mention of the removed APIs. Instead, Zuckerberg emphasized the "stability" of Facebook's mobile platform just as Facebook quietly removed some of the most heavily relied-upon and necessary APIs in Facebook's Platform.



205. At the twenty developer sessions preceding the announcement, not one mention was made of the API removal or that the upcoming changes would simply break nearly all of the more than 40,000 third-party apps that relied on the APIs. After April 30, 2015, the APIs were no longer part of any available version of Facebook's Platform.

206. Facebook thus had successfully destroyed any application that could possibly create a product that could threaten the SDBE that protected Facebook's dominant position and market power. A select few would be required to hand over their most valuable resource—their social data—to their behemoth competitor in exchange for continued access.

IV. THE WHITELIST AND DATA SHARING AGREEMENTS

207. After the announcement and through the full removal of the APIs in April 2015, Facebook continued to make a series of agreements that forced certain competitors to hand their data over to Facebook. For example, Facebook forced certain third-party developers that it

identified as competitive threats with valuable social data to sign Private Extended API agreements—referred to throughout this Complaint as "Whitelist and Data Sharing Agreements" or simply "the Agreements"—in order to obtain access to the Friends and/or News Feed APIs.

208. Facebook's Whitelist and Data Sharing Agreements, as of January 2015, included a provision that acknowledged that the APIs they covered are not available to the general public. An exhibit to each Whitelist and Data Sharing Agreement listed the specific Facebook APIs to which a particular developer was being granted access.

209. These Agreements were only offered in exchange for massive purchases of Facebook's social data through mobile advertising and/or through the provision of the developer's own social data back to Facebook (so-called "reciprocity").

210. As Facebook executives and engineers understood and acknowledged in internal communications, this scheme allowed Facebook to serve as a "data pass-through" among competitors. Competitors with Whitelist and Data Sharing Agreements provided social data to Facebook, which served as a hub that sold data obtained from one competitor to another whitelisted competitor.

211. The result of the network of Whitelist and Data Sharing Agreements was a hub-and-spoke agreement to control the supply of social data. Those who obtained access to the Facebook APIs were required to both provide social data to the hub (Facebook) and to purchase social data from it. If a developer refused to participate in the scheme, it was excluded entirely from Facebook's Platform because the most important APIs—the Friends and News Feed APIs—would not be available to it.

212. In January 2015, Facebook provided Whitelist and Data Sharing Agreements to the dating apps Tinder and Hinge, because of the value of the social data those applications produced.

213. In February 2015, when Airbiquity (another third-party developer) sought a Whitelist and Data Sharing Agreement, Facebook lied to them, telling Airbiquity that the specified

APIs "won't be available to anyone" after April 30, 2015, and that "all similar integrations will be subject to the same deprecations/restrictions."

214. That same month (February 2015), Facebook secretly signed Whitelist and Data Sharing agreements with other third-party developers, including Netflix, Nissan, and Lyft.

215. In April 2015, Facebook's manager of strategic partnerships, Ime Archibong, internally celebrated the fruition of Facebook's three-year plan to eliminate its competition through Platform changes: "Three years coming, but the 'Platform Simplification' initiative finally lands this week."

216. Also in April 2015—as Facebook finally cut off all public access to the Friends and News Feed APIs—Facebook continued to receive requests for Whitelist and Data Sharing Agreements from companies such as Microsoft, Hootsuite, and Walgreens.

217. Facebook had already extracted valuable social data from dozens of competitors, including Foursquare and Pinterest, in the run-up to the announcement and ultimate removal of the APIs. Without discovery, the precise number and identity of those who entered into Whitelist and Data Sharing Agreements with Facebook cannot be known for certain, but publicly available information indicates that dozens of app developers entered into such Agreements with Facebook. Pursuant to these Agreements, dozens of app developers agreed to provide social data to Facebook and to purchase competitor and/or Facebook social data back through advertising. Together, these companies formed a hub and spoke scheme to restrict competition in the Social Data and Social Advertising Markets.

218. There was no pro-competitive benefit to the Agreements, as they were naked restrictions on the supply of Social Data. The anticompetitive effects, however, were staggering and facially apparent. Absent the Agreements and Facebook's overall anticompetitive scheme to exclude third-party developers, other companies would have created their own social data through the proliferation of their own competing social networks. The engagement on their competing networks and the social data generated from that engagement would have increased the value of

their networks because of network effects. As the amount of social data generated and monetized on these competing networks increased, Facebook's SDBE would erode, potentially driving more users to new platforms.

219. None of that could happen as long as Facebook could coercively demand all of the valuable social data generated on any competing platform. The Whitelist and Data Sharing Agreements ensured that competitive threats such as Foursquare could not accumulate enough social data to create their own feedback loop in—and perhaps come to dominate, through network effects—any market in which Facebook anticipated competing or actually competed.

220. The Agreements also ensured that Facebook's decision to destroy forty thousand applications built on the Friends and News Feed APIs would be effective—and remain so. If Facebook did not control the supply and sale of social data, excluded developers could simply build their applications on another platform. But by entering into a network of Whitelist and Data Sharing agreements, Facebook ensured that no such competing platform could arise. The Agreements strengthened and preserved the SDBE and/or prevented the proliferation of rival generators of social data and third-party developer platforms.

221. The Whitelist and Data Sharing Agreements were thus both in and of themselves anticompetitive and part and parcel of Facebook's overall anticompetitive scheme to maintain and expand its dominant position in the Social Data and Social Advertising markets described in this Complaint.

222. In a world where no such Agreements existed, a rival such as Pinterest or Foursquare would obtain more engaged users, resulting in more social data that those competitors could monetize through their third-party or advertising platforms. The thousands of developers denied access to Facebook's Platform would therefore build their applications on Foursquare or Pinterest instead of simply going out of business or changing their products/businesses dramatically to survive. By forcing those and other similarly situated companies to hand over their

social data, Facebook made sure its Platform would be the only viable platform upon which a third-party social application could be built.

223. As explained in the next section, the only remaining threat to Facebook's Social Data and Social Advertising dominance was from a completely independent competitor that did not rely on Facebook's Platform, and thus could not be extorted into handing over its data in exchange for API access. For such companies, Facebook would pay any price to remove them from the market—and use their assets to strengthen Facebook's SDBE.

224. But first, Facebook had to identify such threats to its market dominance. Enter Onavo.

V. THE SURVEILLANCE AND ACQUISITION OF COMPETITIVE THREATS

225. To ensure that its scheme to maintain and expand its market power would work, Facebook had to control an important source of competition: independent social networks and producers of social data. Although Facebook could simply destroy any competition that relied on its Platform by denying access to essential APIs, this would do nothing to stop a competitor that was growing its network of engaged users entirely independent of Facebook.

226. To detect such threats before they became too formidable, Facebook sought a way covertly surveil millions of mobile users to determine what applications they were using, and how. Mobile applications were particularly important—and concerning—to Facebook, as desktop engagement was shrinking while mobile apps rapidly proliferated. By 2012, it was clear to Zuckerberg and to Facebook that any threat to its dominance would come from a mobile application. As explained in this section, Facebook used mobile spyware on an unprecedented scale to surveil, identify, and eventually remove from the market through acquisition competitors that independently threatened Facebook's dominance and/or the SDBE protecting its monopoly, market power and business.

A. Facebook Relies on Onavo's Surveillance of Facebook's Competitors, and Acquires and Uses Onavo's Assets

227. Onavo was an Israeli mobile web analytics company founded by Roi Tiger and Guy Rosen in 2010. The company designed spyware designed to surveil users as they used their mobile devices. To obtain extensive information on a user's usage of mobile applications and of bandwidth, Onavo cloaked its spyware in virtual private networks ("VPNs"), data compression, and even in mobile privacy apps.

228. Onavo sold the mobile usage data it collected to Facebook, which in turn used the real-time information it received from Onavo to determine which mobile applications posed a threat to Facebook's dominance and to the SDBE protecting Facebook from new entrants and competition. Facebook used Onavo data to: (a) identify and target competitors from which Facebook could demand Whitelist and Data Sharing Agreements; (b) identify and target competitors to whom Facebook would completely deny Platform access; and (c) identify and target competitors that Facebook would remove from the competitive landscape entirely through acquisition.

229. Facebook received Onavo information in real time, which included the two most important metrics for competing mobile applications—their reach and engagement. Reach measures the size of an application's user base, and "engagement" measures the extent to which users actively engage with the application. An application with high reach but low engagement cannot generate the sort of social data that Facebook needs to feed its advertising platform with actionable targeting data. Conversely, an application with high engagement but low reach doesn't generate social data from enough people to attract a broad base of advertisers. The greatest threat to Facebook's business would come from an application that exhibited strong reach and strong engagement—and especially one that showed rapid growth in both metrics, indicating the development of network effects.

230. As the potential threat to its market dominance from mobile applications continued to grow, Facebook sought to obtain exclusive control over Onavo's surveillance data—and over its mobile spyware code and installed base. On October 13, 2013, Facebook acquired Onavo.

231. On its blog, Onavo's CEO Guy Rosen and CTO Roi Tiger, announced that Onavo would continue as a standalone brand: "When the transaction closes, we plan to continue running the Onavo mobile utility apps as a standalone brand. As always, we remain committed to the privacy of people who use our application and that commitment will not change."

232. Facebook, however, had other plans. It immediately began integrating Onavo's applications into both its business operations and its acquisition strategy. Facebook, for example, began analyzing data secretly collected from Onavo's Protect software, which was a massive surveillance and data collection scheme disguised as VPN software. Billed as a way to "keep you and your data safe," Onavo Protect in fact monitored all web and mobile application traffic on a user's mobile device.

233. When an Onavo Protect user opened a mobile app or website, Onavo software secretly redirected the traffic to Facebook's servers, where the action was logged in a massive database. Facebook product teams then analyzed the aggregated Onavo data to determine which apps and features people were using in real time, how frequently they used the apps, and for how long. If the data in an app was not encrypted, this information was as specific as (for example) the number of photos the average user likes or posts in a week in that app.

234. Based on a 2017 estimate, Onavo's mobile apps were downloaded an estimated twenty-four million times, and Facebook collected, compiled, and leveraged all of the collected data. By February 2018, Onavo apps had been downloaded thirty-three million times across both iOS and Android.

235. As the former chief technologist for the Federal Trade Commission remarked to the press, Onavo was being leveraged against user interests to stifle competitive innovation:

> Instead of converting data for the purpose of advertising, they're converting it to competitive intelligence . . . . Essentially this

> approach takes data generated by consumers and uses it in ways that directly hurts their interests—for example, to impede competitive innovation.

236. Since 2011 and through the present, Onavo products have provided Facebook with real time data about mobile users on a breadth and scale not available through any other service or app. Using Onavo data, Facebook was able to determine which potential competitors it could target for its Whitelist and Data Sharing agreements; which competitors it could destroy by denying access to crucial APIs; and which competitors is needed to remove from the market through acquisition to preserve its monopoly position and SDBE.

237. Moreover, by monitoring potential threats, Facebook ensured that it had no blind spot—any application that posed a threat to its dominance was dealt with through anticompetitive and unlawful Whitelist and Data Sharing Agreements, destruction by denial of access to vital APIs on Facebook's platform, or by acquisition.

238. By acquiring Onavo, Facebook obtained exclusive access to the only real-time and high-quality source for mobile app user metrics at scale. Because of the acquisition of Onavo, Facebook strengthened the SDBE by ensuring that any threat to its dominance of the Social Data and Social Advertising Markets was dealt with at the earliest possible stage. Indeed, through Onavo, Facebook was able to (and did) track mobile app usage and trends essentially from launch. If a potential Facebook killer was on the rise, Facebook had a unique tool to identify it before anyone else could—and Facebook used it.

239. In the years after it acquired Onavo, Facebook continued to aggressively leverage the company's codebase in deceptively-labeled apps that facilitated maximum surveillance and data collection of mobile users. For example, Facebook placed Onavo spyware in apps whose stated purposes required privileged access to user's mobile devices (in some cases, super-user privileges), allowing Facebook to gather data on virtually every aspect of a user's mobile device usage.

240. The abuses by Facebook were so flagrant that on August 22, 2018, Apple banned Facebook's Onavo app from its App Store. Apple ejected Facebook's app from its marketplace

because it violated Apple's rules prohibiting apps from using data in ways far beyond what is required to run the app and provide advertising. In other words, because Onavo Protect was leveraging far more data than any VPN could conceivably need, it was clear that the true purpose of the app was to spy on Onavo users, and Apple would not allow it.

241. Indeed, the amount of surveillance was jaw-dropping. Facebook's Onavo Protect app reported on users' activities whether their screens were on or off; whether they used WiFi or cellular data; and even when the VPN was turned off. There was simply no rational relationship between the data collected and the purported purpose of the application. Put simply, a VPN that collected data even when the VPN was off was an obvious subterfuge for blatant spying on user behavior.

242. Undeterred, Facebook repackaged its Onavo spyware as a Facebook Research VPN app. Facebook sidestepped the App Store by rewarding teenagers and adults when they downloaded the Research app and gave it root—superuser—access to network traffic on their mobile devices. Facebook has been leveraging its Onavo code in similar ways since at least 2016, administering the program under the codename "Project Atlas"—a name suited to its goal of surveilling app usage on mobile devices in real time.

243. When the news broke in January 2019 that Facebook's Research apps were repackaged Onavo apps designed to spy on users, Facebook immediately withdrew the programs from the Apple App store.

244. Apple again concluded that Facebook had tried to violate its policies. Using Apple's Enterprise Developer Program, which allows the installation of a certificate or policy that provides root access to an iPhone or iPad, Facebook obtained a level of administrative privilege designed for a company's internal IT department. Thus, using a system that allowed organizations to manage their internal mobile devices, Facebook provided its spyware super user access to regular people's iPhones and iPads. Apple balked at the abuse. An Apple spokesman stated:

> We designed our Enterprise Developer Program solely for the internal distribution of apps within an organization. Facebook has

> been using their membership to distribute a data-collecting app to customers, which is a clear breach of their agreement with Apple. Any developer using their enterprise certificates to distribute apps to consumers will have their certificates revoked, which is what we did in this case to protect our users and their data.

245. U.S. Senator Mark Warner immediately called for new legislation to prevent the sort of abuse which Facebook had engaged in. U.S. Senator Richard Blumenthal issued a fierce statement rebuking Facebook's repackaging of the Onavo spyware app as "research": "Wiretapping teens is not research, and it should never be permissible."

246. In addition to Onavo's Protect app, Facebook has attempted to deploy its surveillance software as other forms of utility applications that require extensive or privileged access to mobile devices. For example, Facebook released the Onavo Bolt app, which locked apps behind a passcode or fingerprint while it covertly surveilled users—and sent Facebook the results. Facebook also shut that app down the very day that its surveillance functionality was discovered. The Onavo Bolt app had been installed approximately 10 million times.

247. Facebook continues to possess Onavo's code base and is likely, as it has done before, to repackage its surveillance software into yet another app. Facebook can also easily incorporate surveillance code into any of its mobile applications that enjoy massive installed bases and reach, including Instagram and WhatsApp. Without deterrence or divestiture, Facebook will continue leveraging the surveillance software, infrastructure, and analysis that it acquired as part of its acquisition of Onavo.

B. Facebook Identifies Instagram as a Threat and Acquires the Company.

248. Data from Onavo reported a significant threat on the horizon likely as early as 2011 (and certainly by 2012): a photo-sharing mobile application called Instagram. That app had its origins when founder Kevin Systrom, then 27, learned to code over nights and weekends. Systrom developed an app called Burbn, which allowed users to check in, post plans and share photos. The photo sharing feature immediately became the app's most popular.

249. After meeting venture capitalists from Baseline Ventures and Andreesen Horowitz, Systrom received $500,000 of funding. Systrom soon after met co-founder Mike Krieger—then 25 years old—who focused on the user experience of the app.

250. Seeing the positive reception to the photo sharing aspect of the Burbn app, Krieger and Systrom decided to pivot their business to focus on that feature. They studied their rivals in the category, including an app called Hipstamatic, which included photo-editing features, including the ability to add filters to photos. Hipstamatic, however, had no social capabilities.

251. Seeking to bridge the gap between Hipstamatic photo features and Facebook's elements, Systrom and Krieger stripped Burbn down to its photo, comment, and like capabilities. They then renamed the app Instagram, containing the words "instant" and "telegram."

252. Systrom and Krieger worked tirelessly to polish the user experience of their new application, designing Instagram to streamline the process of taking photos on mobile devices and uploading them to a social platform. The app had a minimalist focus, requiring as few actions as possible from the user. After eight weeks of fine-tuning, the app entered its beta phase and the founders prepared to launch it on iOS.

253. On October 6, 2010, Instagram launched on iOS. That very day it became the top free photo-sharing app on Apple's App Store, racking up twenty-five thousand downloads. Instagram's founders were stunned at the response. As Systrom noted after the launch: "First off, we have to say that we never expected the overwhelming response that we've seen. We went from literally a handful of users to the #1 free photography app in a matter of hours."

254. By the end of the first week, Instagram had been downloaded 100,000 times, and by mid-December 2010, its total downloads had reached one million. The timing of the app was impeccable, as the iPhone 4, with its improved camera, had launched just a few months earlier in June 2010.

255. With Instagram on the rise, investors clamored for a stake. In February 2011, Instagram raised $7 million in Series A funding from a variety of investors, including Benchmark

Capital, which valued the company at around $25 million. In March 2011, Jack Dorsey, the CEO of Twitter, pursued the idea of acquiring Instagram, and Twitter made an offer of approximately $500 million dollars for the company. Systrom declined.

256. By March 2012, the app's user base had swelled to 27 million. That April, Instagram was released on Android phones and was downloaded more than one million times in less than one day. At the time, the company was also in talks to receive another $500 million funding round.

257. Internally, Facebook carefully tracked Instagram's meteoric rise, including through the intelligence it received from Onavo's data collection. Instagram clearly posed a competitive threat to Facebook's dominant position, including in the rapidly expanding market for mobile-based social applications.

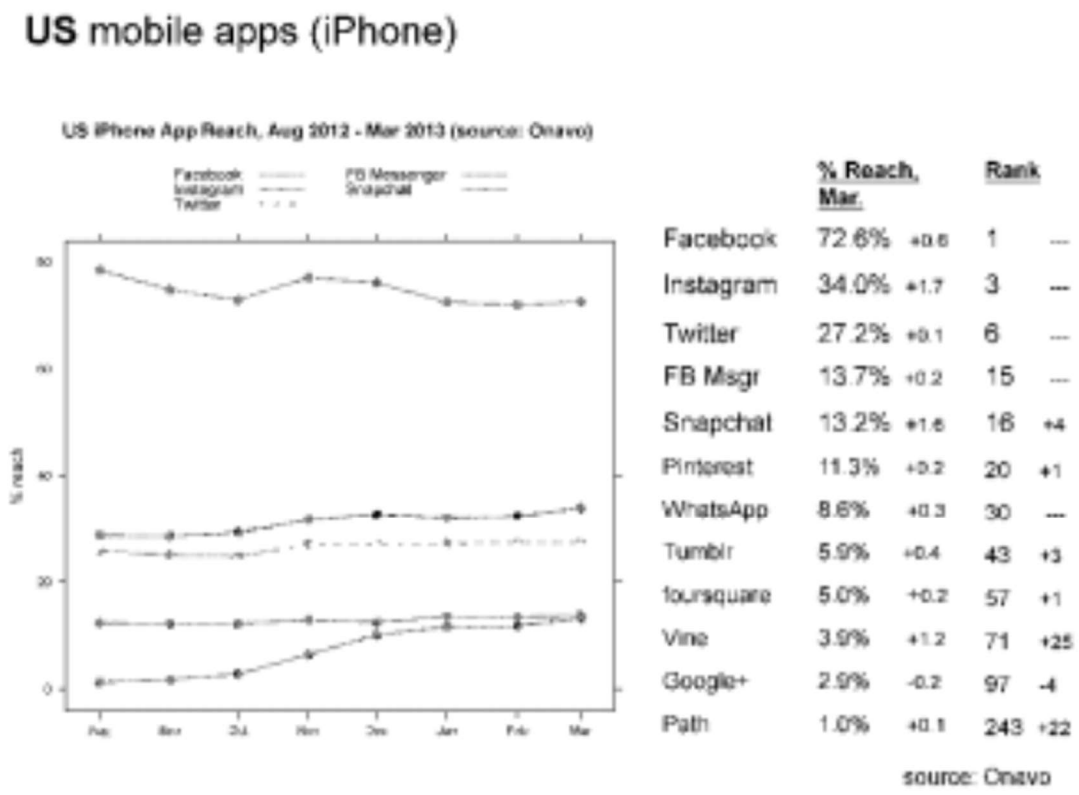
258. Unlike Instagram's streamlined approach to photo sharing, Facebook's photo-sharing was onerous. As Facebook internally recognized, mobile devices were changing how users uploaded and shared photos and it was causing severe problems for Facebook's business. As an internal Facebook presentation explained:

> Before phones, people would take their digital cameras out for special events, vacations, etc. Then, they would post a bunch of photos at once—after uploading them to their computer. With phones, people take and share more photos more often. They share them individually (rather than waiting to upload a bunch at once).

259. This resulted in a large drop in bulk photo uploads on Facebook's core social networking product—a 29% decline from 2012 to 2014. Facebook also observed that text posts were "tanking" 26% because of "migration to phones with cameras." The data was clear—Facebook had to shut down the looming threat from the new photo-sharing app. If Facebook did nothing, Instagram's user base would imminently eclipse Facebook's at its current growth rate, eroding and perhaps even destroying Facebook's SDBE. An independent app with no ties or reliance on Facebook, Instagram could become not only a competing mobile-based social app, but a social network unto itself that could rival Facebook in the amount of engagement and social data

it could produce and monetize.

260. After direct talks with Mark Zuckerberg, Facebook made Instagram an offer to purchase the company for $1 billion in April 2012, with the express promise that the company



would remain independently managed. Facebook consummated the deal immediately prior to its IPO.

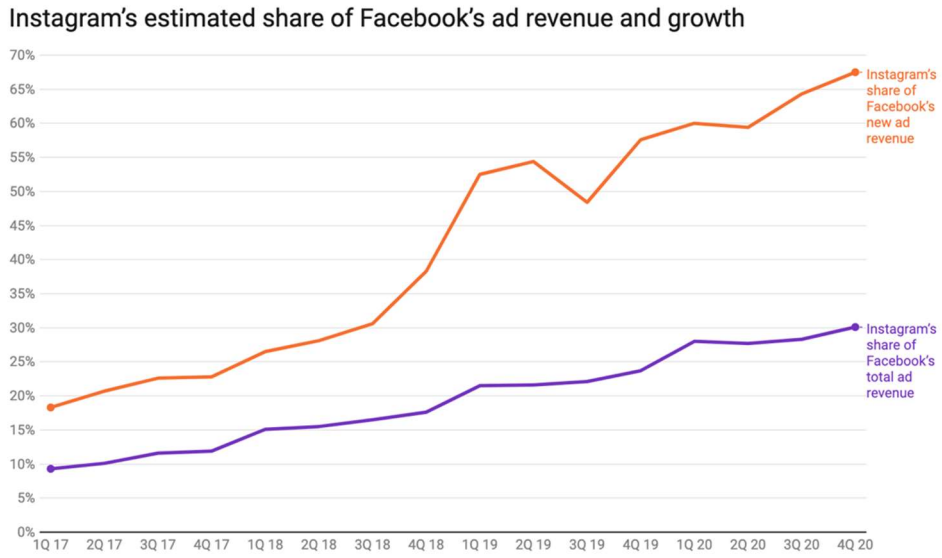
261. Facebook's own Onavo data, which was obtained and published by Buzzfeed, made clear that Instagram posed an existential threat to Facebook. By February 2013, Instagram had grown to 34% of the total user reach among all social apps.

262. With its Instagram acquisition, Facebook's share of mobile photo sharing app users ballooned as Facebook added Instagram's 34% user reach to Facebook's own 72% user reach.

263. Although Instagram had not at the time of the merger meaningfully monetized its user engagement and social data, Facebook quickly did so. By the end of 2013, Facebook had

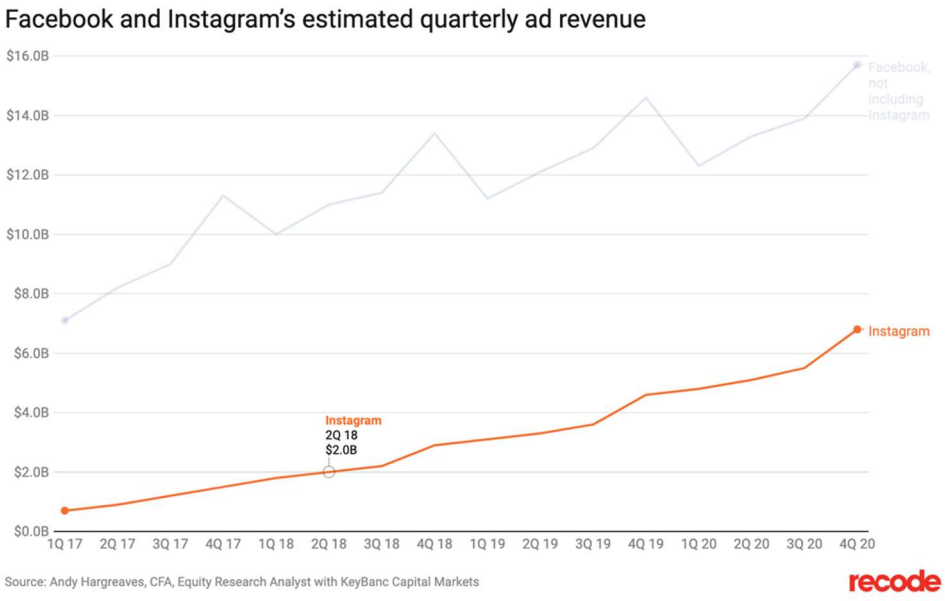
begun showing ads on Instagram. Since then, Instagram has become an ever-increasing proportion of Facebook's advertising revenue and a large share of Facebook's user growth.

264. In 2017, Instagram generated $2 billion, or about 15 percent, of Facebook's $13 billion in ad revenue.



265. By the end of 2018, Instagram had a billion users and was estimated to generate $8 billion to $9 billion in revenue for Facebook in 2018.

266. Instagram also accounts for the bulk of Facebook's new revenue since the acquisition.



267. Instagram allowed Facebook to grow its social network as Facebook's desktop and core mobile application began to stagnate. Together, Facebook and Instagram captured and monetized the social data generated across both apps.

268. The Instagram acquisition ensured that Instagram could not become a rival social network that could generate enough social data to erode the SDBE protecting Facebook's business. It also ensured that Instagram could not build and grow its own developer platform, which would threaten Facebook's scheme to dominate the Social Data and Social Advertising Markets by denying and/or leveraging social-data dependent applications' access to essential APIs. The acquisition accordingly also ensured that Facebook rivals required to enter into Whitelist and Data Sharing Agreements had no other platform choice—and thus no option but to hand over their social data to Facebook.

269. At the time of its IPO in 2012, Facebook struggled to grow its mobile product, let alone to meaningfully monetize the social data it collected through advertising. By 2019, Facebook had achieved an 83% share of the Social Advertising Market by leveraging its Instagram mobile application and its Facebook mobile and desktop applications. No other company comes close in market share.

270. Instagram was instrumental to Facebook's explosive growth in the Social Data and Social Advertising Markets. From the fourth quarter of 2010 until the first quarter of 2011, Facebook's revenue was flat. From 2011's holiday cycle to 2012's opening three months (right before its IPO), Facebook actually ***shrunk***. Facebook then experienced a sudden reversal after its acquisition of Instagram, as mobile revenue began to account for a significant share of revenues, and Instagram allowed Facebook to grow with the rise of mobile applications.

271. Notably, Facebook's acquisition of Instagram also allowed Facebook to exclude third-party apps that provided photo and video sharing functionality from its Platform. If an image sharing or video app contained an important feature, Facebook cloned it, thus paving the way for

excluding a competitive rival from its Platform, while simultaneously taking away that rival's share of users.

272. For example, when Snap, the maker of the app SnapChat, rejected Zuckerberg and Facebook's $3 billion offer to purchase the company and its product, Facebook flagrantly copied key features from Snap and built it into its Instagram product. Thus, when the SnapChat's "stories" feature—which allows a user to post a connected series of images and video—rapidly grew in popularity, Instagram simply cloned it. By late 2016, Instagram had launched a product that mooted one of Snapchat's most popular features.

273. Facebook's own clunky mobile app's clone of the "stories" feature did not have nearly the same traction with users. It was Instagram that provided Facebook the platform to compete head-on with a looming threat among social photo- and video-sharing apps. Without Instagram, Facebook would have faced direct competition. Instead, it leveraged Instagram to obtain and maintain its dominance among social mobile apps and the lucrative social data they generated.

274. Put simply, the acquisition of Instagram dramatically increased Facebook's market share of the Social Data and Social Advertising Markets and strengthened the SDBE protecting Facebook's business.

C. Facebook Acquires WhatsApp.

275. In February 2009, Jan Koum and Brian Acton left Yahoo! and founded a new company called WhatsApp. Koum had an idea for a mobile application that displayed user statuses in an address book on a smartphone—indicating, for example, whether a user was on a call, had low battery, or was at the gym. The pair enlisted the help of a Russian developer, Igor Solomennikov, to build the app. Koum spent days writing backend code for the app to allow it to sync with any phone number in the world.

276. Although the app—named WhatsApp—was initially unsuccessful, a June 2009 development changed everything. That month, Apple introduced "push notifications" for iPhone,

allowing developers to ping app users even when they weren't using the app. Koum immediately updated WhatsApp to ping a user's entire network of friends when their status changed.

277. The feature eventually became a form of instant messaging. Because messages sent through WhatsApp instantaneously notified other users even if the phone was not running the app in the foreground, it became ideal for broadcasting messages to connections within a user's social network, which was built on their phone's contact list.

278. At the time, WhatsApp's only significant competition for this sort of instant messaging was BlackBerry's BBM—which was exclusive to BlackBerry's proprietary hardware platform. WhatsApp, on the other hand, tapped into the vast network of app-enabled consumer smartphones that had emerged, particularly Apple's iPhone.

279. WhatsApp continued to innovate, including by introducing a double checkmark that showed when a message was read by another user. Wanting more from text messaging, including the limited MMS protocol used by cellular networks, WhatsApp set out to build a multimedia messenger system to send messages across a social network in real time to mobile devices.

280. Because WhatsApp's messaging used the mobile phone's internet connection rather than text messages, the app allowed users to avoid text messaging fees entirely. In some countries, text messages through cellular providers were metered. WhatsApp's ability to send messages to any user with a phone using the internet was its most sought-after feature.

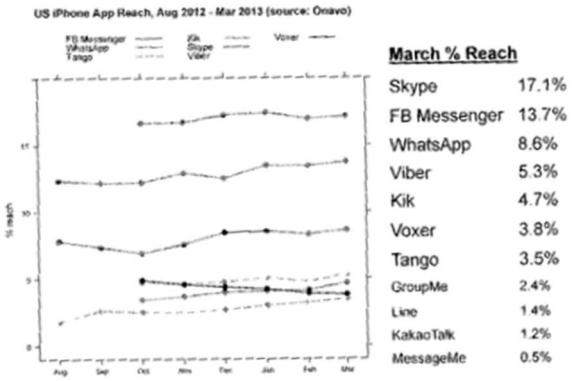
281. In December 2009, WhatsApp updated its app for the iPhone to send photos. User growth spiked, even when WhatsApp charged users for its service. Having created a unique combination of image and messaging apps as one socially powered app, WhatsApp decided to stay a paid service and grew while generating revenue.

282. By early 2011, WhatsApp was one of the top twenty paid apps in Apple's U.S. App Store. The company attracted the attention of venture capital firm Sequoia, and WhatsApp agreed to take $8 million of additional funding in addition to its original $250,000 seed funding.

283. Two years later, in February 2013, WhatsApp's user base had ballooned to 200 million active users. That moth, WhatsApp raised additional funds—another $50 million from Sequoia, at a valuation of $1.5 billion.

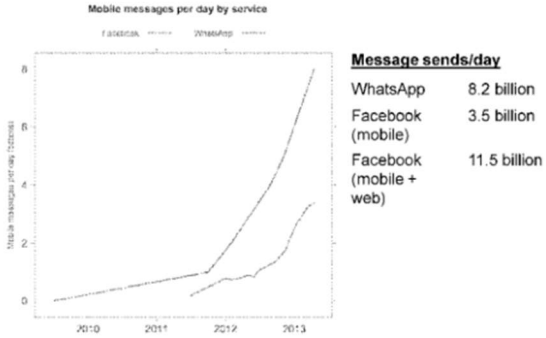
284. Internally, Facebook had carefully tracked WhatsApp's rapid rise. Engagement data from Facebook's Onavo spyware reported that WhatsApp was rivaling Facebook's own Messenger product, and held third place in terms of user reach among mobile messenger apps for iPhone in the U.S as of April 2013.

US mobile messenger apps (iPhone)



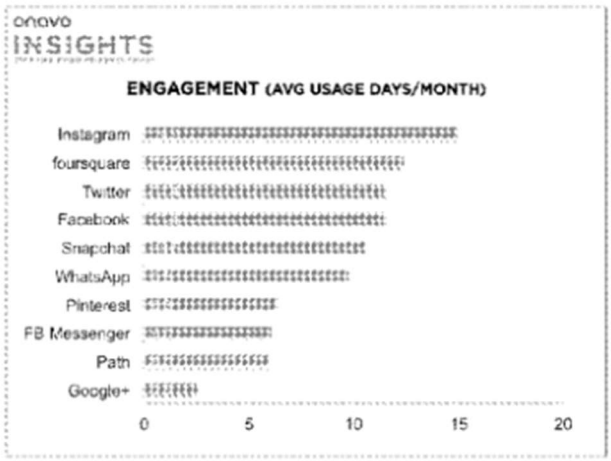
285. The broader picture was even more threatening to Facebook. As Buzzfeed recently reported, Onavo had tracked messages sent through WhatsApp and the number dwarfed Fakebook's own mobile product by more than twofold.

WhatsApp message sends



286. The same Onavo data reported by Buzzfeed showed massive engagement among WhatsApp users, placing it in fifth place behind Facebook's own core product; Facebook's newly-acquired Instagram; Twitter; Foursquare; and Snapchat.

US mobile apps (iPhone only)



source: Onavo

287. WhatsApp, although lacking Facebook's market reach, was drawing from the same pool of limited attention. Given Facebook's own fledgling Messenger App, WhatsApp exposed a massive vulnerability in Facebook's business model. WhatsApp was built on a social network derived directly from a smartphone user's contact list. It did not require Facebook's graph network for growth and could not therefore be shut down by revoking access to Facebook's APIs. Nor could Facebook demand that WhatsApp enter into a Whitelist and Data Sharing agreement.

288. WhatsApp posed a direct threat to Facebook's business, including the SDBE protecting its dominance. WhatsApp allowed for statuses, image sharing, and texting—all of the principal features of Facebook's core products. By 2013, the size of WhatsApp's network and the user engagement in that network made WhatsApp the most direct threat to Facebook's market dominance—and because of Onavo, Facebook knew it.

289. To ensure that it maintained its SDBE, and thereby its dominance of the Social Data and Social Advertising Markets, Facebook sought to remove WhatsApp as a competitor. As The Wall Street Journal reported, Facebook's Vernal internally commented in 2013: "Whats App launching a competing platform is definitely something I'm super-paranoid about." Vernal understood that if WhatsApp created a rival platform, Facebook's own scheme to exclude rivals by leveraging its Platform would fail—developers would migrate to the competing platform provided by WhatsApp.

290. Knowing about WhatsApp's size, its engagement, and its unique potential to erode the SDBE protecting Facebook market dominance, Facebook moved aggressively to remove this existential threat from the competitive landscape. In late 2013, Facebook made an initial bid of $16 billion in stock for WhatsApp. During negotiations in early 2014, Facebook raised its price to $19.6 billion—adding $3.6 billion to the original price as compensation to WhatsApp employees for staying on board at Facebook. When all was said and done, Facebook ultimately paid close to $22 billion for WhatsApp.

291. But for the value of containing and shutting down the growth of WhatsApp's competing social network and platform, the transaction made no possible economic sense to Facebook. WhatsApp's revenues were a meager $10.2 million in 2013. Its six-month revenue for the first half of 2014 totaled $15.9 million, and the company had incurred a staggering net loss of $232 million in that same period. Facebook had paid twenty billion dollars—thousands of times WhatsApp's revenues—to acquire a money-losing company that created software functionality Facebook itself already had as part of its own products, and could easily build from scratch for a fraction of the cost of the acquisition if it wanted to.

292. At the time of the WhatsApp acquisition, Facebook's user reach and user base and engagement was already massive—and unrivaled by any competing messaging app—but the addition of WhatsApp's user base further solidified Facebook's dominance in the Social Data and Social Advertising Markets. More importantly, however, Facebook had removed a serious threat

to its SDBE. If WhatsApp and its nascent social platform were allowed to compete on the merits, Facebook would not have been able to leverage its Platform into continued dominance of the Social Data and Social Advertising Markets, including by using API access to shut down competing third-party apps and to demanding access to other apps' most valuable social data as a condition for their existence.

293. Moreover, because the reach and engagement on WhatsApp generated (and generates) significant social data that Facebook could (and can) leverage and monetize through its mobile advertising channel, Facebook's SDBE strengthened as a result of the WhatsApp acquisition, fortifying Facebook's unrivaled dominance in the Social Data and Social Advertising Markets, and strengthening Facebook's ability to exclude potential entrants to these markets from gaining a foothold with a rival messaging or photo-sharing app.

VI. FACEBOOK'S INTEGRATION OF INSTAGRAM AND WHATSAPP WITH ITS FACEBOOK PRODUCT

294. Based on media reports, Facebook is as of the date of this Complaint scrambling to integrate the backends of its Facebook products with its acquired products, WhatsApp and Instagram. Until recently, Facebook has largely maintained the separateness of the products, but in response to threats of divestiture from antitrust regulators, Facebook has begun an aggressive effort to integrate the backends—the brains of each product—so that divestiture and other equitable relief will be impossible. The integration process is slated to be complete in the first few months of 2020. Unless restrained, Facebook may impair the ability of Plaintiffs to obtain necessary relief in this action.

* * *

295. When it acquired WhatsApp, Facebook publicly stated that it would operate WhatsApp independently from its other Facebook properties, but that turned out not to be the case. Indeed, the European Union found Facebook lied to regulators about its integration plans for

WhatsApp and fined Facebook €110 million. The EC regulator explained the reasons for its fine in a press release, dated May 17, 2017:

> The European Commission has fined Facebook €110 million for providing incorrect or misleading information during the Commission's 2014 investigation under the EU Merger Regulation of Facebook's acquisition of WhatsApp. . . .
>
> When Facebook noticed the acquisition of WhatsApp in 2014, it informed the Commission that it would be unable to establish reliable automated matching between Facebook's users' accounts and WhatsApp users' accounts. It stated this both in the notification form and in a reply to a request for information from the Commission. However, in August 2016, WhatsApp announced updates to its terms of service and privacy policy, including the possibility of linking WhatsApp users' phone numbers with Facebook users' identities.
>
> On 20 December 2016, the Commission addressed a Statement of Objections to Facebook detailing its concerns.
>
> The commission has found that, contrary to Facebook's statements in the 2014 merger review process, the technical possibility of automatically matching Facebook and WhatsApp users' identities already existed in 2014, and that Facebook staff were aware of such a possibility.

296. Facebook had lied to regulators. It was always capable of integrating its advertising targeting systems and in fact had done so. After the acquisition, WhatsApp's founder Brian Acton quit in protest in March 2018, stating on Twitter: "It is time. #deletefacebook."

297. Consistent with the EC's finding, Acton believed Facebook misled European Union regulators about its plans to commingle WhatsApp and Facebook data for use in its ad targeting system. And despite Zuckerberg's promise that he would not try to monetize WhatsApp for five years, Facebook almost immediately began exploring the monetization of WhatsApp without its founders' consent. Acton left behind $850 million in stock when he quit in protest.

298. WhatsApp's other co-founder, Jan Koum, left in April of 2018. Instagram's founders Kevin Systrom and Mike Krieger followed suit shortly after, resigning from Facebook in the Fall of 2018.

299. With the founders of its two acquired competitors—Instagram and WhatsApp—gone, by late 2018 Facebook had unfettered internal license to integrate two of the most powerful rival social networks with Facebook's core business.

300. Facebook, however, knew it was vulnerable to divesture of the acquired assets if it continued to operate them independently. In the face of backlash for its abusive privacy practices, Facebook became alarmed at calls to break up the company.

301. Zuckerberg and Facebook immediately devised a plan to integrate the backends of the WhatsApp, Instagram and Facebook products. On March 6, 2019, Zuckerberg announced a plan to integrate the apps on his blog, cloaking the maneuver as a privacy-related decision to frustrate regulators. Facebook's announced plan would implement a unitary form of end-to-end encryption across its messaging and photo sharing apps, and would integrate the acquired assets (WhatsApp, Instagram, and their respective social data) to make them interoperable with—and inextricable from—Facebook's core product.

302. Although Facebook has already begun the process of integrating its advertising tracking and surveillance infrastructure across applications, the full integration of the so-called backend would give Facebook surveillance, advertising targeting, and market power incomparable from any other social network (and likely any other private entity) on Earth. Once fully integrated, those Instagram and WhatsApp networks can also never become viable platform alternatives to Facebook's Platform. Indeed, once integrated, Instagram and WhatsApp would be not alternatives, but part and parcel of the very Facebook's Graph API and Platform the company has anticompetitively leveraged for dominance in the Social Data and Social Advertising markets to the detriment of thousands of third-party developers, including Plaintiffs and Class Members herein.

303. The back-end integration of Instagram and WhatsApp would also affect the ability of regulators to regulate how user data is shared and stored across the platform. By integrating the data, Facebook would be free to mine it, sell it, and monetize it through advertising, regardless of its source. As the former Chief Technologist for the FCC, Ashkan Soltani, commented: "While positioned as a privacy-friendly play, its timing suggests a competition play to head off any potential regulatory efforts to limit data sharing across services."

304. The back-end integration would be a game changer, bringing together the three largest messaging networks. Once the backend is integrated, the 2.6 billion users across Facebook, WhatsApp and Instagram will be able to communicate across platforms for the first time, creating a massive and unprecedented concentration of market power. Facebook plans to complete its integration efforts imminently, reportedly in early 2020.

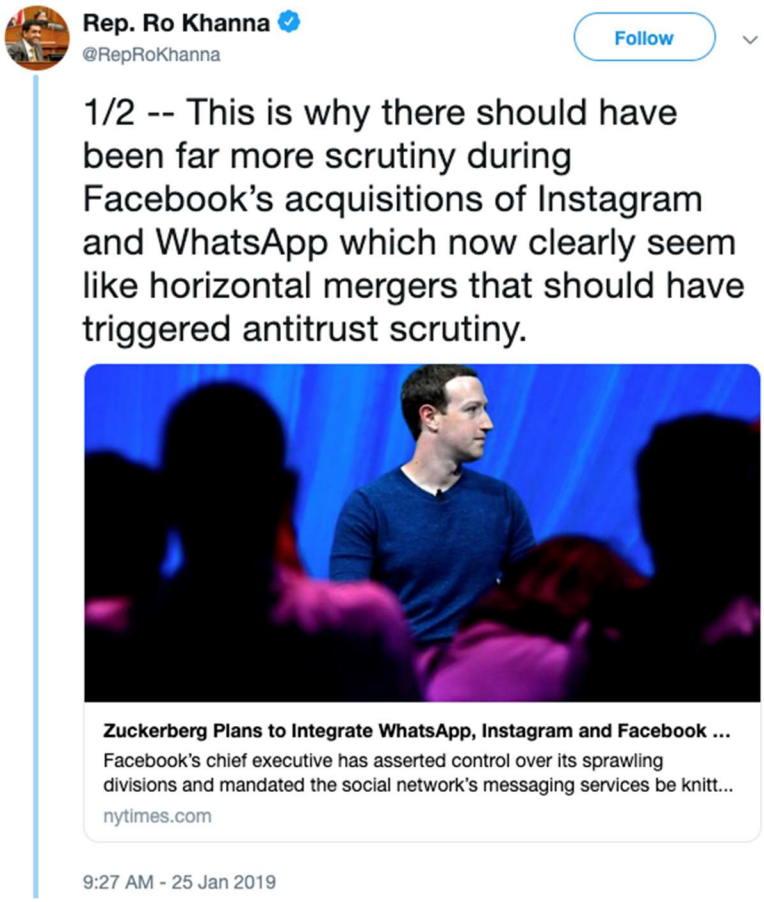
305. The integration effort requires the efforts of thousands of Facebook employees to reconfigure how WhatsApp, Instagram and Facebook Messenger function at their most basic levels, according to a person involved in the effort who spoke anonymously to the press.

306. Internally, some of Facebook's staff working on the integration balked, demanding answers to questions about the purpose of the initiative. When pressed in on December 7, 2019 for answers, Zuckerberg gave vague and meandering answers to questions about the reasons for the integration. As a result, several WhatsApp employees have left or plan to leave because of Zuckerberg's plans.

307. The merger of the platforms would increase the cost of switching to a rival social network—to the extent any viable rival exists outside of the platforms Facebook imminently seeks to integrate (Instagram and WhatsApp). A user making a switch to a non-Facebook rival would have to abandon the largest social network in in the world, which exists as a result of the combination of the three Facebook-owned products. The SDBE protecting this amalgamation of Facebook, Instagram, and WhatsApp would be terrifyingly high, as the social data of billions of users across years of heavy engagement is integrated into a conjoined hurdle blocking new entrants

or would-be entrants to the United States and worldwide Social Data and Social Advertising Markets.

308. The integration of the three products also poses changes to the level of anonymity enjoyed by WhatsApp's users. WhatsApp currently requires only a phone number when new users



sign up. In contrast, Facebook and Facebook Messenger ask users to provide their true identities and will ban users who fail to do so. Integration would mean matching WhatsApp handles to Facebook and Instagram user accounts, allowing for unprecedented level of surveillance and advertising targeting.

309. Lawmakers saw the move to integrate the WhatsApp, Instagram, and Facebook back-ends as flagrantly anticompetitive. United States Congressman Ro Khanna, for example, took to Twitter to lament the fact that Facebook's horizontal mergers with WhatsApp and Instagram were not blocked when they occurred:

310. If those mergers had been blocked, it was clear, as Khanna observed, that Facebook would have had to compete directly with Instagram and WhatsApp:

311. The integration would also connect Facebook-owned products that are dominant in particular geographic region, greatly increasing Facebook's worldwide dominance in Social Data and Social Advertising. Users in Southeast Asia, for example, where WhatsApp is dominant, would be able to directly communicate with users in regions dominated by Facebook's Messenger or Instagram. This would massively increase Facebook's engagement in global messaging and photo sharing, further growing the company's SDBE.

312. Indeed, as reported recently by one source in February 2019, 82% of Indian Internet users use WhatsApp; in Mexico, 91%; in Brazil, 66%; and in the UK, 84% of 25-34 year-olds and 80% of 18-24 year-olds. After integration, these WhatsApp users would all be able to communicate directly with U.S. users of Facebook's other products, meaning Facebook would achieve a significant increase in market share globally in the Social Data and Social Advertising markets.

313. Regulators are aware of this risk. For example, as of the date of this Complaint, the FTC is reportedly considering seeking an injunction to halt Facebook's integration efforts. Antitrust officials, including those at the FTC, are concerned that integration would prevent divestiture should regulators take action against Facebook. Without some means of halting Facebook's integration gambit, the ability to obtain an injunction preventing Facebook from continuing its anticompetitive conduct and to remediate Facebook's anticompetitive acquisitions may be impaired or eliminated.

314. In other words, Facebook's acquisitions are being presently used to reinforce the SDBE, prevent regulatory enforcement, prevent entry by new competitors, expand Facebook's reach, and to maintain its dominance and market power. The integration, if completed, will not only substantially lessen competition, it may allow Facebook to destroy it—for a very long time.

VII. THE RELEVANT MARKETS

315. There are two relevant, or alternatively relevant, markets in this case—the market for social data (the "Social Data Market") and the market for social advertising (the "Social Advertising Market"). Both markets are protected by the Social Data Barrier to Entry described above and in this section.

A. The Social Data Market

316. Facebook and other Social Data market participants acquire social data from their users in exchange for the value they provide to those users. Specifically, social networks provide users with, among other things, the ability to send each other messages, signals, such as "likes" or "pokes," photos and video, view information about others in their network, and the ability to explore other connections among their friends. In exchange, Facebook and other social networks collect data about the interaction among users, including what they share, what they send each other, what they view or find interesting, and even their web and mobile traffic outside of the social network.

317. All of this data is then used to sell targeted advertising on an advertising platform. The advertising Facebook and other social networks provide is unique. It allows fine-tuned targeting of individuals by granular attributes. To achieve the level of granularity that can provide advertisers direct access to targeted demographics, advertising based on social data requires extensive data from a social network's users—data that a social network can only obtain when its users engage on its platform with each other or with content posted to the network.

318. Put simply, Facebook—and other market participants in the Social Data market—sell user data. They obtain that data from user engagement and sell that data to advertisers or third-

party developers. That is, profits in the market can be obtained by selling the data acquired for the least amount of value the market will bear, and then selling that data through an advertising sales channel at a higher price.

319. Because social data is obtained by providing users with mostly free services, participants in the Social Data Market compete for user data based on features, the value and breadth of their network, and other non-price bases. Thus, in a competitive market, social networks compete on the merits to obtain social data by innovating with new products, providing heightened privacy to their users, or increasing the value of their overall social networks.

320. Because social interactions are used to target users for advertisement, the sort of data valuable to participants in the Social Data Market is data resulting from user-to-user or user-to-content interactions that reveal the preferences, affiliations, proclivities, political leanings, or other attributes of the user. Social networks that encourage users to engage with their platform can obtain such user data in a number of ways, including photo and video sharing, messaging, gaming, or other forms of content relying on interactions among users. While a user's interaction with a news article, for example, may be valuable for advertising targeting, that user's decision to share that news article with his friends is the sort of social data for which participants in the Social Data Market compete.

321. Not all data is social data. A person's credit card statement may reveal a user's preferences and spending habits, but because that data is not shared among a network of users, it is not the sort of social data that is acquired and sold in the Social Data Market. In contrast, a user's decision to like a product or share a review of a product with his friends is social data. In other words, social data arises from engagement within a social network among its users.

322. Message boards and video sharing sites may not be market participants because user interactions are not through a network, but instead may be broadcasted for general consumption of anyone who accesses the site. The data obtained is derived from unilateral user conduct, not the propagation of a user's actions through a network.

323. The ability to obtain social data from users thus depends on the ability to keep users engaged on a platform. A social network, such as the failed Google+ social network, for example, obtained a large user base, but as described above, ultimately failed because users did not engage on the platform.

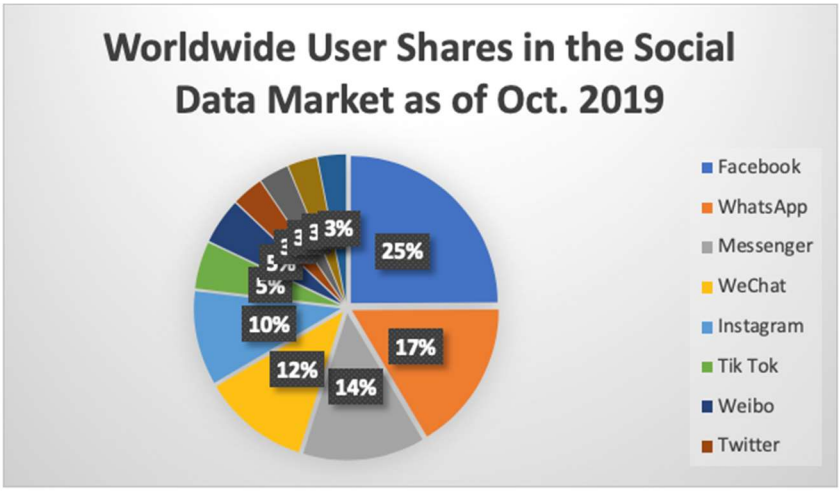
324. Because engagement is the source of the social data for which Social Data Market participants compete and which they ultimately sell through a sales channel such as advertising or API access, a Social Data Market participant's share of the market is best measured by the share of active users on the social network's platform.

325. Indeed, not all participants in the Social Data Market monetize their social data, either because they have nascent businesses or because they have not yet developed a business model, but the data their network generates is valuable in the hands of a competitor capable of monetizing that data. For such firms that compete for social data but do not—or have not yet—monetized that data through a sales channel, their share of the market can only be measured by examining the level of engagement on their platform.

326. Social networks can form in many contexts. As Facebook itself has recognized, messaging, photo sharing, gaming, dating, and other apps may produce social data that Facebook competes for and monetizes. Facebook thus horizontally competes with companies that produce social data in the Social Data Market, regardless of the what specific value is provided to the members of the social network, be it, for example, messaging or photo sharing.

327. Unlike a typical website, video streaming site (*e.g.*, YouTube), or message board (*e.g.*, reddit), wherein users post comments on content for strangers and the general public to see, a social network's value is solely in the data derived from its network—namely, from the strength and value of the specific connections among users. Thus, user-networks built on friendships and familial relationships are stronger than networks of strangers with common interests. A competing entrant that can build a network of highly interrelated users can therefore create enough value to extract valuable and monetizable social data.

328. Since at least as early as 2010, Facebook has occupied a dominant position in the Social Data Market, with a user share worldwide during the relevant period of more than 60% of users on comparable social networks when user shares of its WhatsApp, Instagram, Facebook, and Messenger products are aggregated.



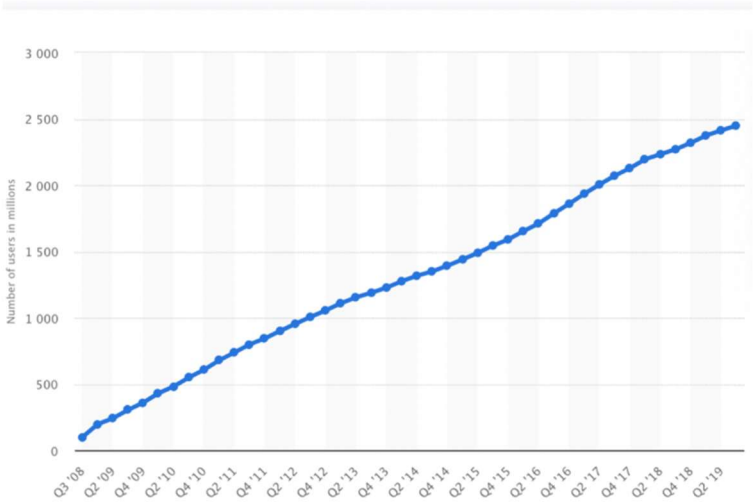
329. As of October 2019, Facebook's share of users worldwide, when aggregating all of its properties, including Instagram, WhatsApp, Facebook Messenger, and Facebook's core product is approximately 66%.

330. The market is highly concentrated both in the United States and globally. Using the Herfindahl-Hirschman Index ("HHI"), a metric that measures market concentration by squaring market participants' shares of the market, it is clear that the Social Data market is highly concentrated—with an HHI of approximately 4586. The Department of Justice's merger guidelines deem markets with HHIs in excess of 2500 as "highly concentrated." *See* U.S. DEPARTMENT OF JUSTICE & FTC, HORIZONTAL MERGER GUIDELINES § 5.3 (2010).

331. Of course, if Facebook never acquired those properties, the WhatsApp and Instagram shares may have been significantly higher and there may have also been more entrants in the market, thus reducing concentration. Nonetheless, the contrast between HHIs before and after aggregating Facebook's properties is striking and makes clear that Facebook has a dominant share of the global user share in the Social Data Market.

332. When social networks such as WeChat—which serves Asian countries with stringent regulatory schemes and high barriers for entry for non-state affiliated companies or foreign companies—are excluded from the market, the market is even more concentrated. In the United States, Facebook's share of users is unquestionably dominant. Between Facebook and Instagram, both of which are highly popular in the United States, Facebook is virtually unrivaled and unparalleled in its share of social data generated in the Social Data Market.

333. Even setting aside WhatsApp and Instagram, Facebook's core product's users have grown in number almost monotonically every year since 2008.



334. Facebook, WhatsApp, and Instagram have managed to capture not just large user bases, but large numbers of ***active*** users.

335. WhatsApp's Monthly Active Users have increased every year since April 2013, from 200 million MAUs to approximately 1.5 billion MAUs since 2017.

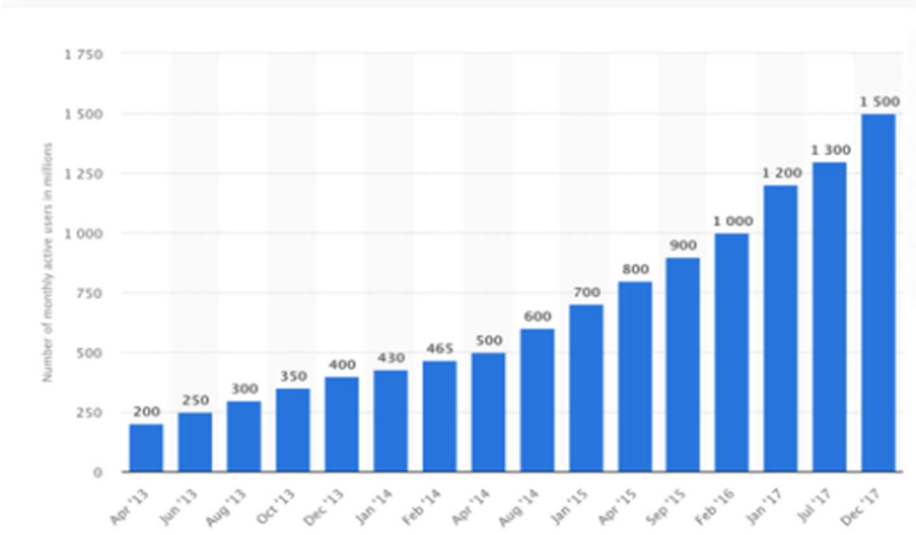


Figure 1: WhatsApp Monthly Active Users (in millions)

336. Instagram has grown from approximately 90 million monthly active users in January 2013 to approximately 1 billion users since June of 2018.

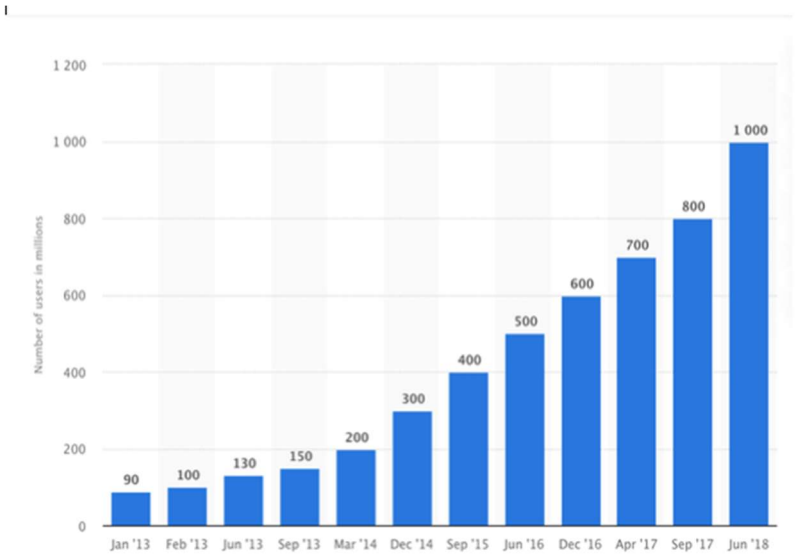


Figure 2: Instagram Monthly Active Users (in millions)

337. Facebook's Messenger product has also grown rapidly in terms of MAUs, with 200 million in April 2014, and more than approximately 1.3 billion since September 2017. Facebook itself has 2.7 billion MAUs in all.

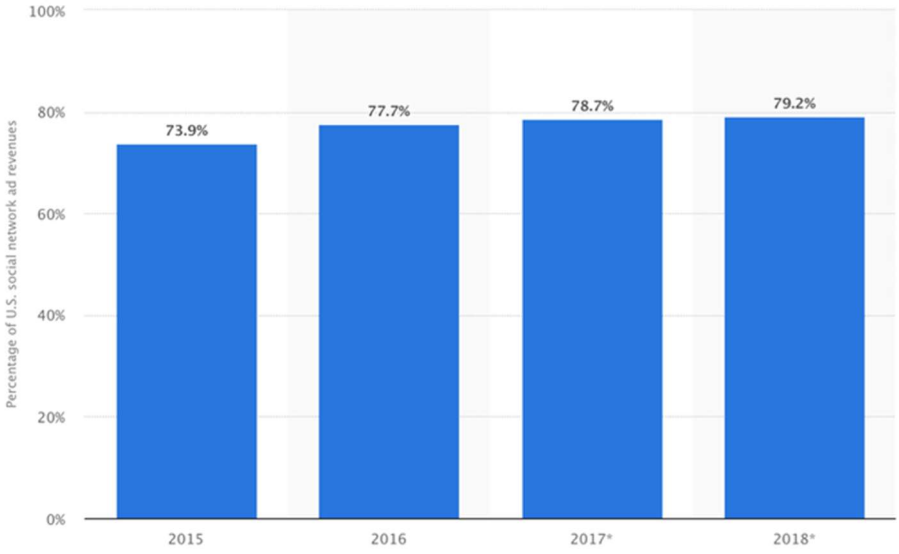
338. That each product's user base is engaged on a monthly basis is a clear sign that each one generates staggering amounts of Social Data that is in proportion to its number of total users. Indeed, for Instagram, Facebook, and WhatsApp, the global number of MAUs is in line with each product's overall user share.

339. Facebook's competitors cannot match even one of Facebook's products. Twitter's MAUs have never exceeded 70 million since 2010 and maintains approximately 68 million as of Q1 2019. WeChat, which has the second largest share to the Facebook's aggregated products with a share of 12% of worldwide users, has approximately 1.151 billion active users as of Q2 2019.

340. Facebook has maintained its dominance ever since 2010 when it emerged as the winner among social network websites such as MySpace and Friendster. It expanded its share further and maintained its dominance after its acquisitions of Instagram and WhatsApp.

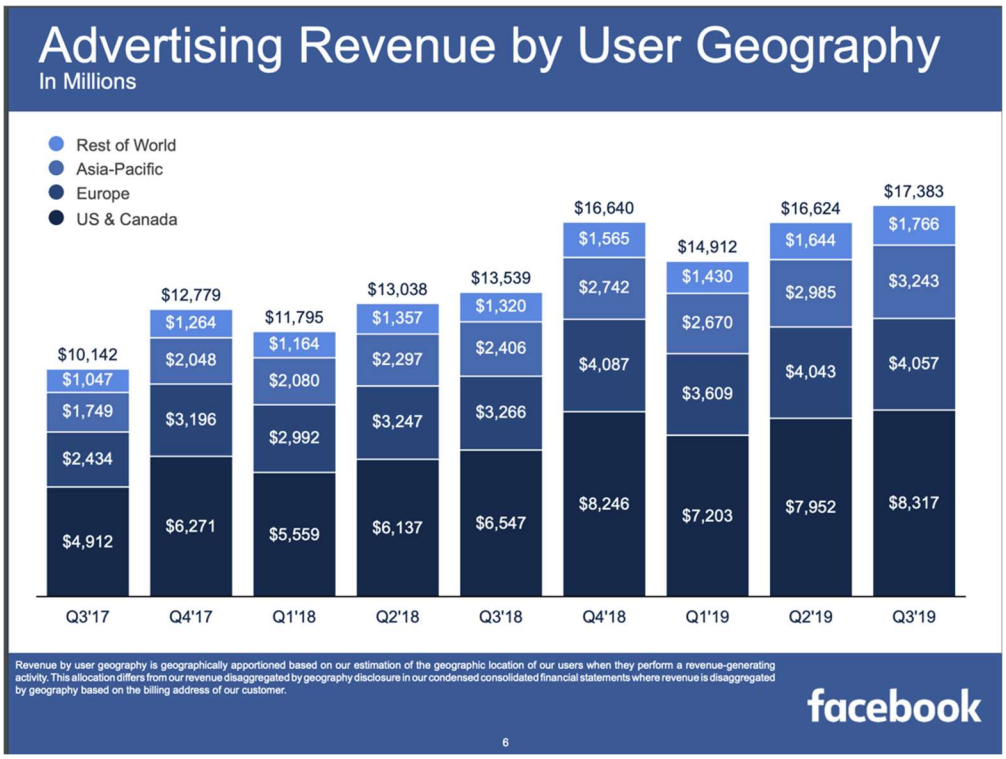
B. The Social Advertising Market

341. In the alternative, Facebook's dominance can be viewed through its sales in its advertising channel. Advertising sold on social networks is not fungible or interchangeable with advertising on other digital platforms. Because of the extensive ability to target advertisements to users on social media sites like Facebook, search and banner advertising are not reasonable substitutes.



342. Facebook's revenue share of the social advertising market is approximately 80%. Its share has been above 70% since 2015.

343. Facebook's advertising revenue has steadily grown both in the United States and globally. Facebook reported advertising revenues totaling $17.383 billion as of Q3 2019. Approximately $8.3 billion of that advertising revenue came from the United States.



344. From 2014, through 2016, Facebook's advertising revenues grew from $2.9 billion to $6.436 billion. During that period, and even before then, Facebook was one of the few social networks that significantly monetized its network by selling advertising. Other competitors did not come close, and Facebook established unrivaled dominance in the Social Advertising Market and maintains that dominance to this day.

345. Twitter, one of Facebook's only competitors to sell significant social advertising during the same period Facebook generated revenue in the Social Advertising Market, has never exceeded $800 million in advertising revenues. Revenues in Q1 2012 were approximately $45 million, growing to $432 million in Q4 2014, and standing at $702 million as of Q3 2019.

346. LinkedIn, another competitor that sells social advertising, generates roughly $2 billion in overall annual revenue by the end of 2018, with some lesser proportion of that coming from advertising.

347. Considering the revenue generated by LinkedIn and Twitter, Facebook's advertising revenue accounts for approximately 86% of the total revenue share across the three largest firms competing in the Social Advertising market. Excluding the contributions from minor competitors that monetize their social networks, the HHI of the Social Advertising Market is approximately 7,685, well beyond what the DOJ considers a highly concentrated market.

C. Barriers to Entry

348. Both markets are protected by the Social Data Barrier to Entry that prevents Facebook's competitors from entering the market. Without a critical mass of social data, market participants in both the Social Data and Social Advertising Markets cannot generate revenue.

349. Moreover, without adequate social data and engagement with the social network, market participants cannot display content to users that would provide enough value to generate engagement and additional social data.

350. Likewise, without a critical mass of social data, advertising targeting will not be possible or will be substantially diminished in effectiveness, thus reducing revenues in the

advertising sales channel of the Social Data Market and social advertising revenue in the Social Advertising Market.

351. A firm's market power in both markets therefore depends on obtaining a critical mass of social data. Because of network effects, users will not use a social network that lacks enough social data to provide targeted content or to provide valuable connections to other users. However, once a certain amount of social data is obtained by a market participant, a feedback loop may form as a result of network effects, further increasing the amount of social data generated by the social network.

352. A new entrant must therefore expend significant amounts of investments in capital, technology and labor to create a network large enough to create the network effects necessary to compete with dominant firms in the market.

353. Because of the large amount of capital and social data required to successfully enter the Social Data and Social Advertising markets, the SDBE effectively excludes entry by a new competitor, even a well-funded one. Indeed, the SDBE prevented Google from successfully entering both the Social Data and Social Advertising markets with its Google+ social networking product.

354. Although Google+ had successfully replicated Facebook's core functionality and even added additional functionality to its software, its entry failed because it lacked the critical mass of Social Data that is required to reverse the network effects protecting Facebook. Without that critical mass, users will not incur the costs of switching from Facebook's social network to a new entrant's social network. That is, a new entrant will not be able to provide a valuable network of engaged users upon entry to justify a Facebook user to change social networks.

355. That is precisely what happened to Google. Although it had a massive user base, it lacked engagement, which meant it did not provide a sufficient amount of social data that could be used to target content and advertising to users. This, in turn, reduced the value of the entrant

social network and accordingly the attraction of switching from Facebook's social network to Google's.

356. The SDBE continues to reinforce Facebook's dominant position. In fact, by excluding rivals and potentially competing social networks through the anticompetitive scheme described in this Complaint, Facebook strengthened the SDBE, providing it a larger share of social data and a stronger monetization channel through social advertising. The additional amount of social data increases the value of its network, and the revenue from social advertising increases the cost of entry for a new rival.

357. Other barriers to entry in both the Social Data and Social Advertising Markets include, but are not limited to, the high cost of development, data management, talent acquisition and retention, server infrastructure, development infrastructure, software technology, software libraries, and a brand and marketing presence sufficient enough to attract an engaged user base.

358. In certain countries in the global markets for Social Data and Advertising Markets (described below), regulatory barriers to entry may exist in the form of government surveillance and other monitoring, government content restrictions and prior restraints on speech, and onerous or complex regulatory schemes. A new entrant would be required, for example, to ensure compliance with EU data privacy laws, which may require it to incur high entry costs, particularly for entry at scale.

D. Relevant Geographic Markets

359. There are two relevant geographic markets for the Social Data and Social Advertising product markets: the U.S. and Global Social Data and Social Advertising markets. Both markets can be viewed in the alternative as U.S. markets or as markets extending across several countries.

360. For the Social Data Market, social data must be compatible with the customers purchasing that data. Thus, social data about a foreign market may be of little use for a U.S. based advertiser. The data may be collected in a different language, may involve interests more pertinent

to a particular geographic region (*e.g.*, American Football vs. Rugby), and may contain a demographic of users that share a common culture or merely a close proximity.

361. The same is true for the Social Advertising Market. An advertiser seeking to sell products designed for consumption in the United States may not have any use for a platform's advertising targeting capabilities outside of the United States. In the U.S., Facebook enjoys higher market shares of the Social Advertising Market than the global shares described above. Thus, Facebook enjoys an even more dominant share of the U.S. Social Advertising Market than it does globally.

362. In the U.S., Facebook's market share of the Social Data Market is even greater than its global market share. Services such as WeChat are geared towards Asian markets, particularly China, and do not generally compete in the U.S. market with Facebook's Messenger, Instagram, and core social networking product. Thus, Facebook's U.S.-based market share is even higher than its global market share referenced above, which is already a dominant share of the market.

363. In the global markets, Facebook's product does not face competition in every country, and not every country is part of the market. Certain countries, such as Russia, China, Iran, and North Korea have extensive Internet monitoring and restriction programs run by governmental or quasi-governmental entities. Because of regulation in these countries, no social network is free to enter those markets and compete on the merits. Those countries, and others like them, are therefore not part of the Social Data Market or Social Advertising Market. Indeed, it may be unlawful for Facebook to monetize social data or social advertising in those countries.

VIII. HARM TO COMPETITION AND ANTITRUST INJURY

364. Facebook's anticompetitive scheme had the purpose and effect of monopolizing the Social Data and/or Social Advertising markets in the United States and/or globally. Facebook's conduct allowed it to maintain the monopoly and market power it had obtained by 2010 in the Social Data and Social Advertising Markets, and/or Facebook intended and attempted to acquire such a monopoly through its anticompetitive scheme. Facebook also entered into unlawful and

unduly restrictive agreements to restrain trade in the Social Data and/or Social Advertising Markets (the "Relevant Markets").

365. Specifically, Facebook engaged in a series of conduct in furtherance of its scheme, including, but not limited to: (a) the removal of important and necessary APIs from its Facebook Platform for the intended purpose of destroying competition in the Relevant Markets; (b) the targeting of competitors for coercive Whitelist and Data Sharing Agreements on pain of denial of access to Facebook's Platform and APIs; (c) the use of secret surveillance software to identify and destroy potential competitive threats; (d) the acquisition of rivals with the purpose and effect of strengthening the SDBE and increasing Facebook's market share and market power in the Relevant Markets; (e) integrating its separate products to prevent antitrust enforcement, obtain a dominant share of the global Relevant Markets, and to frustrate any prospect of divestiture; and (f) misleading developers about the stability of Facebook's Platform to induce them to become dependent on Facebook's social data.

366. Facebook engaged in this conduct while possessing market power in both the Social Data and Social Advertising Markets, both in the United States and globally. Facebook enhanced and/or maintained its market power and monopoly through this scheme and then used it to exclude rivals and potential entrants. Facebook's anticompetitive scheme also reduced consumer choice by stifling innovation among nascent and established competitors that relied on Facebook's Platform for their products and business and by entering into agreements that strengthened the SDBE.

367. In the alternative, Facebook's scheme had the purpose and effect of achieving a dangerous probability of a monopoly in the U.S. and/or Global Social Data and Social Advertising markets.

368. Facebook's decision to remove the Friend and Newsfeed APIs excluded horizontal and/or direct competitors from the Social Data market. Once a potential threat to Facebook or Facebook's SDBE is eliminated, it cannot (a) monetize social data by selling advertising; (b)

accumulate social data sufficient to create a competing platform; and/or (c) even purchase social data from Facebook at full price.

369. That same decision also excluded competition in the Social Advertising Market because the competing third-party applications could not become rival sources of advertising, nor could they become rival social advertising platforms using the social data their applications generated. Moreover, because Facebook eliminated the applications relying on the APIs—including the Friend and News Feed APIs—from the market, the developers of those applications could no longer purchase advertising from Facebook in the Social Advertising Market, even at full price.

370. Facebook sacrificed profits in the Social Data and Social Advertising Markets for the sole purpose of executing its scheme an excluding competition. It would make no rational sense to exclude a competitor that would also be a purchaser of social data or social advertising if they were permitted to exist. It would also make no sense to exclude a third-party app that Facebook could have charged for API or social data access. Put simply, Facebook put anticompetitive conduct ahead of profits.

371. Facebook knew that once its competitors were foreclosed from the Social Data and/or Social Advertising markets by its anticompetitive scheme, Facebook would be free to charge monopoly prices for social data and social advertising without facing any competitive price or quality pressure. In fact, Facebook has reduced the value it provides to users through privacy and feature innovation throughout and after it executed its anticompetitive scheme without sacrificing any significant marginal demand—a clear sign of its market power in the Social Data and Social Advertising Markets. Likewise, Facebook has increased the price of its targeted advertising throughout the period of its anticompetitive scheme and to the present, also a sign of its market power in the Social Data and Social Advertising Markets.

372. Facebook's Whitelist and Data Sharing agreements ensured that Facebook would control competitive threats to its platform and extract their most valuable asset—their social data.

Facebook, by requiring Whitelist and Data Sharing agreements by competitors, ensured that these competitors, some of which were competing social networks, could not become alternative platforms for developers. That meant that when Facebook excluded other developers from the market, they were completely foreclosed and would have no reasonable alternative.

373. After excluding applications that competed with it from the Social Data and/or Social Advertising Markets, Facebook was left with competition from entirely independent apps, which did not rely on Facebook's social data, APIs, or advertising. Rather than compete on the merits with these competitors, Facebook secretly spied on users using the Onavo data and the Onavo assets that it acquired to target potentially competitive threats and then acquired the companies that built the threatening products, even at economically irrational prices.

374. Facebook accordingly used the Onavo data and Onavo-based spyware it owned or had in its possession to track Instagram use. When Instagram's engagement and user reach indicated that it was a potential competitive threat to Facebook, Facebook acquired Instagram and operated it alongside its products, and presently seeks to complete integration of the product with all of its other Facebook properties.

375. Likewise, Facebook secretly tracked mobile users' use of WhatsApp, and when Facebook determined that WhatsApp threatened to become a platform entirely independent of Facebook's network and social data, it purchased WhatsApp at an irrational price of thousands of times the company's revenue.

376. By acquiring potential threats independent of its platform, particularly WhatsApp and Instagram, Facebook ensured that such companies could not be (a) alternative platforms upon which developers excluded by Facebook's API removal could build their apps; (b) alternative sources of social data that could be monetized; or (c) alternative social networks that would attract users, developers, and advertisers, thereby weakening the SDBE protecting Facebook's business.

377. Facebook's past integration of these acquired assets and its continuing effort to integrate these acquired assets has continuing anticompetitive effect and threatens to increase and/or maintain Facebook's dominance in the Social Data and Social Advertising markets.

378. Facebook also used Onavo and the Onavo assets to maintain a real-time view of users' mobile application use and mobile traffic. Facebook used that real-time information to monitor, punish, or acquire any competitive threats. Indeed, Facebook used Onavo surveillance data to target threats for denial of access to crucial APIs; for Whitelist and Data Sharing Agreements; or for targeted removal from the market through acquisition.

379. The net effect of Facebook's scheme was to, *inter alia*, strengthen and maintain the SDBE, protect its monopoly in the Relevant Markets, prevent market entry by a potential rival, and reduce consumer choice.

380. The scheme also ensured that there would be no competition by a rival social network or application on non-price bases, such as, for example, increased privacy, more features, higher quality features, new features, more valuable social connections, reduced advertising to users, or new use cases. The scheme also foreclosed new or alternate business models by competitors or potential competitors, including the business model Facebook itself forwent and sacrificed for anticompetitive purposes—charging developers and competitors for API / Platform access or advertising.

381. Facebook's anticompetitive scheme has also allowed it to raise prices for social data and for social advertising during and after the execution of the scheme. Facebook continues to be one of the only sources for targeted social data or advertising in the United States and in most of the world. As evidence of its market power in the Social Data and Social Advertising Markets, Facebook has raised prices for social data without sacrificing any demand.

382. Facebook's acquisitions of Instagram and WhatsApp continue to harm competition in the Relevant Markets, reduce consumer choice, prevent entry by a potential competitor, and allow Facebook to evade regulators. These assets are being integrated, which will unify global and

domestic U.S. markets, resulting in a significant increase in global market share, preventing a rival from attracting enough users to reach a critical mass of social data, preventing a rival from starting a competing social network, and strengthening the SDBE.

383. If allowed to integrate its products, Facebook's dominance of the Relevant Markets will be virtually impossible to reverse. Facebook's network will have grown to such a size that a new entrant could not build a network large enough to coax Facebook's users to change platforms. Once integration is complete, a new entrant would have to rival Facebook's more than 2-billion-person network of users. Such an entry would be cost prohibitive and require an unprecedented amount of economic and human capital. No competitor or potential entrant exists that at the time of this complaint to successfully attempt such an entry.

384. Facebook's anticompetitive scheme excludes developers, including Plaintiffs, from the Relevant Markets; prevents entry by a competitor in the relevant markets; and strengthens the SDBE protecting Facebook's business.

385. Plaintiffs are therefore harmed in their business and property because they have been excluded from the Relevant Markets; had their business and assets destroyed by Facebook's anticompetitive scheme; and are presently, as a result of Facebook's exclusionary conduct, prevented from entry/reentry in the Relevant Markets or from staging an entry that could threaten Facebook's dominant position in the Relevant Markets.

CONCEALMENT AND TOLLING

386. For many years, Facebook and its executives took great pains to hide the truth about the Platform API withdrawal; the reciprocity agreements; and the rest of the anticompetitive scheme. Through NDAs; through overbroad and/or improper assertions of privilege and confidentiality; through lies to regulators, to the press, to developers, and to the public; and through other means and mechanisms of intentionally suppressing and concealing from public view the true nature, motivation, mechanisms, and intent of Facebook's actions, Defendant managed to hide the specific facts of its anticompetitive conduct from Plaintiffs until November 6, 2019, when NBC

News published a trove of internal Facebook documents and communications that laid bare the truth about Defendants' scheme.

387. Until no earlier than November 6, 2019, Plaintiffs did not know, and could not reasonably have known, the truth about Facebook's anticompetitive conduct, including its purpose and intent to engage in anticompetitive conduct, as alleged in this Complaint.

CLASS ACTION ALLEGATIONS

388. The class's claims all derive directly from a course of conduct by Facebook. Facebook has engaged in uniform and standardized conduct toward the class. Facebook did not materially differentiate in its actions or inactions toward members of the class. The objective facts on these subjects are the same for all class members. Within each Claim for Relief asserted by the class, the same legal standards govern. Accordingly, Plaintiffs bring this lawsuit as a class action on their own behalf and on behalf of all other persons similarly situated as members of the proposed class pursuant to Federal Rules of Civil Procedure 23(a) and (b)(3) and/or (b)(2) and/or (c)(4). This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of those provisions.

The Nationwide Developer Class

389. Plaintiffs bring this action and seek to certify and maintain it as a class action under Rules 23(a); (b)(2); and/or (b)(3); and/or (c)(4) of the Federal Rules of Civil Procedure on behalf of themselves and a Nationwide Developer Class defined as follows:

> All persons, entities, corporations in the United States who were excluded from the Social Data Market or injured by Facebook's decision to withdraw the Graph APIs, for the period beginning May 24, 2010 until April 30, 2015 (the "Class Period").

390. Excluded from the Nationwide Developer Class is Facebook, its employees, officers, directors, legal representatives, heirs, successors, and wholly or partly owned subsidiaries or affiliates; and the judicial officers and their immediate family members and associated court staff assigned to this case.

Numerosity and Ascertainability

391. This action satisfies the requirements of Fed. R. Civ. P. 23(a)(1). There are tens of thousands of developers nationwide and throughout the world that relied on Facebook's Open Graph API during the Class Period. Individual joinder of all Class members is impracticable.

392. The Class is ascertainable because its members can be readily identified using API tokens, developer registrations, and other records and information kept by Facebook or third parties in the usual course of business and within their control. Plaintiffs anticipate providing appropriate notice to the certified Class, in compliance with Fed. R. Civ. P. 23(c)(1)(2)(A) and/or (B), to be approved by the Court after class certification, or pursuant to court order under Fed. R. Civ. P. 23(d).

Predominance of Common Issues

393. This action satisfies the requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3) because questions of law and fact that have common answers that are the same for the Class predominate over questions affecting only individual Class members. These include, without limitation, the following:

a. Whether Defendant monopolized the Social Data Market.

b. Whether Defendant, its employees or affiliates, intended to monopolize the Social Data Market.

c. Whether Defendant attempted to monopolize the Social Data Market.

d. Whether Defendant possessed monopoly or market power in the Social Data Market.

e. Whether user data and data obtained by third parties created a Social Data Barrier to Entry that protected Facebook's market position and/or monopoly, reduced competition or entry in the Social Data Market, and/or increased prices for products in that market, including, but not limited to, advertising and API access.

f. Whether Defendant's decision to withdraw the Friend and Feed Graph APIs lacked any justification and/or whether the procompetitive effects of the decision to do so, if any, was outweighed by the anticompetitive effects.

g. Whether Defendant sacrificed profits to monopolize, or attempt to monopolize, the Social Data Market.

h. Whether the procompetitive effects of the decision to withdraw the Friend and Feed Graph APIs, if any at all existed, could have been accomplished by less restrictive means.

i. Whether the procompetitive effects of Defendant's agreements with whitelisted developers, if any, could have been achieved by less restrictive means.

j. Whether Defendant's agreements with whitelisted developers violated Sections 1 and 2 of the Sherman Act, including whether the agreements restrained trade or strengthened the Social Data Barrier to Entry.

k. Whether the procompetitive effects of Defendant's agreements with whitelisted developers, if any, were outweighed by the anticompetitive effect.

l. Whether the procompetitive effects of Defendant's agreements with whitelisted developers, if any, could have been achieved by less restrictive means.

m. Whether Defendant's purchase of WhatsApp violated Sections 2 of the Sherman Act and 7 of the Clayton Act.

n. Whether Defendant's purchase of Instagram violated Section 2 of the Sherman Act and 7 of the Clayton Act.

o. Whether injunctive relief, prospective relief, or divestiture of WhatsApp, Instagram, Messenger, or any other Facebook line of business is required to remedy the anticompetitive effects of Defendant's conduct and/or Defendant's violations of the antitrust laws.

p. Whether Defendant's conduct harmed competition in the Social Data Market.

q. Whether Defendant's conduct caused price increases or the reduction of consumer or developer choice in the Social Data Market.

r. Whether Defendant's unlawful conduct was a substantial contributing factor in the injury to members of the Class.

Typicality

394. This action satisfies the requirements of Fed. R. Civ. P. 23(a)(3) because Plaintiffs' claims are typical of the claims of other Class members and arise from the same course of conduct by Defendant. The relief Plaintiffs seek is typical of the relief sought for the absent Class members.

Adequate Representation

395. Plaintiffs will fairly and adequately represent and protect the interests of the Class. Plaintiffs have retained counsel with substantial experience in prosecuting consumer class actions, including actions involving defective products.

396. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the Class and have the financial resources to do so. Neither Plaintiffs nor their counsel have interests adverse to those of the Class.

Superiority

397. This action satisfies the requirements of Fed. R. Civ. P. 23(b)(2) because Defendant has acted and refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive and/or corresponding declaratory relief with respect to the Class as a whole.

398. This action satisfies the requirements of Fed. R. Civ. P. 23(b)(3) because a class action is superior to other available methods for the fair and efficient adjudication of this controversy. The common questions of law and fact regarding Defendant's conduct and responsibility predominate over any question affecting only individual Class members.

399. Because the damages suffered by each individual Class member may be relatively smaller than the costs of litigation, the expense and burden of individual litigation would make it

very difficult or impossible for individual Class members to redress the wrongs done to each of them individually, such that most or all Class members would have no rational economic interest in individually controlling the prosecution of specific actions, and the burden imposed on the judicial system by individual litigation by even a small fraction of the Class would be enormous, making class adjudication the superior alternative under Fed. R. Civ. P. 23(b)(3)(A).

400. The conduct of this action as a class action presents far fewer management difficulties, far better conserves judicial resources and the parties' resources, and far more effectively protects the rights of each Class member than would piecemeal litigation. Compared to the expense, burdens, inconsistencies, economic infeasibility, and inefficiencies of individualized litigation, the challenges of managing this action as a class action are substantially outweighed by the benefits to the legitimate interests of the parties, the court, and the public of class treatment in this Court, making class adjudication superior to other alternatives, under Fed. R. Civ. P. 23(b)(3)(D).

401. Plaintiffs are not aware of any obstacles likely to be encountered in the management of this action that would preclude its maintenance as a class action. Rule 23 provides the Court with authority and flexibility to maximize the efficiencies and benefits of the class mechanism and reduce management challenges. The Court may, on motion of Plaintiffs or on its own determination, certify nationwide, statewide, and/or multistate classes for claims sharing common legal questions; utilize the provisions of Rule 23(c)(4) to certify any particular claims, issues, or common questions of fact or law for class-wide adjudication; certify and adjudicate bellwether class claims; and utilize Rule 23(c)(5) to divide any class into subclasses.

REALLEGATION AND INCORPORATION BY REFERENCE

402. Plaintiffs reallege and incorporate by reference all the preceding paragraphs and allegations of this Complaint, as though fully set forth in each of the following Claims for Relief asserted on behalf of the Class.

CLAIMS FOR RELIEF

COUNT I
SECTION 2 SHERMAN ACT: MONOPOLIZATION

403. Defendant has willfully acquired and maintained monopoly power for Facebook in the relevant markets for Social Data and Social Advertising.

404. Facebook possesses monopoly power in the relevant markets for Social Data and Social Advertising. Facebook has the power to control prices or exclude competition in the relevant markets.

405. Since at least as early as 2010, Facebook has occupied a dominant position in the Social Data Market, with a user share worldwide during the relevant period of more than 60% of users on comparable social networks when user shares of its WhatsApp, Instagram, Facebook, and Messenger products are aggregated. As of October 2019, Facebook controlled approximately 66% of worldwide users in the Social Data Market.

406. Facebook's revenue share of the Social Advertising Market is approximately 80%; its share has been above 70% since 2015.

407. Defendant has willfully acquired and maintained monopoly power for Facebook in the relevant markets for Social Data and Social Advertising. As alleged herein Defendant has accomplished this by means of predatory, exclusionary, and anticompetitive conduct, including but not limited to: removing friends, news feed, and other crucial APIs; refusing to sell social data to competing applications developers; extracting social data from competitors through threats of blacklisting and/or through nonconsensual data scraping; targeting competitors for reciprocity or denial of API access; entering into whitelisting and data sharing agreements with competitors; and engaging in covert surveillance of competitors' users in order to detect and ultimately acquire competitive threats before they became too formidable.

408. Defendant's conduct alleged above has had an anticompetitive effect in the relevant markets for Social Data and Social Advertising.

409. Defendant's conduct alleged herein has no legitimate business purpose or procompetitive effect.

410. Defendant's conduct has had a substantial effect on interstate commerce.

411. Plaintiffs and the Nationwide Developer Class have been and will be injured in their business or property as a result of Defendant's conduct alleged herein.

412. Plaintiffs and the Nationwide Developer Class have suffered and will suffer injury of the type that the antitrust laws were intended to prevent. Plaintiffs and the Nationwide Developer Class have been and will be injured by the harm to competition as a result of Defendant's conduct.

COUNT II
SECTION 2 SHERMAN ACT:
ATTEMPTED MONOPOLIZATION

413. As alleged herein, Defendant has engaged in predatory, exclusionary, and anticompetitive conduct, including but not limited to: removing friends, news feed, and other crucial APIs; refusing to sell social data to competing applications developers; extracting social data from competitors through threats of blacklisting and/or through nonconsensual data scraping; targeting competitors for reciprocity or denial of API access; entering into whitelisting and data sharing agreements with competitors; and engaging in covert surveillance of competitors' users in order to detect and ultimately acquire competitive threats before they became too formidable.

414. Defendant's conduct alleged above has had an anticompetitive effect in the relevant markets for Social Data and Social Advertising.

415. Defendant's conduct alleged herein has no legitimate business purpose or procompetitive effect.

416. Defendant has engaged in that conduct with the specific intent of monopolizing the relevant markets for Social Data and Social Advertising.

417. Defendant has engaged in that conduct with a dangerous probability of monopolizing the relevant markets for Social Data and Social Advertising.

418. Defendant's conduct has had a substantial effect on interstate commerce.

419. Plaintiffs and the Nationwide Developer Class have been and will be injured in their business or property as a result of Defendant's conduct alleged herein.

420. Plaintiffs and the Nationwide Developer Class have suffered and will suffer injury of the type that the antitrust laws were intended to prevent. Plaintiffs and the Nationwide Developer Class have been and will be injured by the harm to competition as a result of Defendant's conduct

COUNT III
SECTION 1 SHERMAN ACT:
WHITELIST AND DATA SHARING AGREEMNTS

421. As alleged above, Facebook forced certain third-party developers that it identified as competitive threats that had valuable social data to sign Private Extended API agreements, or as referred to throughout this Complaint as "Whitelist and Data Sharing Agreements," in order to obtain access to the Friend or Newsfeed APIs. In those agreements, Facebook conditioned the provision of social data and/or access to vital Facebook APIs upon massive purchases of Facebook's social data through mobile advertising and/or the provision of the developer's own sensitive social data back to Facebook. The result of the network of Whitelist agreements was a hub-and-spoke agreement to control the supply of social data. Those who obtained access to the Facebook APIs were required to both provide data to the hub (Facebook) and to purchase data from it.

422. As such, Defendant has induced or coerced various software developers, social networks, and other enterprises to enter into one or more contracts, combinations, or conspiracies to unreasonably restrain trade, to control prices or exclude competition, and to willfully acquire and maintain monopoly power for Facebook in the relevant market for markets for Social Data and Social Advertising.

423. Defendant's conduct with respect to the Whitelist and Data Sharing Agreements, as alleged herein, has had an anticompetitive effect in the relevant markets for Social Data and Social Advertising.

424. Defendant's conduct with respect to the Whitelist and Data Sharing Agreements, as alleged herein, has no legitimate business purpose or procompetitive effect.

425. Defendant's conduct with respect to the Whitelist and Data Sharing Agreements, as alleged herein, has had a substantial effect on interstate commerce.

426. Plaintiffs and the Nationwide Developer Class have been and will be injured in their business or property as a result of Defendant's conduct, alleged herein, with respect to the Whitelist and Data Sharing Agreements.

427. Plaintiffs and the Nationwide Developer Class have suffered and will suffer injury of the type that the antitrust laws were intended to prevent. Plaintiffs and the Nationwide Developer Class have been and will be injured by the harm to competition as a result of Defendant's conduct, alleged herein, with respect to the Whitelist and Data Sharing Agreements.

COUNT IV
SECTION 7 CLAYTON ACT:
ACQUISITION AND INTEGRATION OF INSTAGRAM

428. Facebook's acquisition and integration of Instagram and WhatsApp has had, and will have, the effect of substantially lessening competition and tending to create a monopoly in the relevant markets for Social Data and Social Advertising.

429. As alleged herein, Defendant has, dating to the departures of the founders of WhatsApp and Instagram in 2018, begun to put the Instagram and WhatsApp assets to new and anticompetitive purposes.

430. Facebook's acquisition and integration of Instagram and WhatsApp, and Defendant's conduct related thereto, as alleged herein, has had a substantial effect on interstate commerce.

431. Plaintiffs and the Nationwide Developer Class have been and will be injured in their business or property as a result of Defendant's conduct, alleged herein, with respect to the acquisition and integration of Instagram and WhatsApp.

432. Plaintiffs and the Nationwide Developer Class have suffered and will suffer injury of the type that the antitrust laws were intended to prevent. Plaintiffs and the Nationwide Developer Class have been and will be injured by the substantial lessening of competition and tendency to create a monopoly as a result of the acquisition and integration of Instagram and WhatsApp.

COUNT V
SECTION 2 SHERMAN ACT:
ACQUISITION AND INTEGRATION OF WHATSAPP

433. Through Facebook's acquisition and integration of Instagram and WhatsApp, Defendant has willfully acquired and maintained monopoly power for Facebook in the relevant markets for Social Data and Social Advertising.

434. In part through its acquisition of Instagram and WhatsApp, Facebook possesses monopoly power in the relevant markets for Social Data and Social Advertising. Facebook has—and will continue to consolidate—the power to control prices or exclude competition in the relevant markets.

435. Through their acquisition of WhatsApp and Instagram, and through their nearly-complete plan to integrate the backends of the WhatsApp, Instagram and Facebook products, Defendant has acquired, maintained, and consolidated, and continues to willfully acquire, maintain, and consolidate, monopoly power for Facebook in the relevant markets for Social Data and Social Advertising.

436. Once the backend of the three platforms is integrated—an event which reportedly will occur early in 2020—the 2.6 billion users across Facebook, WhatsApp and Instagram will be able to communicate across platforms for the first time, creating a massive and unprecedented concentration of market power.

437. Defendant's conduct alleged herein with respect to the acquisition and integration of Instagram and WhatsApp has had, and will continue to have, an anticompetitive effect in the relevant markets for Social Data and Social Advertising.

438. Defendant's conduct alleged herein with respect to the acquisition and integration of Instagram and WhatsApp has had, and will continue to have, has no legitimate business purpose or procompetitive effect.

439. Facebook's acquisition and integration of Instagram and WhatsApp, and Defendant's conduct related thereto, as alleged herein, have had a substantial effect on interstate commerce.

440. Plaintiffs and the Nationwide Developer Class have been and will be injured in their business or property as a result of Defendant's conduct, alleged herein, with respect to the acquisition and integration of Instagram and WhatsApp.

441. Plaintiffs and the Nationwide Developer Class have suffered and will suffer injury of the type that the antitrust laws were intended to prevent. Plaintiffs and the Nationwide Developer Class have been and will be injured by the substantial lessening of competition and tendency to create a monopoly as a result of the acquisition and integration of Instagram and WhatsApp.

COUNT VI
INJUNCTIVE RELIEF AND DIVESTITURE

442. Plaintiffs seek preliminary and permanent relief against Facebook. To begin with, in the absence of such relief, developers and other competitors will not be able to enter into the Social Data or Social Advertising markets without having to penetrate the SDBE protecting Facebook's business. Even upon entry, Facebook can use its considerable market power, as it has in the past (including as described in this Complaint) to destroy the entrant.

443. Plaintiffs and members of the Class are irreparably harmed by Facebook's maintenance of its unlawful monopoly and market power in the Relevant Markets, including, inter alia, because they are prevented from competing on the merits in those markets or re-entering those markets after having been excluded as a result of Facebook's anticompetitive conduct.

444. Facebook's market share has increased dramatically. As described above, it now has a dominant share in both the Social Data and Social Advertising Markets, as well as the power to raise and/or control the price of advertising or the cost of user data acquisition. Absent injunctive

relief, Facebook's market share is likely going to remain high in the concentrated Relevant Markets, if not grow further.

445. Absent injunctive relief, Facebook's users will lack any viable choices for the services Facebook provides to them in exchange for their data. Because Facebook can control the amount of user data and privacy controls that a user of social networks can demand, other networks could not compete with Facebook simply by increasing the value they provide to users or increasing their costs of social data acquisition.

446. Moreover, Facebook's market power and the SDBE protecting its business continue to foreclose consumer choice because users lack a competitive platform to which they can move if they are unsatisfied with Facebook's demands of them, including the level of privacy provided to them to obtain their social data.

447. In the absence of preliminary and final injunctive relief, the increase in Facebook's position that will result from its continuing illegal conduct, including its imminent integration of its WhatsApp and Instagram products, will so entrench it (and so weaken its competitors) that the cost of reversing Facebook's imminent domination of the Relevant Markets could be prohibitive.

448. Plaintiffs and members of the class have no adequate remedy at law to prohibit Facebook from its continuing abuse of power.

449. Indeed, absent divesture of Facebook's WhatsApp and Instagram assets, Facebook can integrate the apps at any time, consolidating its market power across the globe, likely permanently foreclosing competition in the Relevant Markets for decades to come.

450. Moreover, because Zuckerberg controls all of the voting rights associated with Facebook's common stock, he will likely exert significant control over the company, its assets, its executives, and its partners unless he is divested of such control. There is no adequate remedy of law to prevent the irreparable harm that has—and will continue—to result from Zuckerberg's continued control of Facebook. Plaintiffs and Class Members accordingly request that the Court order Zuckerberg to divest himself of incontestable control over the company.

451. Plaintiffs and Class members respectfully request that the Court immediately appoint a monitor to oversee Facebook's conduct, including its imminent integration of its WhatsApp and Instagram products. Such preliminary relief is the only way to prevent Facebook from impairing the Court's ability to enter a final injunction in this case.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs request that judgment be entered against Defendant and that the Court grant the following:

A. Determine that this action may be maintained as a class action pursuant to Rules 23(a), (b)(2), (b)(3) and/or (c)(4) of the Federal Rules of Civil Procedure, and direct that reasonable notice of this action, as provided by Rule 23(c)(2), be given to the Class, and declare Plaintiffs as the representatives of the Class;

B. Enter a judgment against Defendant in favor of Plaintiffs and the Class;

C. Award the Class damages (i.e., three times their damages) in amount to be determined at trial;

D. Award actual, compensatory, statutory, and consequential damages;

E. Award equitable monetary relief, including restitution and disgorgement of all ill-gotten gains, and the imposition of a constructive trust upon, or otherwise restricting the proceeds of Defendant's ill-gotten gains, to ensure an effective remedy.

F. Grant permanent injunctive relief pursuant to Section 16 of the Clayton Act to remedy the ongoing anticompetitive effects of Defendant's unlawful conduct.

G. Award pre-judgment and post-judgment interest at the highest rate allowed by law;

H. Award Plaintiffs and the Class their costs of suit, including reasonable attorneys' fees as provided by law; and

I. Award such further and additional relief as the case may require and the Court may deem just and proper under the circumstances.

JURY DEMAND

Plaintiffs demand a trial by jury on all claims so triable as a matter of right.

Dated: January 16, 2020

Respectfully submitted,

/s/ Brian J. Dunne
Brian J. Dunne (SBN 275689)
bdunne@piercebainbridge.com
PIERCE BAINBRIDGE BECK PRICE & HECHT LLP
355 S. Grand Ave. 45th Floor
Los Angeles, CA 90071
(213) 262-9866

/s/ Yavar Bathaee
Yavar Bathaee (SBN 282388)
yavar@piercebainbridge.com
Michael M. Pomerantz (NY 2920932)
(*pro hac vice* forthcoming)
mpomerantz@piercebainbridge.com
David L. Hecht (NY 4695961)
(*pro hac vice* forthcoming)
dhecht@piercebainbridge.com
Adam C. Ludemann (NY 5352323)
aludemann@piercebainbridge.com
(*pro hac vice* forthcoming)
PIERCE BAINBRIDGE BECK PRICE & HECHT LLP
277 Park Ave. 45th Floor
New York, NY 10172
(212) 484-9866