

## TABLE OF CONTENTS

	<u>Page</u>
APPENDIX A: Amended Opinion and Order Denying Rehearing of the United States Court of Appeals for the Ninth Circuit (Dec. 4, 2023)	1a
APPENDIX B: Opinion of the United States Court of Appeals for the Ninth Circuit (Oct. 18, 2023)	54a
APPENDIX C: Order Granting Motion to Dismiss Without Leave to Amend of the United States District Court for the Northern District of California (Dec. 20, 2021)	109a
APPENDIX D: Order Granting Motion to Dismiss with Leave to Amend of the Unite States District Court for the Northern District of California (Aug. 7, 2020)	
APPENDIX E: Statutory and Regulatory Provisions Involved	225a
15 U.S.C. § 78j	225a
17 C.F.R. § 240.10b–5	227a

## **APPENDIX A**

## UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

In re: FACEBOOK, INC. SECURITIES LITIGATION,

AMALGAMATED BANK, Lead Plaintiff; PUBLIC EM-PLOYEES' RETIREMENT SYSTEM OF MISSISSIPPI; JAMES KACOURIS, individually and on behalf of all others similarly situated,

Plaintiffs-Appellants,

v.

FACEBOOK, INC.; MARK ZUCKERBERG; SHERYL SANDBERG; DAVID M. WEHNER,

Defendants-Appellees.

No. 22-15077

D.C. No. 5:18-cv-01725-EJD

ORDER AND AMENDED OPINION

Appeal from the United States District Court for the Northern District of California Edward J. Davila, District Judge, Presiding

> Argued and Submitted February 8, 2023 San Francisco, California

> > Filed October 18, 2023 Amended December 4, 2023

Before: M. Margaret McKeown, Jay S. Bybee, and Patrick J. Bumatay, Circuit Judges. Opinion by Judge McKeown; Partial Concurrence and Partial Dissent by Judge Bumatay

## **SUMMARY**\*

#### **Securities Fraud**

The panel filed (1) an order denying a petition for panel rehearing and a petition for rehearing en banc; and (2) an amended opinion affirming in part and reversing in part the district court's dismissal of a securities fraud action against Facebook, Inc., and three of its executives, and remanding for further proceedings.

Cambridge Analytica improperly harvested personal data from millions of unwitting Facebook users and retained copies of the data beyond Facebook's control. Facebook had known of Cambridge Analytica's misconduct for over two years and failed to inform affected users, and Facebook surreptitiously allowed certain whitelisted third-party apps to access users' Facebook friend data without the users' friends' consent.

Facebook shareholders filed suit, alleging that the defendants violated Sections 10(b), 20(a), and 20A of the Securities Exchange Act of 1934 and Rule 10b-5 by making materially misleading statements and omissions regarding the risk of improper access to Facebook users' data, Facebook's internal investigation into Cambridge Analytica, and the control Facebook users had over their data.

The panel held that, under the heightened standard of the Private Securities Litigation Reform Act, the shareholders adequately pleaded falsity as to the

<sup>\*</sup> This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

some of the challenged risk statements. The panel followed In re Alphabet Sec. Litig., 1 F.4th 687 (9th Cir. 2021), which held that falsity allegations were sufficient to survive a motion to dismiss when the complaint plausibly alleged that a company's SEC filings warned that risks "could" occur when, in fact, those risks had already materialized. The panel concluded that the shareholders adequately pleaded falsity as to the statements warning that misuse of Facebook users' data could harm Facebook's business, reputation, and competitive position, and the district court erred by dismissing the complaint as to those statements. The panel concluded, however, that the district court correctly dismissed the challenged statements regarding the risk of security breaches and the risk of the public not perceiving Facebook's products to be "useful, reliable, and trustworthy." The panel left to the district court on remand whether the shareholders could satisfy the other elements of the claims with respect to risk statements.

The panel held that the shareholders did not adequately plead facts giving rise to a strong inference of scienter as to the Cambridge Analytica investigation statements, and the panel affirmed the district court's dismissal as to these statements.

The panel held that the shareholders adequately pleaded loss causation as to some of the user control statements. The panel affirmed the dismissal of the statements related to Facebook's goals of transparency and control, and a June 2018 whitelisting revelation as a standalone claim. The panel reversed the dismissal as to other statements related to Facebook stock price drops.

Concurring in part and dissenting in part, Judge Bumatay joined the majority in holding that the shareholders failed to sufficiently allege a falsity in Facebook's Cambridge Analytica investigation statements. He also joined the majority in holding that the shareholders did allege a falsity and loss from the user control statements, but only as those statements relate to Facebook's practice of "whitelisting." He disagreed with the majority on two fundamental points. In his view, the shareholders failed to sufficiently allege that Facebook's risk factor statements in its public filings were fraudulent, and they did not show that Facebook's user control statements were false based on the Cambridge Analytica revelations.

## COUNSEL

Tom Goldstein (argued) and Erica O. Evans, Goldstein & Russell PC, Bethesda, Maryland; Kevin K. Russell, Goldstein Russell & Woofter LLC, Washington, D.C.; John C. Browne and Jeremy P. Robinson, Bernstein Litowitz Berger & Grossman LLP, New York, New York; Joseph D. Daley, Danielle S. Myers, and Darren J. Robbins, Robbins Geller Rudman & Dowd LLP, San Diego, California; Jason C. Davis, Robbins Geller Rudman & Dowd LLP, San Francisco, California; Kathleen Foley, Munger Tolles & Olson LLP, Washington, D.C.; Jeremy A. Lieberman, Pomerantz LLP, New York, New York; Jennifer Pafiti, Pomerantz LLP, Los Angeles, California; for Plaintiffs-Appellants.

Joshua S. Lipshutz (argued), Katherine M. Meeks, and Trenton J. Van Oss, Gibson Dunn & Crutcher LLP, Washington, D.C.; Brian M. Lutz and Michael J. Kahn, Gibson Dunn & Crutcher LLP, San Francisco, California; Orin S. Snyder, Gibson Dunn & Crutcher LLP, New York, New York; Paul J. Collins, Gibson Dunn & Crutcher LLP, Palo Alto, California; for Defendants-Appellees.

## **ORDER**

An Amended Opinion is being filed simultaneously with this Order.

The panel voted to deny the petition for panel rehearing. Judges McKeown and Bybee recommended denial of the petition for rehearing en banc, and Judge Bumatay voted to grant the petition for rehearing en banc.

The full court has been advised of the petition for rehearing en banc and no judge of the court has requested a vote on whether to rehear the matter en banc. Fed. R. App. P. 35.

Appellees' petition for panel rehearing and rehearing en banc, Dkt. No. 50, is **DENIED**.

## **OPINION**

McKEOWN, Circuit Judge:

In March 2018, news broke that Cambridge Analytica, a British political consulting firm, improperly harvested personal data from millions of unwitting Facebook users and retained copies of the data beyond Facebook's control. In the months that followed, the public learned that Facebook had known of Cambridge Analytica's misconduct for over two years and failed to inform affected users, and that Facebook surreptitiously allowed certain whitelisted third-party apps to access users' Facebook friend data without the users' friends' consent. Facebook and its executives made various statements before and after the news announcements assuring users that they fully controlled their data on Facebook and that no third party would access the data without their consent. In the wake of the Cambridge Analytica and whitelisting scandals, Facebook's stock price suffered two significant drops totaling more than \$200 billion in market capitalization.1

Appellants, collectively "the shareholders," purchased shares of Facebook common stock between February 3, 2017, and July 25, 2018. Soon after the first stock drop in March 2018, they filed a securities fraud action against Facebook and three of its executives: Mark Zuckerberg, Facebook's chief executive officer, Sheryl Sandberg, Facebook's then-chief operating officer, and David Wehner, Facebook's chief financial officer. The shareholders allege that Facebook

<sup>&</sup>lt;sup>1</sup> In late 2021, the parent company Facebook changed its name to Meta Platforms, Inc. Because the events in this case occurred before 2021, we refer to Facebook and its former parent company, Facebook, Inc., simply as Facebook.

and the executives violated Sections 10(b), 20(a), and 20A of the Securities Exchange Act of 1934 and Rule 10b-5 of the Exchange Act's implementing regulations by making materially misleading statements and omissions regarding the risk of improper access to Facebook users' data, Facebook's internal investigation into Cambridge Analytica, and the control Facebook users have over their data. Although the shareholders made multiple claims in their Third Amended Complaint, only these three categories of claims are the subject of this appeal.

This case calls on us to consider whether, under the heightened standard of the Private Securities Litigation Reform Act ("PSLRA"), the shareholders adequately pleaded falsity as to the challenged risk statements, adequately pleaded scienter as to the Cambridge Analytica investigation statements, and adequately pleaded loss causation as to the user control statements. We affirm in part and reverse in part.<sup>2</sup>

#### I. BACKGROUND

The Third Amended Complaint clocked in at 285 pages. Although impressive in terms of magnitude, we nonetheless examine the allegations individually and holistically, not by weight or volume.<sup>3</sup>

 $<sup>^2</sup>$  For ease of reference, we use the categories laid out in the Third Amended Complaint. On appeal, the shareholders challenge the district court's dismissal of the statements in ¶¶ 501–05, 507–14, 519, 525, 530, 533, and 537–38 of the Third Amended Complaint.

<sup>&</sup>lt;sup>3</sup> These facts are based on the allegations in the Third Amended Complaint and may not reflect Facebook's current practices.

Facebook, with more than 1.3 billion daily users at the inception of this case, is the world's largest social media platform. On Facebook, users share personal content, "like" and comment on others' shared content, play games designed by third-party app developers, and more. Facebook collects data from its users, including the types of content they access, the devices they use to access Facebook, their payment information, and their location. The collected data is used to individualize the content a user sees on Facebook. For example, Facebook may suggest local events to a user and tailor the advertisements a user sees. Additionally, a third-party app or website integrated onto the Facebook platform may access user information when the user engages with its services on the platform. For example, a Facebook user may play an online game added to the Facebook platform by a third-party developer. According to Facebook's terms, the game developer could then access the user's age range, location, language preference, list of friends, and other information the user shared with them.

This is not the first time Facebook has found itself in legal hot water over its data sharing practices. In 2012, Facebook settled charges with the Federal Trade Commission ("FTC") that it deceived users by representing that their personal data was private but allowing the data to be shared, including with third-party apps. Facebook entered a twenty-year consent decree as part of the settlement, agreeing not to misrepresent the extent to which Facebook users could control the privacy of their own data. In 2019, the FTC imposed a "record-breaking \$5 billion penalty" on Facebook for violating the consent decree by "deceiving users about their ability to control the privacy of their

personal information."<sup>4</sup> Facebook users have also sued the company alleging that Facebook is dishonest about its privacy practices. See, e.g., In re Facebook, Inc. Internet Tracking Litig., 956 F.3d 589 (9th Cir. 2020); Campbell v. Facebook, Inc., 951 F.3d 1106 (9th Cir. 2020).

In 2014, Zuckerberg announced publicly that Facebook would no longer allow third parties to access and collect data from users' friends, noting that Facebook users were surprised to learn that their Facebook friends could share their data with a third party without their consent. He explained that Facebook users had grown skeptical that their data was safe on the platform, and that Facebook was doing everything it could "to put people first and give people the tools they need" to trust that Facebook would keep their data safe. That same year, however, Zuckerberg and Sandberg created a "reciprocity" system in which certain third-party apps that provided "reciprocal value to Facebook" could be "whitelisted," meaning that those apps were exempt from the ban on third-party data access and collection. The whitelisting practice continued until mid-2018.

In September 2015, Facebook employees noticed that Cambridge Analytica was "receiving vast amounts of Facebook user data." Facebook's political team described Cambridge Analytica as a "sketchy" firm that had "penetrated" Facebook's market and requested an investigation into what Cambridge Analytica was doing with the data. The platform policies

<sup>&</sup>lt;sup>4</sup> Press Release, Fed. Trade Comm'n, FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook.

team concluded that it was unlikely Cambridge Analytica could use Facebook users' data for political purposes without violating Facebook's policies. In November 2015, Facebook paid Aleksandr Kogan, a Cambridge University academic who helped Cambridge Analytica obtain user data from Facebook, to give an internal presentation on the lessons he learned from collecting and working with the Facebook data.

Trouble for Facebook began in December 2015, when The Guardian reported that Cambridge Analytica had created a database of information about American voters by harvesting their Facebook data. The harvested data originated from a personality guiz integrated onto Facebook by Kogan. When Facebook users completed the quiz, Kogan gained access to their data as well as data from their Facebook friends who had not taken the quiz, including each user's name, gender, location, birthdate, "likes," and list of Facebook friends. Facebook's app review team initially rejected the personality quiz because it collected more user data than necessary to operate, but the quiz nonetheless became available to Facebook users. Although only about 250,000 Facebook users took the personality quiz, Kogan harvested data from over thirty million users, most of whom did not consent to the data collection.

Kogan used the Facebook "likes" collected from the quiz to train an algorithm that assigned personality scores to Facebook users, including users who had not taken the quiz. The information was saved in a

<sup>&</sup>lt;sup>5</sup> See Harry Davies, Ted Cruz Using Firm that Harvested Data on Millions of Unwitting Facebook Users, Guardian (Dec. 11, 2015), https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data.

database that classified American voters by scoring them on five personality traits: "openness to experience, conscientiousness, extraversion, agreeableness, and neuroticism (the 'OCEAN scale')." According to *The Guardian*, Cambridge Analytica used the harvested OCEAN scale data to help Ted Cruz's presidential campaign "gain an edge over Donald Trump" in the Republican Party primaries.

In response to the *Guardian* article, a Facebook spokesperson stated that the company was "carefully investigating" the situation, that misusing user data was a violation of Facebook's policies, and that the company would "take swift action" against third parties found to have misused Facebook users' data. In a private email exchange in December 2015, a Facebook executive told a Cambridge Analytica executive that Cambridge Analytica violated Facebook's policies and terms by using data that Kogan "improperly derived" from Facebook. Cambridge Analytica agreed in January 2016 to delete the personality score data harvested from Facebook.

Notwithstanding Cambridge Analytica's assurance that it would delete the data, Facebook continued to investigate the data usage. In June 2016, Facebook negotiated a confidential settlement with Kogan, who certified that he had deleted the data in his possession derived from Facebook "likes." Kogan also provided Facebook with the identity of every entity with which he had shared raw Facebook user data. In doing so, Kogan revealed that he had shared derivative and raw data from Facebook users—not just the personality score data—with Cambridge Analytica's chief executive, Alexander Nix, and that the data was still being used in violation of Facebook's stated policies. Facebook asked Nix to certify that all data harvested from

the Facebook personality quiz was deleted, but Nix refused to do so. In October 2016, *The Washington Post* reported that Cambridge Analytica continued to use data based on the OCEAN scale to benefit the Trump presidential campaign. The article did not say explicitly that the social-media data came from Facebook, but the use of the OCEAN scale suggested that Cambridge Analytica may have been using the data originally harvested from Kogan's personality quiz on Facebook.

## 1. Facebook's Public Filings

Despite the ongoing developments regarding Cambridge Analytica, Facebook represented in its 2016 Form 10-K, filed with the Securities Exchange Commission ("SEC") in February 2017, that thirdparty misuse of Facebook users' personal data was a purely hypothetical risk that could harm the company if it materialized. For example, the 10-K stated that "[a]ny failure to prevent or mitigate . . . improper access to or disclosure of our data or user data . . . could result in the loss or misuse of such data, which could harm [Facebook's] business and reputation and diminish our competitive position." The statements about the risks of improper access or disclosure appeared in the "Risk Factors" section of the 10-K, in a subsection that also discussed the risks of security breaches such as cyberattacks, hacking, and phishing

<sup>&</sup>lt;sup>6</sup> Michael Kranish, Trump's Plan for a Comeback Includes Building a 'Psychographic' Profile of Every Voter, Wash. Post (Oct. 27, 2016), https://www.washingtonpost.com/politics/trumps-plan-for-a-comeback-includes-building-a-psychographic-profile-of-every-voter/2016/10/27/9064a706-9611-11e6-9b7c-57290af48a49 story.html.

that could result in Facebook user data falling into the wrong hands.

## 2. Continued Press about Cambridge Analytica

In March 2017, The Guardian published another article about Cambridge Analytica's political activity. The article discussed how Cambridge Analytica used data derived from Facebook "likes" to train algorithms and quoted a Cambridge Analytica spokesperson's denial that the firm had access to Facebook "likes." The article also quoted a Facebook spokesperson's statement that Facebook's investigation into Cambridge Analytica had not yet uncovered any misconduct related to the firm's work on political matters, specifically the Trump presidential campaign or the Brexit Leave campaign. A Facebook spokesperson made similar comments to journalists later that month.8 Throughout 2017 and early 2018, Facebook and its executives assured Facebook users that "no one is going to get your data that shouldn't have it," that Facebook and its apps had "long been focused on giving people transparency and control," and more.

<sup>&</sup>lt;sup>7</sup> Jamie Doward, Carole Cadwalladr & Alice Gibbs, Watchdog to Launch Inquiry into Misuse of Data in Politics, Guardian (Mar. 4, 2017), https://www.theguardian.com/technology/2017/mar/04/cambridge-analytics-data-brexit-trump.

<sup>&</sup>lt;sup>8</sup> Tim Sculthorpe, Privacy Watchdog Launces a Probe into How the Leave Campaigns Used Voters' Personal Data to Win Brexit, Daily Mail (Mar. 5, 2017), https://www.dailymail.co.uk/news/article-4283102/amp/Privacy-watchdog-launches-probe-Leave-use-data.html; Mattathias Schwartz, Facebook Failed to Protect 30 Million Users From Having Their Data Harvested By Trump Campaign Affiliate, Intercept (Mar. 30, 2017), https://theintercept.com/2017/03/30/facebook-failed-to-protect-30-million-users-from-having-their-data-harvested-by-trump-campaign-affiliate/.

On March 12, 2018, The New York Times and The Guardian contacted Facebook for comment on joint articles the outlets planned to publish about Cambridge Analytica's misuse of Facebook users' data. The articles would report that Cambridge Analytica had not actually deleted the improperly collected Facebook user data from 2015. Before the articles went to print, Facebook announced on its investor relations website that it was suspending Cambridge Analytica for violating its policies by sharing Facebook users' data without the users' consent and for failing to delete the improperly collected data. Facebook explained that, in 2015, it had demanded certification that Cambridge Analytica and Kogan had destroyed the harvested user data, but that Facebook had just learned that not all the data was deleted. Soon after, The New York Times reported that Cambridge Analytica's use of Facebook users' data was "one of the largest data leaks in the social network's history." The article took the position that most people whose data was harvested had not consented to the collection, that Cambridge Analytica had used the data to benefit the Trump presidential campaign in 2016, and that "copies of the data still remain[ed] beyond Facebook's control."10

Other media outlets and government officials sprang into action. Political figures in the United States and Europe called for investigation into the Cambridge Analytica privacy scandal. Reporters

<sup>&</sup>lt;sup>9</sup> Matthew Rosenberg, Nicholas Confessore & Carole Cadwalladr, How *Trump Consultants Exploited the Facebook Data of Millions*, N.Y. Times (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

<sup>&</sup>lt;sup>10</sup> *Id*.

wrote that Facebook knew about the data breach for years and failed to disclose it to the millions of affected users. In particular, CNN observed that "[n]o one ha[d] provided an adequate explanation for why Facebook did not disclose Kogan's violation to the more than 50 million users who were affected when the company first learned about it in 2015." That same day, an article in *Seeking Alpha* warned that "[i]f Cambridge Analytica was able to acquire information on tens of millions of Facebook users so quickly and easily, and then keep the information for years without Facebook suspecting otherwise, then that shows a serious flaw in Facebook's ability to keep exclusive control over its information." <sup>12</sup>

# 3. Facebook's Stock Price Drop and Low Revenue and Profit Growth

The price of Facebook's stock declined significantly in the week that followed the Cambridge Analytica revelations. On March 19, 2018—the first trading day after the news broke—Facebook shares fell almost 7%. The next day, Facebook shares fell an additional 2.5%. After one week, Facebook's stock price had dropped nearly 18% from the price before the news about Cambridge Analytica was published, reflecting a loss of more than \$100 billion in market capitalization. At this juncture, the shareholders filed

<sup>&</sup>lt;sup>11</sup> Dylan Byers, Facebook Is Facing an Existential Crisis, CNN (Mar. 19, 2018), https://money.cnn.com/2018/03/19/technology/business/facebook-data-privacy-crisis/index.html.

<sup>&</sup>lt;sup>12</sup> Erich Reimer, *The Cambridge Analytica Mishap Is Serious for Facebook*, Seeking Alpha (Mar. 19, 2018), https://seekingalpha.com/article/4157578-cambridge-analytica-mishap-is-serious-for-facebook.

their first securities fraud complaint against Facebook.

In the aftermath, Facebook reiterated its statements that users have privacy and control over their personal data on the platform. At an April 2018 press conference, Zuckerberg stated that "you have control over everything you put on the service." Later that month, Zuckerberg issued a public post on Facebook, saying: "You've been hearing a lot about Facebook lately and how your data is being used. While this information can sometimes be confusing and technical, it's important to know that you are in control of your Facebook, what you see, what you share, and what people see about you." Zuckerberg also testified before the United States Senate that users have control over both what they share on Facebook and their personal data connected to advertisements on the platform.

On June 3, 2018, more news emerged about Facebook's privacy practices. *The New York Times* reported that Facebook had continued sharing the data of users and their Facebook friends with dozens of whitelisted third parties like Apple, Microsoft, and Samsung without the users' express consent.<sup>13</sup> The article reported that Facebook's whitelisting policy violated the company's FTC consent decree and contradicted Zuckerberg's 2014 announcement that Facebook's third-party data sharing practice had been shuttered.<sup>14</sup> An FTC investigator testified before the Parliament of the United Kingdom that, for nearly a

<sup>&</sup>lt;sup>13</sup> Gabriel J.X. Dance, Nicholas Confessore & Michael Laforgia, Facebook Gave Device Makers Deep Access to Data on Users and Friends, N.Y. Times (June 3, 2018), https://nyti.ms/3aFIMAI.

<sup>&</sup>lt;sup>14</sup> *Id*.

decade, the whitelisted apps were allowed to completely override Facebook users' privacy settings. Multiple news outlets subsequently reported that Facebook shared its users' data with foreign entities "believed to be national security risks" without the users' knowledge.

Finally, on July 25, 2018, Facebook announced unexpectedly low revenue growth, profitability, and user growth in its Q2 earnings call. Facebook stated that the disappointing revenue growth occurred because it was "putting privacy first" as well as implementing the European Union's General Data Protection Regulation ("GDPR"). Zuckerberg reported that the GDPR rollout also resulted in a decline in monthly Facebook users across Europe. The day after the earnings call, Facebook's stock price dropped nearly 19%. Analysts and investors attributed the stock drop to the company's GDPR implementation, the requisite increased security and privacy required of tech companies, and the Cambridge Analytica and whitelisting scandals.

## 4. Filing of Amended Complaints

The revelation of the Cambridge Analytica and whitelisting scandals and the two Facebook stock price drops precipitated an amended filing by the shareholders in October 2018. The shareholders amended the complaint again in November 2019 (Second Amended Complaint) and October 2020 (Third Amended Complaint). They brought claims against Facebook, Zuckerberg, Sandberg, and Wehner under Sections 10(b), 20(a), and 20A of the Securities Exchange Act of 1934 and Rule 10b-5 of the Exchange Act's implementing regulations. The shareholders allege that Facebook, through the executive defendants

or a company spokesperson, made several false or materially misleading statements between February 3, 2017, and July 25, 2018, "the class period." The challenged statements fall into three categories: (1) statements in Facebook's 2016 Form 10-K regarding the risk of improper third-party access to and disclosure of Facebook users' data; (2) statements regarding Facebook's investigation into Cambridge Analytica's 2015 misconduct; and (3) statements regarding the control Facebook users have over their data on the platform.

The district court dismissed the shareholders' First Amended Complaint and Second Amended Complaint without prejudice under Federal Rule of Civil Procedure 12(b)(6), giving the shareholders leave to amend both times. After determining that the Third Amended Complaint failed to remedy the deficiencies of the first two amended filings, the district court dismissed the shareholders' claims without leave to amend.

#### II. ANALYSIS

Although the scope of claims under Section 10(b) of the Exchange Act and Rule 10b-5 of the Exchange Act's implementing regulations is well understood and well-tread in the Ninth Circuit, these principles bear repeating so that our analysis is viewed in context.

Section 10(b) of the Exchange Act, 15 U.S.C. § 78j(b), prohibits "manipulative or deceptive" practices in connection with the purchase or sale of a security. See In re Alphabet Sec. Litig., 1 F.4th 687, 699 (9th Cir. 2021). Rule 10b-5 of the Exchange Act's implementing regulations is coextensive with Section 10(b). S.E.C. v. Zandford, 535 U.S. 813, 816 n.1

(2002). The Rule prohibits making "any untrue statement of a material fact" or omitting material facts "necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading." Glazer Cap. Mgmt., L.P. v. Forescout Techs., Inc. (Glazer II), 63 F.4th 747, 764 (9th Cir. 2023) (quoting 17 C.F.R. § 240.10b-5(b)). To state a claim under Section 10(b) and Rule 10b-5, "a plaintiff must allege: (1) a material misrepresentation or omission by the defendant ('falsity'); (2) scienter; (3) a connection between the misrepresentation or omission and the purchase or sale of a security; (4) reliance upon the misrepresentation or omission; (5) economic loss; and (6) loss causation." *Id.* (internal quotation marks omitted) (quoting In re NVIDIA Corp. Sec. Litig., 768 F.3d 1046, 1052 (9th Cir. 2014)). Claims under Sections 20(a) and 20A of the Exchange Act are derivative "and therefore require an independent violation of the Exchange Act," so the shareholders must successfully plead a Section 10(b) claim to succeed on their claims under Sections 20(a) and 20A. See Johnson v. Aljian, 490 F.3d 778, 781 (9th Cir. 2007); see also Glazer II, 63 F.4th at 765.

Complaints alleging securities fraud are also subject to heightened pleading requirements under the Private Securities Litigation Reform Act ("PSLRA") and Rule 9(b). *Glazer II*, 63 F.4th at 765. The PSLRA requires that complaints alleging falsity "specify each statement alleged to have been misleading, the reason or reasons why the statement is misleading, and, if an allegation regarding the statement or omission is made on information and belief, the complaint shall state with particularity all facts on which that belief is formed." *Id.* (quoting 15 U.S.C. § 78u-4(b)(1)). To plead scienter under the PSLRA, "the complaint must 'state with particularity facts giving rise to a strong

inference that the defendant acted with the required state of mind." Id. at 766 (quoting 15 U.S.C. § 78u-4(b)(2)(A)). When evaluating "whether the strong inference standard is met," the court first "determines whether any one of the plaintiff's allegations is alone sufficient to give rise to a strong inference of scienter." *Id.* If no individual allegation is sufficient, the court "conducts a 'holistic' review to determine whether the allegations combine to give rise to a strong inference of scienter." Id. (quoting Zucco Partners, LLC v. Digimarc Corp., 552 F.3d 981, 992 (9th Cir. 2009)). Rule 9(b) similarly requires plaintiffs to "state with particularity the circumstances constituting fraud." Id. at 765 (quoting Fed. R. Civ. P. 9(b)). Fraud allegations under Rule 9(b) "must be 'specific enough to give defendants notice of the particular misconduct which is alleged to constitute the fraud charged so that they can defend against the charge and not just deny that they have done anything wrong." Id. (quoting Bly-Magee v. California, 236 F.3d 1014, 1019 (9th Cir. 2001)).

We review de novo the dismissal of a complaint for failure to state a claim, accepting the factual allegations as true and viewing the facts "in the light most favorable" to the shareholders. *Id.* at 763. In addition to the pleading requirements of the PSLRA and Rule 9(b), Rule 8(a) requires that a complaint "contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face." *Id.* (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)). The factual allegations in the complaint must "allow[] the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* (quoting *Iqbal*, 556 U.S. at 678).

#### A. Risk Statements

The essence of the challenged risk statements is that, although Facebook knew Cambridge Analytica had improperly accessed and used Facebook users' data, Facebook represented in its 2016 Form 10-K that only the hypothetical risk of improper third-party misuse of Facebook users' data could harm Facebook's business, reputation, and competitive position. For example, Facebook's 2016 10-K warned that the "failure to prevent or mitigate security breaches and improper access to or disclosure of our data or user data could result in the loss or misuse of such data" and that if "third parties or developers fail to adopt or adhere to adequate data security practices . . . our data or our users' data may be improperly accessed, used, or disclosed." Additionally, two of the challenged statements warn that Facebook cannot provide "absolute [data] security" and that Facebook's business will suffer if the public does not perceive Facebook's products to be "useful, reliable, and trustworthy."

The district court held that the shareholders failed to plead falsity as to the risk statements, but its holding predated our decision in *In re Alphabet*. Without the benefit of our reasoning in *In re Alphabet*, the district court held that the risk statements were not actionably false because Cambridge Analytica's misconduct was public knowledge at the time the statements were made and because, while the 10-K warned of risks of harm to Facebook's business, reputation, and competitive position, the shareholders failed to allege that Cambridge Analytica's misconduct was causing such harm when the statements were made. This approach overlooks the reality of what Facebook knew.

In the securities fraud context, statements and omissions are actionably false or misleading if they "directly contradict what the defendant knew at that time," Khoja v. Orexigen Therapeutics, Inc., 899 F.3d 988, 1008 (9th Cir. 2018), or "create an impression of a state of affairs that differs in a material way from the one that actually exists," Brody v. Transitional Hosps. Corp., 280 F.3d 997, 1006 (9th Cir. 2002). The Exchange Act does not, however, "create an affirmative duty to disclose any and all material information." Glazer II, 63 F.4th at 764 (quoting Matrixx Initiatives, Inc. v. Siracusano, 563 U.S. 27, 44 (2011)). Disclosure is mandatory only when necessary to ensure that a statement made is "not misleading." *Id.* (quoting *Ma*trixx Initiatives, 563 U.S. at 44). Accordingly, if the market has already "become aware of the allegedly concealed information," the allegedly false information or material omission "would already be reflected in the stock's price' and the market 'will not be misled." Provenz v. Miller, 102 F.3d 1478, 1492 (9th Cir. 1996) (quoting In re Convergent Techs. Sec. Litig., 948 F.2d 507, 513 (9th Cir. 1991)).

Our recent decision in *In re Alphabet* is instructive. We held that falsity allegations were sufficient to survive a motion to dismiss when the complaint plausibly alleged that a company's SEC filings warned that risks "could" occur when, in fact, those risks had already materialized. *In re Alphabet*, 1 F.4th at 702–05. This juxtaposition of a "could occur" situation with the fact that the risk had materialized mirrors the allegations in the Facebook scenario. In its 2017 Form 10-K, Alphabet warned of the risk that public concerns about its privacy and security practices "could" harm its reputation and operating results. *Id.* at 694. The following year, Alphabet discovered a privacy bug that had threatened thousands of users' personal data

for three years. Id. at 695. Nonetheless, in its April and July 2018 Form 10-Q filings, Alphabet repeated the 2017 statement that public concern about its privacy and security "could" cause harm. Id. at 696. In the 10-Qs, Alphabet also stated that there had "been no material changes" to its "risk factors" since the 2017 10-K. Id. Although news of the privacy bug had not become public at the time of the 10-Qs, we reasoned that the risks of harm to Alphabet "ripened into actual harm" when Alphabet employees discovered the privacy bug and the "new risk that this discovery would become public." Id. at 703. The plaintiffs thus "plausibly allege[d] that Alphabet's warning in each Form 10-Q of risks that 'could' or 'may' occur [was] misleading to a reasonable investor when Alphabet knew that those risks had materialized." Id. at 704.

As in *In re Alphabet*, the shareholders here adequately pleaded falsity as to the statements in Facebook's 2016 10-K that represented the risk of third parties improperly accessing and using Facebook users' data as purely hypothetical. The shareholders pleaded with particularity that Facebook employees flagged Cambridge Analytica in September 2015 for potentially violating Facebook's terms, that Kogan taught Facebook in November 2015 about the dataset Cambridge Analytica had compiled, and that a Facebook executive told Cambridge Analytica in December 2015 that the firm had violated Facebook's user data policies. The shareholders also alleged that after Facebook learned in June 2016 that Cambridge Analytica lied in December 2015 about deleting the data derived from Facebook "likes," Cambridge Analytica's chief executive refused to certify that the data had actually been deleted. These allegations, if true, more than support the claim that Facebook was aware of Cambridge Analytica's misconduct before February

2017, so Facebook's statements about risk management "directly contradict[ed]" what the company knew when it filed its 2016 10-K with the SEC. *Glazer II*, 63 F.4th at 764.

Referencing Facebook's risk statements as including damage to its business, reputation, and competitive position, the dissent asserts that the risk statements in Facebook's 2016 10-K were not false or materially misleading because they "do not represent that Facebook was free from significant breaches at the time of the filing." The inadequacy of the risk statements, however, is not that Facebook did not disclose Cambridge Analytica's breach of its security practices. Instead, the problem is that Facebook represented the risk of improper access to or disclosure of Facebook user data as purely hypothetical when that exact risk had already transpired. A reasonable investor reading the 10-K would have understood the risk of a third party accessing and utilizing Facebook user data improperly to be merely conjectural.

The dissent's suggestion that the shareholders have not adequately pleaded falsity because they "have not sufficiently alleged that Facebook knew that its reputation and business were *already* harmed at the time of the filing of the 10-K" fares no better. Our case law does not require harm to have materialized for a statement to be materially misleading. Facebook's statement was plausibly materially misleading even if Facebook did not yet know the extent of the reputational harm it would suffer as a result of the breach: Because Facebook presented the prospect of a breach as purely hypothetical when it had already occurred, such a statement could be misleading even if the magnitude of the ensuing harm was still un-

known. Put differently, a company may make a materially misleading statement when it "speaks entirely of as-yet-unrealized risks" when the risks have "already come to fruition." Berson v. Applied Signal Tech., 527 F.3d 982, 987 (9th Cir. 2008); see also In re Alphabet, 1 F.4th at 702–05 (holding that risk statements in Alphabet's SEC filings were materially misleading even where Alphabet's identified harm of damage to its "business, financial condition, results of operations," and more had not yet materialized at the time of the filings). The mere fact that Facebook did not know whether its reputation was already harmed when filing the 10-K does not avoid the reality that it "create[d] an impression of a state of affairs that differ[ed] in a material way from the one that actually exist[ed]." *Brody*, 280 F.3d at 1006.

The dissent endeavors to distinguish *In re Alpha*bet by explaining that before Alphabet made SEC filings containing material misstatements, it circulated an internal memorandum detailing that there would be immediate regulatory scrutiny if the public discovered its privacy bug. While true, our holding did not rest on the internal memorandum to conclude that the statements were plausibly materially misleading; instead, we reasoned that a warning of "risks that 'could' or 'may' occur is misleading to a reasonable investor when Alphabet knew that those risks"—the privacy bug itself—"had materialized." 1 F.4th at 704. Here, as in *In re Alphabet*, it is the fact of the breach itself, rather than the anticipation of reputational or financial harm, that caused anticipatory statements to be materially misleading. The shareholders have therefore adequately pleaded that the risk statements in Facebook's 2016 10-K directly contradicted what Facebook knew at the time such that, in the dissent's words, Facebook "knew a risk had come to fruition" and "chose to bury it."

Notably, although the dissent seemingly perceives it otherwise, the extent of Cambridge Analytica's misconduct was not yet public when Facebook filed its 2016 10-K. At the time, the articles in The Guardian and The Washington Post had alerted readers that Cambridge Analytica collected data from "a massive pool of mainly unwitting US Facebook users." But the Guardian article quoted a Facebook spokesperson saying that the company would take "swift action" if Cambridge Analytica was found to have violated Facebook's policies, as well as a Ted Cruz spokesperson saying that the data was acquired legally and with the permission of Facebook users. In response to the article, Facebook stated it was "carefully investigating." Although the articles may have raised concerns about Cambridge Analytica's conduct, Facebook did not confirm before the 2016 10-K was filed that Cambridge Analytica had acted improperly or whether Facebook had taken the "swift action" promised if it learned of violations.

Indeed, Facebook's first public statement about the results of its investigation—which came in March 2017, a month after the 2016 10-K was filed—represented that no misconduct had been discovered. At the time the 10-K was filed in February 2017, the news of Cambridge Analytica's misconduct was far from "transmitted to the public with a degree of intensity and credibility sufficient to effectively counterbalance any misleading impression." *Provenz*, 102 F.3d at 1493 (citation omitted).

Importantly, and contrary to the dissent's position, the placement of the risk statements in Facebook's 2016 10-K alongside the possibilities of cyberattacks, hacking, and phishing, which the shareholders do not allege had materialized at the time of the 10-K, does not rescue Facebook's omission that the risk of improper access and disclosure had occurred from being materially misleading. A close read of the 10-K reveals that the stated hypothetical risks included the risk of a third-party developer harvesting Facebook users' data without their consent. Indeed, the title of the 10-K subsection in which the risk statements appeared included the statement that "improper access to or disclosure of" Facebook's "user data" could harm the company's reputation and business. The subsection itself stated that "[a]ny failure to prevent or mitigate security breaches and improper access to or disclosure of our data or user data could result in the loss or misuse of such data." Kogan and Cambridge Analytica's actions, while not a cyberattack, hacking, or phishing, fit the bill of Facebook failing to prevent or mitigate improper access to or disclosure of Facebook data. The risk of a third-party improperly accessing Facebook user data through methods other than hacking, phishing, or any other security breach was prominent throughout the subsection and covered the claimed misconduct of Cambridge Analytica. Collapsing the risks of improper access to and use of Facebook users' data in the same section as the risk of cyberattacks cannot rescue the risk statements from being false or materially misleading.

Additionally, Facebook's disclosure that "computer malware, viruses, social engineering (predominantly spear phishing attacks), and general hacking have become more prevalent in our industry, have occurred on our systems in the past, and will occur on our systems in the future" does not bring the risk statements within the protection of the PSLRA's safe

harbor provision for forward-looking statements. Under the safe harbor, a company is not liable for a forward-looking statement "accompanied by meaningful cautionary statements identifying important factors that could cause actual results to differ materially from those in the forward-looking statement." *Glazer II*, 63 F.4th at 767 (quoting 15 U.S.C. § 78u-5(c)(1)(A)).

Our recent decision in Weston Family Partnership v. Twitter, Inc., 29 F.4th 611 (9th Cir. 2022), provides a good illustration of statements falling within the safe harbor provision. There, Twitter disclosed its plan to improve the "stability, performance, and flexibility," of its mobile app promotion product gradually "over multiple quarters" and made clear that the company was "not there yet" in terms of its stability goals. Id. at 616. At the time, Twitter knew of a software bug affecting its mobile app promotion product but did not disclose the bug's impact. Id. We explained that Twitter's disclosure was both forward-looking and accompanied by the type of "meaningful cautionary language" necessary to invoke the safe harbor provision despite the nondisclosure of the software bug. Id. at 623.

Here, rather than making cautionary forward-looking statements, Facebook warned that it could not provide "absolute security," that it would continue to be subject to cyberattacks, and that third parties with inadequate data security practices could compromise users' data. Such broad pronouncements without meaningful acknowledgement of the known risks of improper data access and disclosure does not suffice to invoke the safe harbor provision. There is a big chasm between "absolute security" and sidestepping the reality of what Facebook allegedly knew about the compromised data.

At this stage, the shareholders adequately pleaded falsity as to the statements warning that misuse of Facebook users' data could harm Facebook's business, reputation, and competitive position and the district court erred by dismissing the complaint as to those statements. The district court, however, correctly dismissed the challenged statements regarding the risk of security breaches and the risk of the public not perceiving Facebook's products to be "useful, reliable, and trustworthy." Those statements do not relate to the misuse of Facebook user data by Cambridge Analytica, and the shareholders do not allege that those risks had materialized at the time of the 2016 10-K such that they were false or materially misleading. We leave to the district court on remand whether the shareholders can satisfy the other elements of the claims with respect to risk statements.

## B. Cambridge Analytica Investigation Statements

The challenged Cambridge Analytica investigation statements include statements made by a Facebook spokesperson to journalists in March 2017 that Facebook's internal investigation into Cambridge Analytica had "not uncovered anything that suggest[ed] wrongdoing" related to Cambridge Analytica's work on the Brexit and Trump campaigns. The district court held that the shareholders failed to plead scienter as to the Cambridge Analytica investigation statements. We agree.

To plead scienter, the shareholders "must 'state with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind." *Glazer II*, 63 F.4th at 766 (quoting 15 U.S.C. § 78u-4(b)(2)(A)). "A 'strong inference' exists 'if a reasonable person would deem the inference of scienter

cogent and at least as compelling as any opposing inference one could draw from the facts alleged." *Id.* (quoting *Tellabs, Inc. v. Makor Issues & Rts., Ltd.*, 551 U.S. 308, 324 (2007)). For obvious reasons, an actionably misleading statement must be made by a spokesperson "who has actual or apparent authority." *In re ChinaCast Educ. Corp. Sec. Litig.*, 809 F.3d 471, 476 (9th Cir. 2015) (quoting *Hollinger v. Titan Cap. Corp.*, 914 F.2d 1564, 1577 n.28 (9th Cir. 1990)). Thus, "a key inquiry" in evaluating a motion to dismiss "is whether the complaint sufficiently alleges scienter attributable to the corporation." *Id.* at 479.

Of first order is identifying "whether the complaint adequately alleged that the maker omitted material information knowingly, intentionally, or with deliberate recklessness." *In re Alphabet*, 1 F.4th at 705. "Deliberate recklessness is a higher standard than mere recklessness and requires more than a motive to commit fraud." *Glazer II*, 63 F.4th at 765 (quoting *Schueneman v. Arena Pharms., Inc.*, 840 F.3d 698, 705 (9th Cir. 2016)). Instead, "deliberate recklessness" involves "an *extreme* departure from the standards of ordinary care" that presents "a danger of misleading buyers or sellers" that "is so *obvious*" that the spokesperson "must have been aware of it." *Id.* (quoting *Schueneman*, 840 F.3d at 705).

Simply raising an inference that a company's executive "should have" discovered misconduct, not that the executive actually knew of misconduct, is insufficient "to meet the stringent scienter pleading requirements of the PSLRA." Glazer Cap. Mgmt., LP v. Magistri (Glazer I), 549 F.3d 736, 748–49 (9th Cir. 2008). In Glazer I, the defendant CEO signed a merger agreement before announcing months later that an investigation early in the merger-related due diligence

process uncovered possible Foreign Corrupt Practices Act violations. *Id.* at 740. The plaintiffs argued that because the violations were discovered early, information about the violations "must have been readily available and therefore known to [the CEO] when he signed the merger agreement." *Id.* at 748. We held that the CEO learning of the violations shortly after due diligence was not enough "to create a strong inference of scienter." *Id.* The only strong inference to be drawn was that the CEO *should* have known of the possible violations, not that he actually knew about them, which was insufficient to plead scienter. *Id.* 

As in Glazer I, the shareholders pleaded only that the Facebook spokesperson should have known that Facebook's investigation into Cambridge Analytica had uncovered misconduct, not that the spokesperson actually knew of any misconduct or even that there was a strong inference of an "intent to deceive, manipulate, or defraud." Id. at 742 (quoting Ernst & Ernst v. Hochfelder, 425 U.S. 185, 193 n.12 (1976)). The mere reference by an unidentified spokesperson to Facebook's investigation is insufficient to show that the spokesperson knowingly or intentionally made false or materially misleading statements about the investigation. The shareholders' allegations do not rise to the level of showing that it was "so obvious" that Facebook's investigation had uncovered misconduct related to Cambridge Analytica's political work that the spokesperson "must have been aware of it." Glazer II, 63 F.4th at 765 (citation omitted).

Although one might reasonably expect the spokesperson to have verified the accuracy of the statements before making them, securities fraud actions are not tort actions, and "[m]ere negligence—even headscratching mistakes—does not amount to fraud." Prodanova v. H.C. Wainwright & Co., 993 F.3d 1097, 1103 (9th Cir. 2021). Nothing in the complaint suggests that the Cambridge Analytica investigation statements involved an extreme departure from the standards of ordinary care, and the shareholders thus fall short of raising a strong inference that the spokesperson acted with the necessary malintent. In light of the absence of scienter, we need not assess the alleged falsity of the statements. We affirm the district court's dismissal of the allegations and agree that the shareholders failed to plead scienter as to the Cambridge Analytica investigation statements.

#### C. User Control Statements

Throughout the class period, Facebook made several statements about users' control over their personal data. The statements assured Facebook users that they had control over their information and content on Facebook and that Facebook's priorities of transparency and user control aligned with the GDPR framework. The following Facebook statements are illustrative: "People can control the audience for their posts and the apps that can receive their data," "[e]very person gets to control who gets to see their content," and "[w]e respected the privacy settings that people had in place." The shareholders assert that Facebook's stock price dropped after reporting on the Cambridge Analytica scandal in March 2018 and Facebook's whitelisting policy in June 2018 revealed the falsity of Facebook's statements about users' control over their data. They allege that the stock price drops caused them to suffer economic loss.

Pleading loss causation requires a showing that the "share price fell significantly after the truth became known." *In re Oracle Corp. Sec. Litig.*, 627 F.3d 376, 392 (9th Cir. 2010) (quoting *Dura Pharms.*, *Inc.* 

v. Broudo, 544 U.S. 336, 347 (2005)). "[L]oss causation is simply a variant of proximate cause." Lloyd v. CVB Fin. Corp., 811 F.3d 1200, 1210 (9th Cir. 2016). The shareholders must show that Facebook's "misstatement, as opposed to some other fact, foreseeably caused the plaintiff's loss." Id. The shareholders' "burden of pleading loss causation is typically satisfied by allegations that the defendant revealed the truth through 'corrective disclosures' which 'caused the company's stock price to drop and investors to lose money." Id. at 1209 (quoting Halliburton Co. v. Erica P. John Fund, Inc., 573 U.S. 258, 264 (2014)).

"At the pleading stage, the plaintiff's task is to allege with particularity facts 'plausibly suggesting' that [such] showings can be made." In re BofI Holding, Inc., Sec. Litig., 977 F.3d 781, 791 (9th Cir. 2020) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 557 (2007)); see also Or. Pub. Emps. Ret. Fund v. Apollo *Grp.*, *Inc.*, 774 F.3d 598, 605 (9th Cir. 2014) ("Rule 9(b) applies to all elements of a securities fraud action, including loss causation."); accord Katyle v. Penn Nat'l Gaming, Inc., 637 F.3d 462, 471 (4th Cir. 2011). "So long as the complaint alleges facts that, if taken as true, plausibly establish loss causation, a Rule 12(b)(6) dismissal is inappropriate." Grigsby v. BofI Holding, Inc., 979 F.3d 1198, 1206 (9th Cir. 2020) (quoting In re Gilead Sci. Sec. Litig., 536 F.3d 1049, 1057 (9th Cir. 2008)).

As an initial matter, the district court correctly held that the shareholders failed to plead sufficiently that Facebook's statements about the company's commitment to transparency and control in line with the GDPR framework violated Section 10(b) and Rule 10b-5. As Facebook notes, those statements "merely

reiterated Facebook's ongoing commitment to 'transparency and control" rather than assuring users they controlled their Facebook data, and thus were not false when they were made. Further, the June 2018 whitelisting revelation, which was unaccompanied by a stock price drop, is not actionable. *See Lloyd*, 811 F.3d at 1210. We affirm the dismissal of the statements related to Facebook's goals of transparency and control, and the June 2018 whitelisting revelation as a standalone claim. However, we reverse the dismissal as to other statements related to the stock drops.

## 1. March 2018 Stock Price Drop

Most of the challenged user control statements occurred after the March 16, 2018, revelation about Cambridge Analytica and thus cannot be pegged to the March 2018 stock price drop. However, the user control statements that preceded the revelation are relevant here, and the shareholders adequately pleaded loss causation as to the statements assuring users that they control their content and information on the platform.

The shareholders adequately pleaded that the March 2018 revelation about Cambridge Analytica was the first time Facebook investors were alerted that Facebook users did not have complete control over their own data. As previously discussed, the 2015 and 2016 articles in *The Guardian* and *The Washington Post* did not reveal that Cambridge Analytica had misused Facebook users' data. Facebook's public response to the *Guardian* article in 2015 was that it was "carefully investigating" Cambridge Analytica.

The shareholders also adequately allege that Facebook did not make public statements about the Cambridge Analytica issue between 2015 and 2018.

Before the March 2018 news broke, reasonable investors would not have known that Cambridge Analytica had improperly accessed Facebook users' data such that users did not have control over their personal information on the platform. In the week that followed the revelation, Facebook's stock dropped nearly 18%, representing a loss of over \$100 billion in market capitalization and plausibly causing economic loss for the shareholders.

The Cambridge Analytica revelation thus satisfies the pleading criteria for a corrective disclosure, which requires allegations that "the defendant's fraud was 'revealed to the market and caused the resulting loss[]." Grigsby, 979 F.3d at 1205 (emphasis omitted) (quoting Loos v. Immersion Corp., 762 F.3d 880, 887 (9th Cir. 2014)). A disclosure is not corrective if the information comes entirely from public sources "of which the stock market was presumed to be aware." Id. (quoting Loos, 762 F.3d at 889). Here, because the 2015 and 2016 articles about Cambridge Analytica did not provide investors the necessary information to learn that Facebook users did not control their data. the shareholders adequately alleged that the March 2018 revelation was a corrective disclosure as to Facebook's statements that users control their data on the platform. We reverse the district court's dismissal of Facebook's statements about users controlling their own Facebook data that preceded the March 16, 2018, revelation.

# 2. July 2018 Stock Price Drop

The July 2018 drop occurred immediately after Facebook's disappointing earnings report and was tied to approximately \$100 billion of shareholder value loss. At the time, it was the largest single-day stock price drop in U.S. history. The question is

whether the shareholders adequately pleaded loss causation as to Facebook's user control statements predating the March 16, 2018, Cambridge Analytica revelation and the June 3, 2018, whitelisting revelation, even though the stock drop did not occur until July 25, 2018.

Because loss causation requires that the defendant's misstatement, rather than some other fact, fore-seeably caused the plaintiff's loss, establishing loss causation requires more than "an earnings miss" or the market's reaction to a company's "poor financial health generally." *In re Oracle*, 627 F.3d at 392. Simply pleading "that the market reacted to the purported 'impact' of the alleged fraud—the earnings miss—rather than to the fraudulent acts themselves" is not sufficient. *Id*.

Illustrative of a disconnect between earnings and causation is In re Oracle, where the shareholders argued that Oracle's misstatements regarding the "quality and success" of its Suite 11i product, rather than its struggling financial health, caused the company's stock price to drop. Id. at 392–93. The shareholders posited that because the stock price drop occurred immediately after the truth about Suite 11i became public, the revelation of the truth must have caused the price drop. Id. In affirming summary judgment for Oracle, we explained that the "overwhelming evidence produced during discovery indicate[d] the market understood Oracle's earnings miss to be a result of several deals lost in the final weeks of the quarter due to customer concern over the declining economy," not the alleged Suite 11i fraud. Id. at 393.

Another wrinkle here is whether loss causation allegations can survive a motion to dismiss even when the stock price drop did not immediately follow the

revelation of the misstatement. In *In re Gilead*, the market learned in August 2003 that Gilead had aggressively marketed a drug by claiming that the company had "carefully complied with federal and state regulations" when, in fact, a warning letter from the Food and Drug Administration had informed Gilead that its marketing claims were unlawful. 536 F.3d at 1051. Gilead's stock price did not drop until October 2003, following a press release revealing "less-thanexpected revenues." Id. at 1054, 1058. Despite the time gap between the revelation and the stock price drop, the shareholders claimed that Gilead's misrepresentations caused its stock price to inflate, and the subsequent disappointing revenue performance and stock price drop sufficed to plead loss causation. *Id.* at 1056.

Acknowledging the time gap, we held that the shareholders adequately pleaded loss causation and reiterated that there is no "bright-line rule requiring an immediate market reaction" after a revelation because "[t]he market is subject to distortions that prevent the ideal of a free and open public market from occurring." Id. at 1057–58 (alteration in original) (citation omitted). Accordingly, the shareholders plausibly alleged that Gilead's stock price drop occurred immediately after the company revealed its disappointing revenue numbers, and the drop was caused by lower demand resulting from the warning letters. Id. As we explained, it was reasonable for the public to fail to appreciate the significance of the warning letters until learning of Gilead's disappointing revenue posting. Id. Because the shareholders pleaded sufficient facts to raise a reasonable expectation that discovery would reveal evidence of the warning letter's "effect on demand," the loss causation claim survived Gilead's motion to dismiss. Id. at 1058.

For Facebook's July 2018 stock price drop to be actionable, it must be because Facebook's earnings report revealed new information to the market; specifically, that Facebook's Q2 earnings call in July 2018 allowed the public to "appreciate [the] significance" of the Cambridge Analytica and whitelisting scandals. *Id.* The disappointing Q2 earnings performance alone cannot satisfy the shareholders' burden of pleading loss causation.

Here, as in *In re Gilead*, the shareholders adequately pleaded that the Cambridge Analytica and whitelisting revelations, not any other factor, caused the July 2018 stock price drop. Although the stock drop occurred nearly two months after the whitelisting revelation, the shareholders allege with particularity that the drop was caused by "dramatically lowered user engagement, substantially decreased advertising revenue and earnings, and reduced growth expectations going forward" on account of the Cambridge Analytica and whitelisting scandals. The shareholders further detail how the GDPR rollout had little impact on the July 2018 earnings report, and how investors and market analysts explicitly connected the revenue drop to the scandals. These allegations suffice to plausibly plead "a causal relationship" between the Cambridge Analytica and whitelisting revelations and the dramatic drop in Facebook's stock price. Id. at 1057; see also Grigsby, 979 F.3d at 1206 (emphasizing that while "plaintiffs must satisfy the particularity standard of Rule 9(b)," that standard "does not require that the causation inference be *more* than 'plausible"). We emphasize that this case is at the very early motion to dismiss stage, and that discovery and further proceedings are necessary to illuminate the issues surrounding loss causation.

Our dissenting colleague would affirm the district court's dismissal of the user control statements as they relate to the Cambridge Analytica revelation. Stated differently, the dissent would hold that only the July 2018 stock price drop was actionable, and only as to the whitelisting revelation, not the Cambridge Analytica revelation.

In support, the dissent contends that the 2018 "Cambridge Analytica disclosures did not make the user control statements materially false," because "Cambridge Analytica's lies to Facebook and its continued violation of Facebook's privacy policies do not mean that Facebook's privacy protections do not actually exist." But the question is not whether and when Cambridge Analytica lied to Facebook, but whether and when Facebook learned of Cambridge Analytica's deception. It is true that in January 2016, Cambridge Analytica agreed to delete the personality score data it harvested from Facebook. But recall that the shareholders pleaded that Facebook had reason to know in June 2016—only five months later—that Cambridge Analytica had received much more information from Facebook than just the personality score data and that Cambridge Analytica was still using a model based on the data in violation of Facebook's policies. The shareholders further allege that when Facebook found out, it tried to require Cambridge Analytica's CEO to certify that all data harvested from the personality guiz was deleted, but the CEO refused to do so. Thus, the shareholders pleaded with particularity that Facebook knew Cambridge Analytica did not delete all the data it had improperly accessed.

We agree with the dissent that "a supposed bad actor violating Facebook's privacy controls to improperly access user data doesn't make the company's statements about its policies misleading." But labeling Cambridge Analytica as a "bad actor" is not the issue. It was not Cambridge Analytica's deception that made Facebook's user control statements misleading. Rather, it was that Facebook knew Cambridge Analytica retained access to improperly collected user data after Cambridge Analytica certified that it had deleted the personality score data, and Facebook nonetheless falsely represented to users that they had control over their data on the platform. The shareholders adequately pleaded loss causation as to the stock price drops that occurred after the Cambridge Analytica revelation in March and July 2018. Accordingly, we reverse the district court's dismissal of Facebook's statements regarding data control that predated the June 3, 2018, whitelisting revelation.

### III. CONCLUSION

We affirm in part and reverse in part as to dismissal based on the risk statements and user control statements, and we affirm as to dismissal based on the Cambridge Analytica investigation statements. Specifically, we affirm the dismissal of the statements in  $\P 503-05$ , 530, 533, and 537-38 of the Third Amended Complaint, reverse the district court's dismissal of the statements in  $\P 501-02$ , 507-14, 519, and 525, and remand for further proceedings. Each party shall bear its own costs.

AFFIRMED IN PART, REVERSED IN PART, AND REMANDED IN PART.

BUMATAY, J., concurring in part and dissenting in part:

At issue here are three general categories of alleged false statements: (1) statements about Facebook's risk factors, (2) statements about Facebook's investigation of Cambridge Analytica, and (3) statements about Facebook users' control over their data. I join the majority in holding that the plaintiff Shareholders failed to sufficiently allege a falsity in the second category—Facebook's Cambridge Analytica investigation statements. I also join the majority in holding that Shareholders *did* allege a falsity and loss from the third category of user control statements—but only as those statements relate to Facebook's practice of "whitelisting."

So I disagree with the majority on two fundamental points. First, Shareholders failed to sufficiently allege that Facebook's risk factor statements in its public filings were fraudulent. Second, Shareholders didn't show that Facebook's user control statements were false based on the Cambridge Analytica revelations. I briefly set out my disagreement below.

I.

## **Risk Factor Statements**

Federal securities law creates no "affirmative duty to disclose any and all material information." *Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. 27, 44 (2011). Rather, companies must disclose information "only when necessary 'to make . . . statements made, in light of the circumstances under which they were made, not misleading." *Id.* (quoting 17 CFR § 240.10b–5(b)). Thus, companies "can control what they have to disclose . . . by controlling what they say to the market." *Id.* at 45.

Indeed, companies have no "obligation to offer an instantaneous update of every internal" or "fleeting" development. Weston Fam. P'ship LLLP v. Twitter, Inc., 29 F.4th 611, 620 (9th Cir. 2022). Instead, a "company must disclose a negative internal development only if its omission would make other statements materially misleading." Id. Put differently, statements and omissions are actionable only if they "directly contradict what the defendant knew at that time," Khoja v. Orexigen Therapeutics, Inc., 899 F.3d 988, 1008 (9th Cir. 2018), or "create an impression of a state of affairs that differs in a material way from the one that actually exists," Brody v. Transitional Hosps. Corp., 280 F.3d 997, 1006 (9th Cir. 2002). In assessing this question, we look to the "total mix" of information available to the reasonable investor and whether the alleged misstatement "significantly altered" the decisionmaking of the reasonable investor. Retail Wholesale & Dep't Store Union Loc. 338 Ret. Fund v. Hewlett-Packard Co., 845 F.3d 1268, 1274 (9th Cir. 2017) (simplified); see also In re Syntex Corp. Sec. Litig., 95 F.3d 922, 929 (9th Cir. 1996) (requiring evaluation of the "statement in full and in context at the time it was made").

Shareholders' allegations stem from Facebook's 2016 SEC Form 10-K "Risk Factors" statements, dated February 3, 2017. Facebook made these statements in the context of the following bolded headline:

"Security breaches and improper access to or disclosure of our data or user data, or other hacking and phishing attacks on our systems, could harm our reputation and adversely affect our business."

Under that header, Facebook gave these warnings:

- "Any failure to prevent or mitigate security breaches and improper access to or disclosure of our data or user data could result in the loss or misuse of such data, which could harm our business and reputation and diminish our competitive position."
- "We provide limited information to ... third parties based on the scope of services provided to us. However, if these third parties or developers fail to adopt or adhere to adequate data security practices ... our data or our users' data may be improperly accessed, used, or disclosed."

Shareholders argue—and the majority agrees—that all three of these statements are misleading because, by February 2017, Facebook already knew that Cambridge Analytica had gained improper access to the data of tens of millions of Facebook users. According to the majority, this means that the statements directly contradicted what the company knew when it filed its 10-K.

There's a problem with this analysis. Even if Facebook knew about the full extent of the so-called Cambridge Analytica scandal at this point, none of this makes the risk factor statements false. Recall the facts of the scandal. In 2015, Facebook became aware that Cambridge Analytica—through a consulting academic—had developed a personality quiz that harvested data from more than thirty million Facebook users, often without the users' consent. This quiz gave Cambridge Analytica access to Facebook users' name, gender, location, birthdate, "likes," and "friends," which made it possible to develop an algorithm to sort

Facebook users according to personality traits. Cambridge Analytica then allegedly used that algorithm to help political campaigns.

Regardless of the severity of Cambridge Analytica's alleged misconduct, a careful reading of the 10-K statements shows that these risk factor statements warn about harm to Facebook's "business" and "reputation" that "could" materialize based on improper access to Facebook users' data—not about the occurrence or non-occurrence of data breaches. How do we know that? Well, the statements say so. The first and second statements expressly advise that improper breaches "could harm" Facebook's "business" and "reputation."

And although the third statement does not expressly mention business and reputational harm, we know that is its focus for two reasons. First, Facebook reported the statement under the bolded section about breaches and improper actions "could harm [Facebook's] reputation and adversely affect our business." Second, the very next sentence places that statement into more context: "Affected users or government authorities could initiate legal or regulatory actions against us in connection with any security breaches or improper disclosure of data, which could cause us to incur significant expense and liability or result in orders or consent decrees forcing us to modify our business practices."

Taken together, Facebook's risk factor statements warn about harm to its "reputation" and "business" that *may* come to light if the public or the government learns about improper access to its data. These statements do not represent that Facebook was free from significant breaches at the time of the filing. And if a reasonable investor thought so based on Facebook's

10-K statements, that "reasonable" investor wasn't acting so reasonably. Indeed, within the same section, Facebook warned that "computer malware, viruses, social engineering (predominantly spear phishing attacks), and general hacking have become more prevalent in our industry, have occurred on our systems in the past, and will occur on our systems in the future." Facebook expressly advised that it experienced previous attempts to swipe its data and that it would continue to face such threats. Beyond Facebook's own statements, much about the Cambridge Analytica scandal was already public. In a December 2015 article, The Guardian reported that Cambridge Analytica had harvested data from "tens of millions" of Facebook users "without their permission." These are the same facts Shareholders use to claim Facebook deceived the public with more than two years later.

So, on their face, none of the 10-K risk factor statements are false or misleading. The statements advise that improper access to data *could* harm Facebook's reputation and business. And Shareholders have not sufficiently alleged that Facebook knew its reputation and business were *already* harmed at the time of the filing of the 10-K. Nor do they allege that Facebook was aware of government entities or users launching regulatory or legal actions based on the Cambridge Analytica scandal in February 2017.

While acknowledging these shortcomings in the Shareholders' complaint, the majority takes the sur-

<sup>&</sup>lt;sup>1</sup> See Harry Davies, Ted Cruz Using Firm that Harvested Data on Millions of Unwitting Facebook Users, The Guardian (Dec. 11, 2015), https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data.

prisingly broad view that it's irrelevant that "Facebook did not know whether its reputation was ... harmed" at the time of the 10-K filing. Maj. Op. 24. The majority instead asserts that it's enough that a breach had occurred, never mind whether the breach led to a discernible effect on Facebook's reputation or business at the time. *Id*. The majority goes so far as to say that a fraud occurs even if the harm caused by the breach was completely "unknown" to Facebook. Id. But if it was "unknown" whether the breach led to reputational or business harm, it's hard to see how the risk factor statements were untrue. Stating that harm could result from a breach is not falsified by some "unknown" possibility of harm from a breach. In other words. Facebook's risk factor statements could not "directly contradict what the defendant knew at that time" if any harm was unknown to Facebook at the time. Khoja, 899 F.3d at 1008.2

And *In re Alphabet, Inc. Securities Litigation*, 1 F.4th 687 (9th Cir. 2021), doesn't transform every risk statement into a false or misleading statement if a risk later comes to fruition. Nor does it create a new requirement that a company disclose every bad thing

<sup>&</sup>lt;sup>2</sup> Given the majority's analysis of these statements, it's difficult to see how Shareholders can ever satisfy the scienter requirement. Indeed, "[a] complaint will survive . . . only if a reasonable person would deem the inference of scienter cogent and at least as compelling as any opposing inference one could draw from the facts alleged." *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 324 (2007). Such a strong inference requires an "intent to deceive, manipulate, or defraud," or "deliberate recklessness"—which is "an *extreme* departure from the standards of ordinary care." *Schueneman v. Arena Pharmaceuticals, Inc.*, 840 F.3d 698, 705 (9th Cir. 2016). If the harm from Cambridge Analytica's breach was unknown at the time of the filing of the 10-K, it's doubtful this standard can be met.

that ever happened to it. In that case, Alphabet stated in two quarterly disclosure forms that certain risks "could adversely affect our business, financial condition, [and] results of operations," but that "[t]here have been no material changes to our risk factors since our [last] Annual Report on Form 10-K." 1 F.4th at 696 (simplified). What Alphabet didn't disclose is that, before the reports came out, its internal Google investigators had discovered a software glitch in one of its programs that allowed third parties to collect users' private data. Id. at 695. Google's legal and policy staff quickly recognized the problem and warned in an internal memorandum that these security issues would likely trigger an immediate regulatory response and cause its senior executives to testify before Congress. Id. at 696. When news inevitably broke six months later, Alphabet's shares plummeted in value and, sure enough, there were calls for government investigation. Id. at 697. We concluded that "[r]isk disclosures that speak entirely of as-yet-unrealized risks and contingencies and do not alert the reader that some of these risks may already have come to fruition can mislead reasonable investors." Id. at 703 (simplified). In Alphabet's case, the "warning in each [quarterly report] of risks that 'could' or 'may' occur [was] misleading to a reasonable investor [because] Alphabet knew that those risks had materialized." Id. at 704.

Contrary to the majority's assertion, this case is nothing like *Alphabet*. In *Alphabet*, the company knew a risk had come to fruition—set out as clear as day in an internal company memo—that a data bug would cause it greater regulatory scrutiny. *Id.* at 696. Rather than disclose its assessment, Alphabet chose to bury it and even stated that no material changes existed in its risk factors. *Id.* at 696–97, 703. Here,

Facebook might have known of breaches of its data even potentially serious breaches—when it gave its risk statements, but Shareholders don't allege that Facebook knew that those breaches would lead to immediate harm to its business or reputation. As the majority concedes, the harm from Cambridge Analytica's breach of Facebook's policies was "unknown" at the time of the 10-K filing. See Maj. Op. 24. Nor did Facebook lull investors into complacency by suggesting that nothing had changed on its risks front. These facts make all the difference here. Cf. Weston, 29 F.4th at 621 (dismissing fraud claims alleging that Twitter's risk warning statement—that its "product and services may contain undetected software errors, which could harm our business and operating results"—was misleading because the risk had materialized by then).

Because Facebook did not present false or misleading risk statements, and *Alphabet* did not modify a common-sense understanding of truthfulness and disclosure, we should have affirmed the dismissal of this claim.

# II.

### **User Control Statements**

The next category of alleged falsehoods concerns Facebook's representations that users control their data and information. During the relevant period for this lawsuit, Facebook and its executives made various statements emphasizing users' control over the data they shared with Facebook, such as—

"You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings." Facebook's

Statement of Rights and Responsibilities web page, ~ January 30, 2015 to May 25, 2018.

- "[W]hen you share on Facebook you need to know No one is going to get your data that shouldn't have it. That we're not going to make money in ways that you would feel uncomfortable with off your data. And that you're controlling who you share with Privacy for us is making sure that you feel secure, sharing on Facebook." Sheryl Sandberg, *Axios* interview, October 12, 2017.
- "Our apps have long been focused on giving people transparency and control...."
   Sheryl Sandberg, Facebook Gather Conference, January 23, 2018.

#### A.

Shareholders have adequately shown that these statements were misleading based on the allegation that Facebook "whitelisted" third parties. According to the Shareholders, at the same time these statements were made, Facebook continued to allow certain "whitelisted" third parties, mostly app developers and device manufacturers, to continue to access data against a user's wishes. Shareholders allege that Facebook overrode user privacy settings to allow these third parties access to the data of, not only the Facebook user, but that of the user's friends as well. In fact, Facebook paid the Federal Trade Commission \$5 billion to settle charges stemming from the "whitelisting" allegations.

These facts are enough to plead that the statements were false—the only question is whether the

statements caused Shareholders any loss. See Grigsby v. BofI Holding, Inc., 979 F.3d 1198, 1204 (9th Cir. 2020) (explaining that "investors must demonstrate that the defendant's deceptive conduct caused their claimed economic loss") (simplified). Facebook's "whitelisting" program became public on June 3, 2018, when the New York Times reported that Facebook shared users' and their friends' data with multiple "whitelisted" companies. When it comes to false statements, a plaintiff can usually show loss causation by pointing to an immediate stock drop after the falsity was uncovered. Id. at 1205 ("A plaintiff can satisfy the loss-causation pleading burden by alleging that a corrective disclosure revealed the truth of a defendant's misrepresentation and thereby caused the company's stock price to drop and investors to lose money.") (simplified). The wrinkle here is that Facebook's stock didn't drop immediately after the whitelisting became public. It wasn't until several weeks later—July 26, 2018, the day after Facebook announced slower growth than expected—that Facebook's stock dropped by almost 19%. Facebook contends that this temporal gap proves that its misleading user control statements didn't cause Shareholders any loss.

But sometimes it takes time for the full scope of a loss from a misrepresentation to materialize. As *In re Gilead Sciences Securities Litigation*, 536 F.3d 1049, 1058 (9th Cir. 2008) recognized, a "limited temporal gap between the time a misrepresentation is publicly revealed and the subsequent decline in stock value does not render a plaintiff's theory of loss causation per se implausible." Indeed, in that case, three months had passed between the disclosure of Gilead's alleged deceptive marketing practices and the stock drop after Gilead missed revenue targets. *Id.* at 1057–58. De-

spite this gap, we concluded the plaintiffs had plausibly alleged that the less-than-expected revenue was caused by lower end-user demand, which, in turn, was caused by disclosing the company's deceptive marketing. *Id.* at 1058. Thus, an "immediate market reaction" is not necessary when the market might "fail[] to appreciate [the] significance" of a disclosure right away. *Id.* at 1057–58.

So, we shouldn't be too quick to dismiss a claim based on a delay in the manifestation of loss. In my view, it's plausible that the whitelisting revelation made on June 18 caused user engagement and advertising revenue to diminish, which contributed to the lower earnings announced on July 25 and the immediate stock drop. Facebook counters that the European Union's new privacy regulations—not the whitelisting revelation—caused the lower July 25 earnings. That might be right. But, at the very least, Shareholders deserve some discovery to prove their theory of loss causation.

## В.

But the analysis of the user control statement must be different when it comes to the Cambridge Analytica scandal. Shareholders allege—and the majority agrees—that new revelations about Cambridge Analytica from March 2018 also proved Facebook's user control statements were false. As a reminder, in late 2015, Facebook discovered that Cambridge Analytica obtained personality score data harvested from Facebook data and demanded that Cambridge Analytica delete all such data. In response, Cambridge Analytica certified to Facebook that it would delete the data. On March 16, 2018, Facebook announced that it had received reports from the media that Cambridge

Analytica did not destroy the data and that it was suspending Cambridge Analytica from the platform. News reports then confirmed that Cambridge Analytica continued to possess and use harvested data from Facebook. Within a week of these disclosures, Facebook's shares dropped nearly 18%. Shareholders contend that these revelations prove the falsity of Facebook's user control statements.

These Cambridge Analytica disclosures did not make the user control statements materially false. To prevail, Shareholders must show that the Facebook user control statements "affirmatively create[d] an impression of a state of affairs that differ[ed] in a material way from the one that actually exist[ed]." *Brody*, 280 F.3d at 1006. But Cambridge Analytica's lies to Facebook and its continued violation of Facebook's privacy policies do not mean that Facebook's privacy protections do not actually exist. Aside from the whitelisting issue described above, Facebook seemingly described its privacy policies accurately. Cambridge Analytica's violation of those policies doesn't falsify them.

Imagine a bank. Say that the bank announces a range of security measures to protect its customers' money. Then consider if a bank robber defeats those measures, breaks in, and ultimately steals a bag of cash. Would anyone say that the bank lied about its security measures? Clearly, no. Here, a supposed bad actor violating Facebook's privacy controls to improperly access user data doesn't make the company's statements about its policies misleading.

What makes our ruling all the more odd is that much of the Cambridge Analytica scandal was already public by the time of the user control statements. The first article about it dropped in 2015. So it's hard to see how this new "revelation" added to the "total mix" of information available to Shareholders or "significantly altered" their decision-making. See Retail Wholesale & Dep't Store Union Loc. 338 Ret. Fund, 845 F.3d at 1274. We thus should have limited Facebook's liability for the user control statements to the "whitelisting" allegations.

# III.

For these reasons, I respectfully dissent from Part II.A of the majority opinion, from Part II.C as it relates to Cambridge Analytica, and from Part III.

# **APPENDIX B**

# UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

In re: FACEBOOK, INC. SECURITIES LITIGATION,

AMALGAMATED BANK, Lead Plaintiff; PUBLIC EM-PLOYEES' RETIREMENT SYSTEM OF MISSISSIPPI; JAMES KACOURIS, individually and on behalf of all others similarly situated,

Plaintiffs-Appellants,

v.

FACEBOOK, INC.; MARK ZUCKERBERG; SHERYL SANDBERG; DAVID M. WEHNER,

Defendants-Appellees.

No. 22-15077 D.C. No. 5:18-cv-01725-EJD

**OPINION** 

Appeal from the United States District Court for the Northern District of California Edward J. Davila, District Judge, Presiding

> Argued and Submitted February 8, 2023 San Francisco, California

> > Filed October 18, 2023

Before: M. Margaret McKeown, Jay S. Bybee, and Patrick J. Bumatay, Circuit Judges.

Opinion by Judge McKeown; Partial Concurrence and Partial Dissent by Judge Bumatay

## **SUMMARY**\*

# **Securities Exchange Act of 1934**

The panel affirmed in part and reversed in part the district court's judgment dismissing under Fed. R. Civ. P. 12(b)(6) for failure to state a claim a Third Amended Complaint in which purchasers of Facebook common stock between February 3, 2017, and July 25, 2018, ("the shareholders") allege that Facebook and its executives violated Sections 10(b), 20(a), and 20A of the Securities Exchange Act of 1934 and Rule 10b-5 of the Exchange Act's implementing regulations by making materially misleading statements and omissions regarding (1) the risk of improper access to Facebook users' data, (2) Facebook's internal investigation into British political consulting firm Cambridge Analytica, and (3) the control Facebook users have over their data.

In March 2018, news broke that Cambridge Analytica improperly harvested personal data from millions of unwitting Facebook users and retained copies of the data beyond Facebook's control. In the months that followed, the public learned that Facebook had known of Cambridge Analytica's misconduct for over two years and failed to inform affected users, and that Facebook surreptitiously allowed certain whitelisted third-party apps to access users' Facebook friend data without the users' friends' consent. Facebook and its executives made various statements before and after the news announcements assuring users that they fully controlled their data on Facebook and that no

<sup>\*</sup> This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

third party would access the data without their consent. In the wake of the Cambridge Analytica and whitelisting scandals, Facebook's stock price suffered two significant drops totaling more than \$200 billion in market capitalization.

The panel considered whether, under the heightened standard of the Private Securities Litigation Reform Act, the shareholders (1) adequately pleaded falsity as to the challenged risk statements, (2) adequately pleaded scienter as to the Cambridge Analytica investigation statements, and (3) adequately pleaded loss causation as to the user control statements.

First, the panel held that the shareholders adequately pleaded falsity as to the statements warning that misuse of Facebook users' data could harm Facebook's business, reputation, and competitive position and the district court erred by dismissing the complaint as to those statements. The panel wrote that, as in In re Alphabet Sec. Litig., 1 F.4th 687 (9th Cir. 2021), the shareholders here adequately pleaded falsity as to statements in a 2016 Form 10-K filing with the SEC in which Facebook represented the risk of third parties improperly accessing and using Facebook users' data as purely hypothetical. The panel held that the district court correctly dismissed the challenged statements regarding the risk of security breaches and the risk of the public not perceiving Facebook's products to be "useful, reliable, and trustworthy"; those statements do not relate to the misuse of Facebook user data by Cambridge Analytica, and the shareholders do not allege that those risks had materialized at the time of the 2016 10-K such that they were false or materially misleading. The panel left to the district court on remand whether the shareholders

can satisfy the other elements of the claims with respect to risk statements.

Second, the panel agreed with the district court that the shareholders failed to plead scienter as to Cambridge Analytica investigation statements, including ones made by a Facebook spokesperson to journalists in March 2017 that Facebook's internal investigation into Cambridge Analytica had "not uncovered anything that suggest[ed] wrongdoing" related to Cambridge Analytica's work on the Brexit and Trump campaigns. The panel wrote that the shareholders pleaded only that the spokesperson should have known that Facebook's investigation had uncovered misconduct, not that the spokesperson actually knew of any misconduct or even that there was a strong inference of an "intent to deceive, manipulate, or defraud."

Third, as to Facebook's user control statements:

The panel affirmed the dismissal as to statements related to Facebook's goals of transparency and control—statements that were not false when they were made. The panel also affirmed the dismissal of a standalone claim relating to the June 2018 whitelisting revelation, given that the revelation was unaccompanied by a stock price drop.

The panel held that the shareholders adequately pleaded loss causation as to Facebook's statements—made before the March 16, 2018, stock price drop—assuring users that they control their content and information on the platform. The panel wrote that the shareholders adequately pleaded that the March 2018 revelation about Cambridge Analytica was the first time Facebook investors were alerted that Facebook users did not have complete control over their own

data, and also adequately pleaded that Facebook did not make public statements about the Cambridge Analytica issue between 2015 and 2018.

The panel held that the shareholders adequately pleaded that the Cambridge Analytica and whitelisting revelations, not any other factor, caused the July 2018 stock drop. The panel therefore reversed the district court's dismissal of claims as to Facebook's statements regarding data control that predated the June 3, 2018, whitelisting revelation.

The panel remanded for further proceedings.

Judge Bumatay concurred in part and dissented in part. He joined the majority in holding that the shareholders failed to sufficiently allege a falsity in Facebook's Cambridge Analytica investigation statements. He also joined the majority in holding that the shareholders did allege a falsity and loss from the user control statements—but only as those statements relate to Facebook's practice of "whitelisting." He disagreed with the majority on two fundamental points. In his view, the shareholders failed to sufficiently allege that Facebook's risk factor statements in its public filings were fraudulent, and didn't show that Facebook's user control statements were false based on the Cambridge Analytica revelations.

## COUNSEL

Thomas C. Goldstein (argued), Kevin K. Russell, and Erica O. Evans, Goldstein Russell & Woofter LLC, Bethesda, Maryland; John C. Browne and Jeremy P. Robinson, Bernstein Litowitz Berger & Grossman LLP, New York, New York; Joseph D. Daley, Danielle S. Myers, and Darren J. Robbins, Robbins Geller Rudman & Dowd LLP, San Diego, California; Jason C. Davis, Robbins Geller Rudman & Dowd LLP, San Francisco, California; Kathleen Foley, Munger Tolles & Olson LLP, Washington, D.C.; Jeremy A. Lieberman, Pomerantz LLP, New York, New York; Jennifer Pafiti, Pomerantz LLP, Los Angeles, California; for Plaintiff-Appellant.

Joshua S. Lipshutz (argued), Katherine M. Meeks, and Trenton J. Van Oss, Gibson Dunn & Crutcher LLP, Washington, D.C.; Brian M. Lutz and Michael J. Kahn, Gibson Dunn & Crutcher LLP, San Francisco, California; Orin S. Snyder, Gibson Dunn & Crutcher LLP, New York, New York; Paul J. Collins, Gibson Dunn & Crutcher LLP, Palo Alto, California; for Defendant-Appellee.

## **OPINION**

McKEOWN, Circuit Judge:

In March 2018, news broke that Cambridge Analytica, a British political consulting firm, improperly harvested personal data from millions of unwitting Facebook users and retained copies of the data beyond Facebook's control. In the months that followed, the public learned that Facebook had known of Cambridge Analytica's misconduct for over two years and failed to inform affected users, and that Facebook surreptitiously allowed certain whitelisted third-party apps to access users' Facebook friend data without the users' friends' consent. Facebook and its executives made various statements before and after the news announcements assuring users that they fully controlled their data on Facebook and that no third party would access the data without their consent. In the wake of the Cambridge Analytica and whitelisting scandals, Facebook's stock price suffered two significant drops totaling more than \$200 billion in market capitalization.1

Appellants, collectively "the shareholders," purchased shares of Facebook common stock between February 3, 2017, and July 25, 2018. Soon after the first stock drop in March 2018, they filed a securities fraud action against Facebook and three of its executives: Mark Zuckerberg, Facebook's chief executive officer, Sheryl Sandberg, Facebook's then-chief operating officer, and David Wehner, Facebook's chief financial officer. The shareholders allege that Facebook

<sup>&</sup>lt;sup>1</sup> In late 2021, the parent company Facebook changed its name to Meta Platforms, Inc. Because the events in this case occurred before 2021, we refer to Facebook and its former parent company, Facebook, Inc., simply as Facebook.

and the executives violated Sections 10(b), 20(a), and 20A of the Securities Exchange Act of 1934 and Rule 10b-5 of the Exchange Act's implementing regulations by making materially misleading statements and omissions regarding the risk of improper access to Facebook users' data, Facebook's internal investigation into Cambridge Analytica, and the control Facebook users have over their data. Although the shareholders made multiple claims in their Third Amended Complaint, only these three categories of claims are the subject of this appeal.

This case calls on us to consider whether, under the heightened standard of the Private Securities Litigation Reform Act ("PSLRA"), the shareholders adequately pleaded falsity as to the challenged risk statements, adequately pleaded scienter as to the Cambridge Analytica investigation statements, and adequately pleaded loss causation as to the user control statements. We affirm in part and reverse in part.<sup>2</sup>

### I. BACKGROUND

The Third Amended Complaint clocked in at 285 pages. Although impressive in terms of magnitude, we nonetheless examine the allegations individually and holistically, not by weight or volume.<sup>3</sup>

 $<sup>^2</sup>$  For ease of reference, we use the categories laid out in the Third Amended Complaint. On appeal, the shareholders challenge the district court's dismissal of the statements in  $\P\P$  501–05, 507–14, 519, 525, 530, 533, and 537–38 of the Third Amended Complaint.

<sup>&</sup>lt;sup>3</sup> These facts are based on the allegations in the Third Amended Complaint and may not reflect Facebook's current practices.

Facebook, with more than 1.3 billion daily users at the inception of this case, is the world's largest social media platform. On Facebook, users share personal content, "like" and comment on others' shared content, play games designed by third-party app developers, and more. Facebook collects data from its users, including the types of content they access, the devices they use to access Facebook, their payment information, and their location. The collected data is used to individualize the content a user sees on Facebook. For example, Facebook may suggest local events to a user and tailor the advertisements a user sees. Additionally, a third-party app or website integrated onto the Facebook platform may access user information when the user engages with its services on the platform. For example, a Facebook user may play an online game added to the Facebook platform by a third-party developer. According to Facebook's terms, the game developer could then access the user's age range, location, language preference, list of friends, and other information the user shared with them.

This is not the first time Facebook has found itself in legal hot water over its data sharing practices. In 2012, Facebook settled charges with the Federal Trade Commission ("FTC") that it deceived users by representing that their personal data was private but allowing the data to be shared, including with third-party apps. Facebook entered a twenty-year consent decree as part of the settlement, agreeing not to misrepresent the extent to which Facebook users could control the privacy of their own data. In 2019, the FTC imposed a "record-breaking \$5 billion penalty" on Facebook for violating the consent decree by "deceiving users about their ability to control the privacy of their

personal information."<sup>4</sup> Facebook users have also sued the company alleging that Facebook is dishonest about its privacy practices. See, e.g., In re Facebook, Inc. Internet Tracking Litig., 956 F.3d 589 (9th Cir. 2020); Campbell v. Facebook, Inc., 951 F.3d 1106 (9th Cir. 2020).

In 2014, Zuckerberg announced publicly that Facebook would no longer allow third parties to access and collect data from users' friends, noting that Facebook users were surprised to learn that their Facebook friends could share their data with a third party without their consent. He explained that Facebook users had grown skeptical that their data was safe on the platform, and that Facebook was doing everything it could "to put people first and give people the tools they need" to trust that Facebook would keep their data safe. That same year, however, Zuckerberg and Sandberg created a "reciprocity" system in which certain third-party apps that provided "reciprocal value to Facebook" could be "whitelisted," meaning that those apps were exempt from the ban on third-party data access and collection. The whitelisting practice continued until mid-2018.

In September 2015, Facebook employees noticed that Cambridge Analytica was "receiving vast amounts of Facebook user data." Facebook's political team described Cambridge Analytica as a "sketchy" firm that had "penetrated" Facebook's market and requested an investigation into what Cambridge Analytica was doing with the data. The platform policies

<sup>&</sup>lt;sup>4</sup> Press Release, Fed. Trade Comm'n, FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook.

team concluded that it was unlikely Cambridge Analytica could use Facebook users' data for political purposes without violating Facebook's policies. In November 2015, Facebook paid Aleksandr Kogan, a Cambridge University academic who helped Cambridge Analytica obtain user data from Facebook, to give an internal presentation on the lessons he learned from collecting and working with the Facebook data.

Trouble for Facebook began in December 2015, when The Guardian reported that Cambridge Analytica had created a database of information about American voters by harvesting their Facebook data. The harvested data originated from a personality guiz integrated onto Facebook by Kogan. When Facebook users completed the quiz, Kogan gained access to their data as well as data from their Facebook friends who had not taken the quiz, including each user's name, gender, location, birthdate, "likes," and list of Facebook friends. Facebook's app review team initially rejected the personality quiz because it collected more user data than necessary to operate, but the quiz nonetheless became available to Facebook users. Although only about 250,000 Facebook users took the personality quiz, Kogan harvested data from over thirty million users, most of whom did not consent to the data collection.

Kogan used the Facebook "likes" collected from the quiz to train an algorithm that assigned personality scores to Facebook users, including users who had not taken the quiz. The information was saved in a

<sup>&</sup>lt;sup>5</sup> See Harry Davies, Ted Cruz Using Firm that Harvested Data on Millions of Unwitting Facebook Users, Guardian (Dec. 11, 2015),https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data.

database that classified American voters by scoring them on five personality traits: "openness to experience, conscientiousness, extraversion, agreeableness, and neuroticism (the 'OCEAN scale')." According to *The Guardian*, Cambridge Analytica used the harvested OCEAN scale data to help Ted Cruz's presidential campaign "gain an edge over Donald Trump" in the Republican Party primaries.

In response to the *Guardian* article, a Facebook spokesperson stated that the company was "carefully investigating" the situation, that misusing user data was a violation of Facebook's policies, and that the company would "take swift action" against third parties found to have misused Facebook users' data. In a private email exchange in December 2015, a Facebook executive told a Cambridge Analytica executive that Cambridge Analytica violated Facebook's policies and terms by using data that Kogan "improperly derived" from Facebook. Cambridge Analytica agreed in January 2016 to delete the personality score data harvested from Facebook.

Notwithstanding Cambridge Analytica's assurance that it would delete the data, Facebook continued to investigate the data usage. In June 2016, Facebook negotiated a confidential settlement with Kogan, who certified that he had deleted the data in his possession derived from Facebook "likes." Kogan also provided Facebook with the identity of every entity with which he had shared raw Facebook user data. In doing so, Kogan revealed that he had shared derivative and raw data from Facebook users—not just the personality score data—with Cambridge Analytica's chief executive, Alexander Nix, and that the data was still being used in violation of Facebook's stated policies. Facebook asked Nix to certify that all data harvested from

the Facebook personality quiz was deleted, but Nix refused to do so. In October 2016, *The Washington Post* reported that Cambridge Analytica continued to use data based on the OCEAN scale to benefit the Trump presidential campaign. The article did not say explicitly that the social-media data came from Facebook, but the use of the OCEAN scale suggested that Cambridge Analytica may have been using the data originally harvested from Kogan's personality quiz on Facebook.

# 1. Facebook's Public Filings

Despite the ongoing developments regarding Cambridge Analytica, Facebook represented in its 2016 Form 10-K, filed with the Securities Exchange Commission ("SEC") in February 2017, that thirdparty misuse of Facebook users' personal data was a purely hypothetical risk that could harm the company if it materialized. For example, the 10-K stated that "[a]ny failure to prevent or mitigate . . . improper access to or disclosure of our data or user data . . . could result in the loss or misuse of such data, which could harm [Facebook's] business and reputation and diminish our competitive position." The statements about the risks of improper access or disclosure appeared in the "Risk Factors" section of the 10-K, in a subsection that also discussed the risks of security breaches such as cyberattacks, hacking, and phishing

<sup>&</sup>lt;sup>6</sup> Michael Kranish, Trump's Plan for a Comeback Includes Building a 'Psychographic' Profile of Every Voter, Wash. Post (Oct. 27, 2016), https://www.washingtonpost.com/politics/trumps-plan-for-a-comeback-includes-building-a-psychographic-profile-of-every-voter/2016/10/27/9064a706-9611-11e6-9b7c-57290af48a49 story.html.

that could result in Facebook user data falling into the wrong hands.

# 2. Continued Press about Cambridge Analytica

In March 2017, The Guardian published another article about Cambridge Analytica's political activity. The article discussed how Cambridge Analytica used data derived from Facebook "likes" to train algorithms and quoted a Cambridge Analytica spokesperson's denial that the firm had access to Facebook "likes." The article also quoted a Facebook spokesperson's statement that Facebook's investigation into Cambridge Analytica had not yet uncovered any misconduct related to the firm's work on political matters, specifically the Trump presidential campaign or the Brexit Leave campaign. A Facebook spokesperson made similar comments to journalists later that month.8 Throughout 2017 and early 2018, Facebook and its executives assured Facebook users that "no one is going to get your data that shouldn't have it," that Facebook and its apps had "long been focused on giving people transparency and control," and more.

<sup>&</sup>lt;sup>7</sup> Jamie Doward, Carole Cadwalladr & Alice Gibbs, Watchdog to Launch Inquiry into Misuse of Data in Politics, Guardian (Mar. 4, 2017), https://www.theguardian.com/technology/2017/mar/04/cambridge-analytics-data-brexit-trump.

<sup>&</sup>lt;sup>8</sup> Tim Sculthorpe, *Privacy Watchdog Launces a Probe into How the Leave Campaigns Used Voters' Personal Data to Win Brexit*, Daily Mail (Mar. 5, 2017), https://www.dailymail.co.uk/news/article-4283102/amp/Privacy-watchdog-launches-probe-Leave-use-data.html; Mattathias Schwartz, *Facebook Failed to Protect 30 Million Users From Having Their Data Harvested By Trump Campaign Affiliate*, Intercept (Mar. 30, 2017), https://theintercept.com/2017/03/30/facebook-failed-to-protect-30-million-users-from-having-their-data-harvested-by-trump-campaign-affiliate/.

On March 12, 2018, The New York Times and The Guardian contacted Facebook for comment on joint articles the outlets planned to publish about Cambridge Analytica's misuse of Facebook users' data. The articles would report that Cambridge Analytica had not actually deleted the improperly collected Facebook user data from 2015. Before the articles went to print, Facebook announced on its investor relations website that it was suspending Cambridge Analytica for violating its policies by sharing Facebook users' data without the users' consent and for failing to delete the improperly collected data. Facebook explained that, in 2015, it had demanded certification that Cambridge Analytica and Kogan had destroyed the harvested user data, but that Facebook had just learned that not all the data was deleted. Soon after, The New York Times reported that Cambridge Analytica's use of Facebook users' data was "one of the largest data leaks in the social network's history." The article took the position that most people whose data was harvested had not consented to the collection, that Cambridge Analytica had used the data to benefit the Trump presidential campaign in 2016, and that "copies of the data still remain[ed] beyond Facebook's control."10

Other media outlets and government officials sprang into action. Political figures in the United States and Europe called for investigation into the Cambridge Analytica privacy scandal. Reporters

<sup>&</sup>lt;sup>9</sup> Matthew Rosenberg, Nicholas Confessore & Carole Cadwalladr, How Trump Consultants Exploited the Facebook Data of Millions, N.Y. Times (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

<sup>&</sup>lt;sup>10</sup> *Id*.

wrote that Facebook knew about the data breach for years and failed to disclose it to the millions of affected users. In particular, CNN observed that "[n]o one ha[d] provided an adequate explanation for why Facebook did not disclose Kogan's violation to the more than 50 million users who were affected when the company first learned about it in 2015." That same day, an article in *Seeking Alpha* warned that "[i]f Cambridge Analytica was able to acquire information on tens of millions of Facebook users so quickly and easily, and then keep the information for years without Facebook suspecting otherwise, then that shows a serious flaw in Facebook's ability to keep exclusive control over its information." <sup>12</sup>

# 3. Facebook's Stock Price Drop and Low Revenue and Profit Growth

The price of Facebook's stock declined significantly in the week that followed the Cambridge Analytica revelations. On March 19, 2018—the first trading day after the news broke—Facebook shares fell almost 7%. The next day, Facebook shares fell an additional 2.5%. After one week, Facebook's stock price had dropped nearly 18% from the price before the news about Cambridge Analytica was published, reflecting a loss of more than \$100 billion in market capitalization. At this juncture, the shareholders filed

<sup>&</sup>lt;sup>11</sup> Dylan Byers, Facebook Is Facing an Existential Crisis, CNN (Mar. 19, 2018), https://money.cnn.com/2018/03/19/technology/business/facebook-data-privacy-crisis/index.html.

<sup>&</sup>lt;sup>12</sup> Erich Reimer, *The Cambridge Analytica Mishap Is Serious for Facebook*, Seeking Alpha (Mar. 19, 2018), https://seekingalpha.com/article/4157578-cambridge-analytica-mishap-is-serious-for-facebook.

their first securities fraud complaint against Facebook.

In the aftermath, Facebook reiterated its statements that users have privacy and control over their personal data on the platform. At an April 2018 press conference, Zuckerberg stated that "you have control over everything you put on the service." Later that month, Zuckerberg issued a public post on Facebook, saying: "You've been hearing a lot about Facebook lately and how your data is being used. While this information can sometimes be confusing and technical, it's important to know that you are in control of your Facebook, what you see, what you share, and what people see about you." Zuckerberg also testified before the United States Senate that users have control over both what they share on Facebook and their personal data connected to advertisements on the platform.

On June 3, 2018, more news emerged about Facebook's privacy practices. *The New York Times* reported that Facebook had continued sharing the data of users and their Facebook friends with dozens of whitelisted third parties like Apple, Microsoft, and Samsung without the users' express consent.<sup>13</sup> The article reported that Facebook's whitelisting policy violated the company's FTC consent decree and contradicted Zuckerberg's 2014 announcement that Facebook's third-party data sharing practice had been shuttered.<sup>14</sup> An FTC investigator testified before the Parliament of the United Kingdom that, for nearly a

<sup>&</sup>lt;sup>13</sup> Gabriel J.X. Dance, Nicholas Confessore & Michael Laforgia, Facebook Gave Device Makers Deep Access to Data on Users and Friends, N.Y. Times (June 3, 2018), https://nyti.ms/3aFIMAI.

<sup>&</sup>lt;sup>14</sup> *Id*.

decade, the whitelisted apps were allowed to completely override Facebook users' privacy settings. Multiple news outlets subsequently reported that Facebook shared its users' data with foreign entities "believed to be national security risks" without the users' knowledge.

Finally, on July 25, 2018, Facebook announced unexpectedly low revenue growth, profitability, and user growth in its Q2 earnings call. Facebook stated that the disappointing revenue growth occurred because it was "putting privacy first" as well as implementing the European Union's General Data Protection Regulation ("GDPR"). Zuckerberg reported that the GDPR rollout also resulted in a decline in monthly Facebook users across Europe. The day after the earnings call, Facebook's stock price dropped nearly 19%. Analysts and investors attributed the stock drop to the company's GDPR implementation, the requisite increased security and privacy required of tech companies, and the Cambridge Analytica and whitelisting scandals.

## 4. Filing of Amended Complaints

The revelation of the Cambridge Analytica and whitelisting scandals and the two Facebook stock price drops precipitated an amended filing by the shareholders in October 2018. The shareholders amended the complaint again in November 2019 (Second Amended Complaint) and October 2020 (Third Amended Complaint). They brought claims against Facebook, Zuckerberg, Sandberg, and Wehner under Sections 10(b), 20(a), and 20A of the Securities Exchange Act of 1934 and Rule 10b-5 of the Exchange Act's implementing regulations. The shareholders allege that Facebook, through the executive defendants

or a company spokesperson, made several false or materially misleading statements between February 3, 2017, and July 25, 2018, "the class period." The challenged statements fall into three categories: (1) statements in Facebook's 2016 Form 10-K regarding the risk of improper third-party access to and disclosure of Facebook users' data; (2) statements regarding Facebook's investigation into Cambridge Analytica's 2015 misconduct; and (3) statements regarding the control Facebook users have over their data on the platform.

The district court dismissed the shareholders' First Amended Complaint and Second Amended Complaint without prejudice under Federal Rule of Civil Procedure 12(b)(6), giving the shareholders leave to amend both times. After determining that the Third Amended Complaint failed to remedy the deficiencies of the first two amended filings, the district court dismissed the shareholders' claims without leave to amend.

## II. ANALYSIS

Although the scope of claims under Section 10(b) of the Exchange Act and Rule 10b-5 of the Exchange Act's implementing regulations is well understood and well-tread in the Ninth Circuit, these principles bear repeating so that our analysis is viewed in context.

Section 10(b) of the Exchange Act, 15 U.S.C. § 78j(b), prohibits "manipulative or deceptive" practices in connection with the purchase or sale of a security. See In re Alphabet Sec. Litig., 1 F.4th 687, 699 (9th Cir. 2021). Rule 10b-5 of the Exchange Act's implementing regulations is coextensive with Section 10(b). S.E.C. v. Zandford, 535 U.S. 813, 816 n.1

(2002). The Rule prohibits making "any untrue statement of a material fact" or omitting material facts "necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading." Glazer Cap. Mgmt., L.P. v. Forescout Techs., Inc. (Glazer II), 63 F.4th 747, 764 (9th Cir. 2023) (quoting 17 C.F.R. § 240.10b-5(b)). To state a claim under Section 10(b) and Rule 10b-5, "a plaintiff must allege: (1) a material misrepresentation or omission by the defendant ('falsity'); (2) scienter; (3) a connection between the misrepresentation or omission and the purchase or sale of a security; (4) reliance upon the misrepresentation or omission; (5) economic loss; and (6) loss causation." *Id.* (internal quotation marks omitted) (quoting In re NVIDIA Corp. Sec. Litig., 768 F.3d 1046, 1052 (9th Cir. 2014)). Claims under Sections 20(a) and 20A of the Exchange Act are derivative "and therefore require an independent violation of the Exchange Act," so the shareholders must successfully plead a Section 10(b) claim to succeed on their claims under Sections 20(a) and 20A. See Johnson v. Aljian, 490 F.3d 778, 781 (9th Cir. 2007); see also Glazer II, 63 F.4th at 765.

Complaints alleging securities fraud are also subject to heightened pleading requirements under the Private Securities Litigation Reform Act ("PSLRA") and Rule 9(b). *Glazer II*, 63 F.4th at 765. The PSLRA requires that complaints alleging falsity "specify each statement alleged to have been misleading, the reason or reasons why the statement is misleading, and, if an allegation regarding the statement or omission is made on information and belief, the complaint shall state with particularity all facts on which that belief is formed." *Id.* (quoting 15 U.S.C. § 78u-4(b)(1)). To plead scienter under the PSLRA, "the complaint must 'state with particularity facts giving rise to a strong

inference that the defendant acted with the required state of mind." Id. at 766 (quoting 15 U.S.C. § 78u-4(b)(2)(A)). When evaluating "whether the strong inference standard is met," the court first "determines whether any one of the plaintiff's allegations is alone sufficient to give rise to a strong inference of scienter." *Id.* If no individual allegation is sufficient, the court "conducts a 'holistic' review to determine whether the allegations combine to give rise to a strong inference of scienter." Id. (quoting Zucco Partners, LLC v. Digimarc Corp., 552 F.3d 981, 992 (9th Cir. 2009)). Rule 9(b) similarly requires plaintiffs to "state with particularity the circumstances constituting fraud." Id. at 765 (quoting Fed. R. Civ. P. 9(b)). Fraud allegations under Rule 9(b) "must be 'specific enough to give defendants notice of the particular misconduct which is alleged to constitute the fraud charged so that they can defend against the charge and not just deny that they have done anything wrong." Id. (quoting Bly-Magee v. California, 236 F.3d 1014, 1019 (9th Cir. 2001)).

We review de novo the dismissal of a complaint for failure to state a claim, accepting the factual allegations as true and viewing the facts "in the light most favorable" to the shareholders. *Id.* at 763. In addition to the pleading requirements of the PSLRA and Rule 9(b), Rule 8(a) requires that a complaint "contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face." *Id.* (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)). The factual allegations in the complaint must "allow[] the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* (quoting *Iqbal*, 556 U.S. at 678).

## A. Risk Statements

The essence of the challenged risk statements is that, although Facebook knew Cambridge Analytica had improperly accessed and used Facebook users' data, Facebook represented in its 2016 Form 10-K that only the hypothetical risk of improper third-party misuse of Facebook users' data could harm Facebook's business, reputation, and competitive position. For example, Facebook's 2016 10-K warned that the "failure to prevent or mitigate security breaches and improper access to or disclosure of our data or user data could result in the loss or misuse of such data" and that if "third parties or developers fail to adopt or adhere to adequate data security practices . . . our data or our users' data may be improperly accessed, used, or disclosed." Additionally, two of the challenged statements warn that Facebook cannot provide "absolute [data] security" and that Facebook's business will suffer if the public does not perceive Facebook's products to be "useful, reliable, and trustworthy."

The district court held that the shareholders failed to plead falsity as to the risk statements, but its holding predated our decision in *In re Alphabet*. Without the benefit of our reasoning in *In re Alphabet*, the district court held that the risk statements were not actionably false because Cambridge Analytica's misconduct was public knowledge at the time the statements were made and because, while the 10-K warned of risks of harm to Facebook's business, reputation, and competitive position, the shareholders failed to allege that Cambridge Analytica's misconduct was causing such harm when the statements were made. This approach overlooks the reality of what Facebook knew.

In the securities fraud context, statements and omissions are actionably false or misleading if they "directly contradict what the defendant knew at that time," Khoja v. Orexigen Therapeutics, Inc., 899 F.3d 988, 1008 (9th Cir. 2018), or "create an impression of a state of affairs that differs in a material way from the one that actually exists," Brody v. Transitional Hosps. Corp., 280 F.3d 997, 1006 (9th Cir. 2002). The Exchange Act does not, however, "create an affirmative duty to disclose any and all material information." Glazer II, 63 F.4th at 764 (quoting Matrixx Initiatives, Inc. v. Siracusano, 563 U.S. 27, 44 (2011)). Disclosure is mandatory only when necessary to ensure that a statement made is "not misleading." *Id.* (quoting *Ma*trixx Initiatives, 563 U.S. at 44). Accordingly, if the market has already "become aware of the allegedly concealed information," the allegedly false information or material omission "would already be reflected in the stock's price' and the market 'will not be misled." Provenz v. Miller, 102 F.3d 1478, 1492 (9th Cir. 1996) (quoting In re Convergent Techs. Sec. Litig., 948 F.2d 507, 513 (9th Cir. 1991)).

Our recent decision in *In re Alphabet* is instructive. We held that falsity allegations were sufficient to survive a motion to dismiss when the complaint plausibly alleged that a company's SEC filings warned that risks "could" occur when, in fact, those risks had already materialized. *In re Alphabet*, 1 F.4th at 702–05. This juxtaposition of a "could occur" situation with the fact that the risk had materialized mirrors the allegations in the Facebook scenario. In its 2017 Form 10-K, Alphabet warned of the risk that public concerns about its privacy and security practices "could" harm its reputation and operating results. *Id.* at 694. The following year, Alphabet discovered a privacy bug that had threatened thousands of users' personal data

for three years. Id. at 695. Nonetheless, in its April and July 2018 Form 10-Q filings, Alphabet repeated the 2017 statement that public concern about its privacy and security "could" cause harm. Id. at 696. In the 10-Qs, Alphabet also stated that there had "been no material changes" to its "risk factors" since the 2017 10-K. Id. Although news of the privacy bug had not become public at the time of the 10-Qs, we reasoned that the risks of harm to Alphabet "ripened into actual harm" when Alphabet employees discovered the privacy bug and the "new risk that this discovery would become public." Id. at 703. The plaintiffs thus "plausibly allege[d] that Alphabet's warning in each Form 10-Q of risks that 'could' or 'may' occur [was] misleading to a reasonable investor when Alphabet knew that those risks had materialized." Id. at 704.

As in *In re Alphabet*, the shareholders here adequately pleaded falsity as to the statements in Facebook's 2016 10-K that represented the risk of third parties improperly accessing and using Facebook users' data as purely hypothetical. The shareholders pleaded with particularity that Facebook employees flagged Cambridge Analytica in September 2015 for potentially violating Facebook's terms, that Kogan taught Facebook in November 2015 about the dataset Cambridge Analytica had compiled, and that a Facebook executive told Cambridge Analytica in December 2015 that the firm had violated Facebook's user data policies. The shareholders also alleged that after Facebook learned in June 2016 that Cambridge Analytica lied in December 2015 about deleting the data derived from Facebook "likes," Cambridge Analytica's chief executive refused to certify that the data had actually been deleted. These allegations, if true, more than support the claim that Facebook was aware of Cambridge Analytica's misconduct before February

2017, so Facebook's statements about risk management "directly contradict[ed]" what the company knew when it filed its 2016 10-K with the SEC. *Glazer II*, 63 F.4th at 764.

Referencing Facebook's risk statements as including damage to its business, reputation, and competitive position, the dissent asserts that the risk statements in Facebook's 2016 10-K were not false or materially misleading because they "do not represent that Facebook was free from significant breaches at the time of the filing." The inadequacy of the risk statements, however, is not that Facebook did not disclose Cambridge Analytica's breach of its security practices. Instead, the problem is that Facebook represented the risk of improper access to or disclosure of Facebook user data as purely hypothetical when that exact risk had already transpired. A reasonable investor reading the 10-K would have understood the risk of a third party accessing and utilizing Facebook user data improperly to be merely conjectural.

The dissent's suggestion that the shareholders have not adequately pleaded falsity because they "have not sufficiently alleged that Facebook knew that its reputation and business were *already* harmed at the time of the filing of the 10-K" fares no better. Our case law does not require harm to have materialized for a statement to be materially misleading. Facebook's statement was plausibly materially misleading even if Facebook did not yet know the extent of the reputational harm it would suffer as a result of the breach: Because Facebook presented the prospect of a breach as purely hypothetical when it had already occurred, such a statement could be misleading even if the magnitude of the ensuing harm was still un-

known. Put differently, a company may make a materially misleading statement when it "speaks entirely of as-yet-unrealized risks" when the risks have "already come to fruition." Berson v. Applied Signal Tech., 527 F.3d 982, 987 (9th Cir. 2008); see also In re Alphabet, 1 F.4th at 702–05 (holding that risk statements in Alphabet's SEC filings were materially misleading even where Alphabet's identified harm of damage to its "business, financial condition, results of operations," and more had not yet materialized at the time of the filings). The mere fact that Facebook did not know whether its reputation was already harmed when filing the 10-K does not avoid the reality that it "create[d] an impression of a state of affairs that differ[ed] in a material way from the one that actually exist[ed]." *Brody*, 280 F.3d at 1006.

The dissent endeavors to distinguish *In re Alpha*bet by explaining that before Alphabet made SEC filings containing material misstatements, it circulated an internal memorandum detailing that there would be immediate regulatory scrutiny if the public discovered its privacy bug. While true, our holding did not rest on the internal memorandum to conclude that the statements were plausibly materially misleading; instead, we reasoned that a warning of "risks that 'could' or 'may' occur is misleading to a reasonable investor when Alphabet knew that those risks"—the privacy bug itself—"had materialized." 1 F.4th at 704. Here, as in *In re Alphabet*, it is the fact of the breach itself, rather than the anticipation of reputational or financial harm, that caused anticipatory statements to be materially misleading. The shareholders have therefore adequately pleaded that the risk statements in Facebook's 2016 10-K directly contradicted what Facebook knew at the time such that, in the dissent's words, Facebook "knew a risk had come to fruition" and "chose to bury it."

Notably, although the dissent seemingly perceives it otherwise, the extent of Cambridge Analytica's misconduct was not yet public when Facebook filed its 2016 10-K. At the time, the articles in The Guardian and The Washington Post had alerted readers that Cambridge Analytica collected data from "a massive pool of mainly unwitting US Facebook users." But the Guardian article quoted a Facebook spokesperson saying that the company would take "swift action" if Cambridge Analytica was found to have violated Facebook's policies, as well as a Ted Cruz spokesperson saying that the data was acquired legally and with the permission of Facebook users. In response to the article, Facebook stated it was "carefully investigating." Although the articles may have raised concerns about Cambridge Analytica's conduct, Facebook did not confirm before the 2016 10-K was filed that Cambridge Analytica had acted improperly or whether Facebook had taken the "swift action" promised if it learned of violations.

Indeed, Facebook's first public statement about the results of its investigation—which came in March 2017, a month after the 2016 10-K was filed—represented that no misconduct had been discovered. At the time the 10-K was filed in February 2017, the news of Cambridge Analytica's misconduct was far from "transmitted to the public with a degree of intensity and credibility sufficient to effectively counterbalance any misleading impression." *Provenz*, 102 F.3d at 1493 (citation omitted).

Importantly, and contrary to the dissent's position, the placement of the risk statements in Face-

book's 2016 10-K alongside the possibilities of cyberattacks, hacking, and phishing, which the shareholders do not allege had materialized at the time of the 10-K, does not rescue Facebook's omission that the risk of improper access and disclosure had occurred from being materially misleading. A close read of the 10-K reveals that the stated hypothetical risks included the risk of a third-party developer harvesting Facebook users' data without their consent. Indeed, the title of the 10-K subsection in which the risk statements appeared included the statement that "improper access to or disclosure of" Facebook's "user data" could harm the company's reputation and business. The subsection itself stated that "[a]ny failure to prevent or mitigate security breaches and improper access to or disclosure of our data or user data could result in the loss or misuse of such data." Kogan and Cambridge Analytica's actions, while not a cyberattack, hacking, or phishing, fit the bill of Facebook failing to prevent or mitigate improper access to or disclosure of Facebook data. The risk of a third-party improperly accessing Facebook user data through methods other than hacking, phishing, or any other security breach was prominent throughout the subsection and covered the claimed misconduct of Cambridge Analytica. Collapsing the risks of improper access to and use of Facebook users' data in the same section as the risk of cyberattacks cannot rescue the risk statements from being false or materially misleading.

Additionally, Facebook's disclosure that "computer malware, viruses, social engineering (predominantly spear phishing attacks), and general hacking have become more prevalent in our industry, have occurred on our systems in the past, and will occur on our systems in the future" does not bring the risk statements within the protection of the PSLRA's safe

harbor provision for forward-looking statements. Under the safe harbor, a company is not liable for a forward-looking statement "accompanied by meaningful cautionary statements identifying important factors that could cause actual results to differ materially from those in the forward-looking statement." *Glazer II*, 63 F.4th at 767 (quoting 15 U.S.C. § 78u-5(c)(1)(A)).

Our recent decision in Weston Family Partnership v. Twitter, Inc., 29 F.4th 611 (9th Cir. 2022), provides a good illustration of statements falling within the safe harbor provision. There, Twitter disclosed its plan to improve the "stability, performance, and flexibility," of its mobile app promotion product gradually "over multiple quarters" and made clear that the company was "not there yet" in terms of its stability goals. Id. at 616. At the time, Twitter knew of a software bug affecting its mobile app promotion product but did not disclose the bug's impact. Id. We explained that Twitter's disclosure was both forward-looking and accompanied by the type of "meaningful cautionary language" necessary to invoke the safe harbor provision despite the nondisclosure of the software bug. Id. at 623.

Here, rather than making cautionary forward-looking statements, Facebook warned that it could not provide "absolute security," that it would continue to be subject to cyberattacks, and that third parties with inadequate data security practices could compromise users' data. Such broad pronouncements without meaningful acknowledgement of the known risks of improper data access and disclosure does not suffice to invoke the safe harbor provision. There is a big chasm between "absolute security" and sidestepping the reality of what Facebook allegedly knew about the compromised data.

At this stage, the shareholders adequately pleaded falsity as to the statements warning that misuse of Facebook users' data could harm Facebook's business, reputation, and competitive position and the district court erred by dismissing the complaint as to those statements. The district court, however, correctly dismissed the challenged statements regarding the risk of security breaches and the risk of the public not perceiving Facebook's products to be "useful, reliable, and trustworthy." Those statements do not relate to the misuse of Facebook user data by Cambridge Analytica, and the shareholders do not allege that those risks had materialized at the time of the 2016 10-K such that they were false or materially misleading. We leave to the district court on remand whether the shareholders can satisfy the other elements of the claims with respect to risk statements.

# B. Cambridge Analytica Investigation Statements

The challenged Cambridge Analytica investigation statements include statements made by a Facebook spokesperson to journalists in March 2017 that Facebook's internal investigation into Cambridge Analytica had "not uncovered anything that suggest[ed] wrongdoing" related to Cambridge Analytica's work on the Brexit and Trump campaigns. The district court held that the shareholders failed to plead scienter as to the Cambridge Analytica investigation statements. We agree.

To plead scienter, the shareholders "must 'state with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind." *Glazer II*, 63 F.4th at 766 (quoting 15 U.S.C. § 78u-4(b)(2)(A)). "A 'strong inference' exists 'if a reasonable person would deem the inference of scienter

cogent and at least as compelling as any opposing inference one could draw from the facts alleged." *Id.* (quoting *Tellabs, Inc. v. Makor Issues & Rts., Ltd.*, 551 U.S. 308, 324 (2007)). For obvious reasons, an actionably misleading statement must be made by a spokesperson "who has actual or apparent authority." *In re ChinaCast Educ. Corp. Sec. Litig.*, 809 F.3d 471, 476 (9th Cir. 2015) (quoting *Hollinger v. Titan Cap. Corp.*, 914 F.2d 1564, 1577 n.28 (9th Cir. 1990)). Thus, "a key inquiry" in evaluating a motion to dismiss "is whether the complaint sufficiently alleges scienter attributable to the corporation." *Id.* at 479.

Of first order is identifying "whether the complaint adequately alleged that the maker omitted material information knowingly, intentionally, or with deliberate recklessness." *In re Alphabet*, 1 F.4th at 705. "Deliberate recklessness is a higher standard than mere recklessness and requires more than a motive to commit fraud." *Glazer II*, 63 F.4th at 765 (quoting *Schueneman v. Arena Pharms., Inc.*, 840 F.3d 698, 705 (9th Cir. 2016)). Instead, "deliberate recklessness" involves "an *extreme* departure from the standards of ordinary care" that presents "a danger of misleading buyers or sellers" that "is so *obvious*" that the spokesperson "must have been aware of it." *Id.* (quoting *Schueneman*, 840 F.3d at 705).

Simply raising an inference that a company's executive "should have" discovered misconduct, not that the executive actually knew of misconduct, is insufficient "to meet the stringent scienter pleading requirements of the PSLRA." Glazer Cap. Mgmt., LP v. Magistri (Glazer I), 549 F.3d 736, 748–49 (9th Cir. 2008). In Glazer I, the defendant CEO signed a merger agreement before announcing months later that an investigation early in the merger-related due diligence

process uncovered possible Foreign Corrupt Practices Act violations. *Id.* at 740. The plaintiffs argued that because the violations were discovered early, information about the violations "must have been readily available and therefore known to [the CEO] when he signed the merger agreement." *Id.* at 748. We held that the CEO learning of the violations shortly after due diligence was not enough "to create a strong inference of scienter." *Id.* The only strong inference to be drawn was that the CEO *should* have known of the possible violations, not that he actually knew about them, which was insufficient to plead scienter. *Id.* 

As in Glazer I, the shareholders pleaded only that the Facebook spokesperson should have known that Facebook's investigation into Cambridge Analytica had uncovered misconduct, not that the spokesperson actually knew of any misconduct or even that there was a strong inference of an "intent to deceive, manipulate, or defraud." Id. at 742 (quoting Ernst & Ernst v. Hochfelder, 425 U.S. 185, 193.12 (1976)). The mere reference by an unidentified spokesperson to Facebook's investigation is insufficient to show that the spokesperson knowingly or intentionally made false or materially misleading statements about the investigation. The shareholders' allegations do not rise to the level of showing that it was "so obvious" that Facebook's investigation had uncovered misconduct related to Cambridge Analytica's political work that the spokesperson "must have been aware of it." Glazer II, 63 F.4th at 765 (citation omitted).

Although one might reasonably expect the spokesperson to have verified the accuracy of the statements before making them, securities fraud actions are not tort actions, and "[m]ere negligence—even headscratching mistakes—does not amount to fraud." Prodanova v. H.C. Wainwright & Co., 993 F.3d 1097, 1103 (9th Cir. 2021). Nothing in the complaint suggests that the Cambridge Analytica investigation statements involved an extreme departure from the standards of ordinary care, and the shareholders thus fall short of raising a strong inference that the spokesperson acted with the necessary malintent. In light of the absence of scienter, we need not assess the alleged falsity of the statements. We affirm the district court's dismissal of the allegations and agree that the shareholders failed to plead scienter as to the Cambridge Analytica investigation statements.

#### C. User Control Statements

Throughout the class period, Facebook made several statements about users' control over their personal data. The statements assured Facebook users that they had control over their information and content on Facebook and that Facebook's priorities of transparency and user control aligned with the GDPR framework. The following Facebook statements are illustrative: "People can control the audience for their posts and the apps that can receive their data," "[e]very person gets to control who gets to see their content," and "[w]e respected the privacy settings that people had in place." The shareholders assert that Facebook's stock price dropped after reporting on the Cambridge Analytica scandal in March 2018 and Facebook's whitelisting policy in June 2018 revealed the falsity of Facebook's statements about users' control over their data. They allege that the stock price drops caused them to suffer economic loss.

Pleading loss causation requires a showing that the "share price fell significantly after the truth became known." *In re Oracle Corp. Sec. Litig.*, 627 F.3d 376, 392 (9th Cir. 2010) (quoting *Dura Pharms.*, *Inc.* 

v. Broudo, 544 U.S. 336, 347 (2005)). "[L]oss causation is simply a variant of proximate cause." Lloyd v. CVB Fin. Corp., 811 F.3d 1200, 1210 (9th Cir. 2016). The shareholders must show that Facebook's "misstatement, as opposed to some other fact, foreseeably caused the plaintiff's loss." Id. The shareholders' "burden of pleading loss causation is typically satisfied by allegations that the defendant revealed the truth through 'corrective disclosures' which 'caused the company's stock price to drop and investors to lose money." Id. at 1209 (quoting Halliburton Co. v. Erica P. John Fund, Inc., 573 U.S. 258, 264 (2014)).

Neither the Federal Rules of Civil Procedure nor the federal securities laws "impose any special further requirement in respect to the pleading of proximate causation or economic loss" beyond the "short and plain statement of the claim" required by Rule 8. Dura *Pharms.*, 544 U.S. at 346. At the pleading stage, it is generally inappropriate to dismiss for failure to establish loss causation. In re Gilead Scis. Sec. Litig., 536 F.3d 1049, 1057 (9th Cir. 2008) (agreeing that loss causation "is a matter of proof at trial and not to be decided on a Rule 12(b)(6) motion to dismiss" (citation omitted)). Put differently, if a complaint proffers sufficient facts "to raise a reasonable expectation that discovery will reveal evidence" of loss causation, the allegations therein should survive a motion to dismiss. Id. (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 556 (2007)).

As an initial matter, the district court correctly held that the shareholders failed to plead sufficiently that Facebook's statements about the company's commitment to transparency and control in line with the GDPR framework violated Section 10(b) and Rule 10b-5. As Facebook notes, those statements "merely

reiterated Facebook's ongoing commitment to 'transparency and control" rather than assuring users they controlled their Facebook data, and thus were not false when they were made. Further, the June 2018 whitelisting revelation, which was unaccompanied by a stock price drop, is not actionable. *See Lloyd*, 811 F.3d at 1210. We affirm the dismissal of the statements related to Facebook's goals of transparency and control, and the June 2018 whitelisting revelation as a standalone claim. However, we reverse the dismissal as to other statements related to the stock drops.

# 1. March 2018 Stock Price Drop

Most of the challenged user control statements occurred after the March 16, 2018, revelation about Cambridge Analytica and thus cannot be pegged to the March 2018 stock price drop. However, the user control statements that preceded the revelation are relevant here, and the shareholders adequately pleaded loss causation as to the statements assuring users that they control their content and information on the platform.

The shareholders adequately pleaded that the March 2018 revelation about Cambridge Analytica was the first time Facebook investors were alerted that Facebook users did not have complete control over their own data. As previously discussed, the 2015 and 2016 articles in *The Guardian* and *The Washington Post* did not reveal that Cambridge Analytica had misused Facebook users' data. Facebook's public response to the *Guardian* article in 2015 was that it was "carefully investigating" Cambridge Analytica.

The shareholders also adequately allege that Facebook did not make public statements about the Cambridge Analytica issue between 2015 and 2018.

Before the March 2018 news broke, reasonable investors would not have known that Cambridge Analytica had improperly accessed Facebook users' data such that users did not have control over their personal information on the platform. In the week that followed the revelation, Facebook's stock dropped nearly 18%, representing a loss of over \$100 billion in market capitalization and plausibly causing economic loss for the shareholders.

The Cambridge Analytica revelation thus satisfies the pleading criteria for a corrective disclosure, which requires allegations that "the defendant's fraud was 'revealed to the market and caused the resulting loss[]." Grigsby v. BofI Holding, Inc., 979 F.3d 1198, 1205 (9th Cir. 2020) (quoting Loos v. Immersion Corp., 762 F.3d 880, 887 (9th Cir. 2014)). A disclosure is not corrective if the information comes entirely from public sources "of which the stock market was presumed to be aware." *Id.* (quoting Loos, 762 F.3d at 889). Here, because the 2015 and 2016 articles about Cambridge Analytica did not provide investors the necessary information to learn that Facebook users did not control their data, the shareholders adequately alleged that the March 2018 revelation was a corrective disclosure as to Facebook's statements that users control their data on the platform. We reverse the district court's dismissal of Facebook's statements about users controlling their own Facebook data that preceded the March 16, 2018, revelation.

# 2. July 2018 Stock Price Drop

The July 2018 drop occurred immediately after Facebook's disappointing earnings report and was tied to approximately \$100 billion of shareholder value loss. At the time, it was the largest single-day stock price drop in U.S. history. The question is

whether the shareholders adequately pleaded loss causation as to Facebook's user control statements predating the March 16, 2018, Cambridge Analytica revelation and the June 3, 2018, whitelisting revelation, even though the stock drop did not occur until July 25, 2018.

Because loss causation requires that the defendant's misstatement, rather than some other fact, fore-seeably caused the plaintiff's loss, establishing loss causation requires more than "an earnings miss" or the market's reaction to a company's "poor financial health generally." *In re Oracle*, 627 F.3d at 392. Simply pleading "that the market reacted to the purported 'impact' of the alleged fraud—the earnings miss—rather than to the fraudulent acts themselves" is not sufficient. *Id*.

Illustrative of a disconnect between earnings and causation is In re Oracle, where the shareholders argued that Oracle's misstatements regarding the "quality and success" of its Suite 11i product, rather than its struggling financial health, caused the company's stock price to drop. Id. at 392–93. The shareholders posited that because the stock price drop occurred immediately after the truth about Suite 11i became public, the revelation of the truth must have caused the price drop. Id. In affirming summary judgment for Oracle, we explained that the "overwhelming evidence produced during discovery indicate[d] the market understood Oracle's earnings miss to be a result of several deals lost in the final weeks of the quarter due to customer concern over the declining economy," not the alleged Suite 11i fraud. Id. at 393.

Another wrinkle here is whether loss causation allegations can survive a motion to dismiss even when the stock price drop did not immediately follow the

revelation of the misstatement. In *In re Gilead*, the market learned in August 2003 that Gilead had aggressively marketed a drug by claiming that the company had "carefully complied with federal and state regulations" when, in fact, a warning letter from the Food and Drug Administration had informed Gilead that its marketing claims were unlawful. 536 F.3d at 1051. Gilead's stock price did not drop until October 2003, following a press release revealing "less-thanexpected revenues." Id. at 1054, 1058. Despite the time gap between the revelation and the stock price drop, the shareholders claimed that Gilead's misrepresentations caused its stock price to inflate, and the subsequent disappointing revenue performance and stock price drop sufficed to plead loss causation. *Id.* at 1056.

Acknowledging the time gap, we held that the shareholders adequately pleaded loss causation and reiterated that there is no "bright-line rule requiring an immediate market reaction" after a revelation because "[t]he market is subject to distortions that prevent the ideal of a free and open public market from occurring." Id. at 1057–58 (alteration in original) (citation omitted). Accordingly, the shareholders plausibly alleged that Gilead's stock price drop occurred immediately after the company revealed its disappointing revenue numbers, and the drop was caused by lower demand resulting from the warning letters. Id. As we explained, it was reasonable for the public to fail to appreciate the significance of the warning letters until learning of Gilead's disappointing revenue posting. Id. Aligning ourselves with the Second and Third Circuits, we concluded that "loss causation is a matter of proof at trial" so "it is normally inappropriate to rule on loss causation at the pleading stage." *Id*. at 1057 (quoting Emergent Cap. Inv. Mgmt., LLC v.

Stonepath Grp., Inc., 343 F.3d 189, 197 (2d Cir. 2003)); see also McCabe v. Ernst & Young, LLP, 494 F.3d 418, 427 n.4 (3d Cir. 2007). Because the shareholders pleaded sufficient facts to raise a reasonable expectation that discovery would reveal evidence of the warning letter's "effect on demand," the loss causation claim survived Gilead's motion to dismiss. In re Gilead, 536 F.3d at 1058.

For Facebook's July 2018 stock price drop to be actionable, it must be because Facebook's earnings report revealed new information to the market; specifically, that Facebook's Q2 earnings call in July 2018 allowed the public to "appreciate [the] significance" of the Cambridge Analytica and whitelisting scandals. *Id.* The disappointing Q2 earnings performance alone cannot satisfy the shareholders' burden of pleading loss causation.

Here, as in *In re Gilead*, the shareholders adequately pleaded that the Cambridge Analytica and whitelisting revelations, not any other factor, caused the July 2018 stock price drop. Although the stock drop occurred nearly two months after the whitelisting revelation, the shareholders sufficiently allege that the drop was caused by "dramatically lowered user engagement, substantially decreased advertising revenue and earnings, and reduced growth expectations going forward" on account of the Cambridge Analytica and whitelisting scandals. The shareholders further detail how the GDPR rollout had little impact on the July 2018 earnings report, and how investors and market analysts explicitly connected the revenue drop to the scandals. These allegations suffice to plead "a causal relationship" between the Cambridge Analytica and whitelisting revelations and the dramatic drop in Facebook's stock price. *Id.* at 1057. We emphasize that this case is at the very early motion to dismiss stage, that the shareholders have raised "a reasonable expectation that discovery will reveal evidence" of loss causation, *id.* (quoting *Twombly*, 550 U.S. at 556), and that discovery and further proceedings are necessary to illuminate the issues surrounding loss causation.

Our dissenting colleague would affirm the district court's dismissal of the user control statements as they relate to the Cambridge Analytica revelation. Stated differently, the dissent would hold that only the July 2018 stock price drop was actionable, and only as to the whitelisting revelation, not the Cambridge Analytica revelation.

In support, the dissent contends that the 2018 "Cambridge Analytica disclosures did not make the user control statements materially false," because "Cambridge Analytica's lies to Facebook and its continued violation of Facebook's privacy policies do not mean that Facebook's privacy protections do not actually exist." But the question is not whether and when Cambridge Analytica lied to Facebook, but whether and when Facebook learned of Cambridge Analytica's deception. It is true that in January 2016, Cambridge Analytica agreed to delete the personality score data it harvested from Facebook. But recall that the shareholders pleaded that Facebook had reason to know in June 2016—only five months later—that Cambridge Analytica had received much more information from Facebook than just the personality score data and that Cambridge Analytica was still using a model based on the data in violation of Facebook's policies. The shareholders further allege that when Facebook found out, it tried to require Cambridge Analytica's CEO to certify that all data harvested from the personality quiz was deleted, but the CEO refused to do so. Thus, the shareholders pleaded with particularity that Facebook knew Cambridge Analytica did not delete all the data it had improperly accessed.

We agree with the dissent that "a supposed bad actor violating Facebook's privacy controls to improperly access user data doesn't make the company's statements about its policies misleading." But labeling Cambridge Analytica as a "bad actor" is not the issue. It was not Cambridge Analytica's deception that made Facebook's user control statements misleading. Rather, it was that Facebook knew Cambridge Analytica retained access to improperly collected user data after Cambridge Analytica certified that it had deleted the personality score data, and Facebook nonetheless falsely represented to users that they had control over their data on the platform. The shareholders adequately pleaded loss causation as to the stock price drops that occurred after the Cambridge Analytica revelation in March and July 2018. Accordingly, we reverse the district court's dismissal of Facebook's statements regarding data control that predated the June 3, 2018, whitelisting revelation.

## III. CONCLUSION

We affirm in part and reverse in part as to dismissal based on the risk statements and user control statements, and we affirm as to dismissal based on the Cambridge Analytica investigation statements. Specifically, we affirm the dismissal of the statements in  $\P 503-05$ , 530, 533, and 537-38 of the Third Amended Complaint, reverse the district court's dismissal of the statements in  $\P 501-02$ , 507-14, 519, and 525, and remand for further proceedings. Each party shall bear its own costs.

AFFIRMED IN PART, REVERSED IN PART, AND REMANDED IN PART.

BUMATAY, J., concurring in part and dissenting in part:

At issue here are three general categories of alleged false statements: (1) statements about Facebook's risk factors, (2) statements about Facebook's investigation of Cambridge Analytica, and (3) statements about Facebook users' control over their data. I join the majority in holding that the plaintiff Shareholders failed to sufficiently allege a falsity in the second category—Facebook's Cambridge Analytica investigation statements. I also join the majority in holding that Shareholders *did* allege a falsity and loss from the third category of user control statements—but only as those statements relate to Facebook's practice of "whitelisting."

So I disagree with the majority on two fundamental points. First, Shareholders failed to sufficiently allege that Facebook's risk factor statements in its public filings were fraudulent. Second, Shareholders didn't show that Facebook's user control statements were false based on the Cambridge Analytica revelations. I briefly set out my disagreement below.

I.

## **Risk Factor Statements**

Federal securities law creates no "affirmative duty to disclose any and all material information." *Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. 27, 44 (2011). Rather, companies must disclose information "only when necessary 'to make . . . statements made, in light of the circumstances under which they were made, not misleading." *Id.* (quoting 17 CFR § 240.10b–5(b)). Thus, companies "can control what they have to disclose . . . by controlling what they say to the market." *Id.* at 45.

Indeed, companies have no "obligation to offer an instantaneous update of every internal" or "fleeting" development. Weston Fam. P'ship LLLP v. Twitter, Inc., 29 F.4th 611, 620 (9th Cir. 2022). Instead, a "company must disclose a negative internal development only if its omission would make other statements materially misleading." Id. Put differently, statements and omissions are actionable only if they "directly contradict what the defendant knew at that time," Khoja v. Orexigen Therapeutics, Inc., 899 F.3d 988, 1008 (9th Cir. 2018), or "create an impression of a state of affairs that differs in a material way from the one that actually exists," Brody v. Transitional Hosps. Corp., 280 F.3d 997, 1006 (9th Cir. 2002). In assessing this question, we look to the "total mix" of information available to the reasonable investor and whether the alleged misstatement "significantly altered" the decisionmaking of the reasonable investor. Retail Wholesale & Dep't Store Union Loc. 338 Ret. Fund v. Hewlett-Packard Co., 845 F.3d 1268, 1274 (9th Cir. 2017) (simplified); see also In re Syntex Corp. Sec. Litig., 95 F.3d 922, 929 (9th Cir. 1996) (requiring evaluation of the "statement in full and in context at the time it was made").

Shareholders' allegations stem from Facebook's 2016 SEC Form 10-K "Risk Factors" statements, dated February 3, 2017. Facebook made these statements in the context of the following bolded headline:

"Security breaches and improper access to or disclosure of our data or user data, or other hacking and phishing attacks on our systems, could harm our reputation and adversely affect our business."

Under that header, Facebook gave these warnings:

- "Any failure to prevent or mitigate security breaches and improper access to or disclosure of our data or user data could result in the loss or misuse of such data, which could harm our business and reputation and diminish our competitive position."
- "We provide limited information to ...
  third parties based on the scope of services provided to us. However, if these
  third parties or developers fail to adopt or
  adhere to adequate data security practices ... our data or our users' data may
  be improperly accessed, used, or disclosed."

Shareholders argue—and the majority agrees—that all three of these statements are misleading because, by February 2017, Facebook already knew that Cambridge Analytica had gained improper access to the data of tens of millions of Facebook users. According to the majority, this means that the statements directly contradicted what the company knew when it filed its 10-K.

There's a problem with this analysis. Even if Facebook knew about the full extent of the so-called Cambridge Analytica scandal at this point, none of this makes the risk factor statements false. Recall the facts of the scandal. In 2015, Facebook became aware that Cambridge Analytica—through a consulting academic—had developed a personality quiz that harvested data from more than thirty million Facebook users, often without the users' consent. This quiz gave Cambridge Analytica access to Facebook users' name, gender, location, birthdate, "likes," and "friends," which made it possible to develop an algorithm to sort

Facebook users according to personality traits. Cambridge Analytica then allegedly used that algorithm to help political campaigns.

Regardless of the severity of Cambridge Analytica's alleged misconduct, a careful reading of the 10-K statements shows that these risk factor statements warn about harm to Facebook's "business" and "reputation" that "could" materialize based on improper access to Facebook users' data—not about the occurrence or non-occurrence of data breaches. How do we know that? Well, the statements say so. The first and second statements expressly advise that improper breaches "could harm" Facebook's "business" and "reputation."

And although the third statement does not expressly mention business and reputational harm, we know that is its focus for two reasons. First, Facebook reported the statement under the bolded section about breaches and improper actions "could harm [Facebook's] reputation and adversely affect our business." Second, the very next sentence places that statement into more context: "Affected users or government authorities could initiate legal or regulatory actions against us in connection with any security breaches or improper disclosure of data, which could cause us to incur significant expense and liability or result in orders or consent decrees forcing us to modify our business practices."

Taken together, Facebook's risk factor statements warn about harm to its "reputation" and "business" that *may* come to light if the public or the government learns about improper access to its data. These statements do not represent that Facebook was free from significant breaches at the time of the filing. And if a reasonable investor thought so based on Facebook's

10-K statements, that "reasonable" investor wasn't acting so reasonably. Indeed, within the same section, Facebook warned that "computer malware, viruses, social engineering (predominantly spear phishing attacks), and general hacking have become more prevalent in our industry, have occurred on our systems in the past, and will occur on our systems in the future." Facebook expressly advised that it experienced previous attempts to swipe its data and that it would continue to face such threats. Beyond Facebook's own statements, much about the Cambridge Analytica scandal was already public. In a December 2015 article, The Guardian reported that Cambridge Analytica had harvested data from "tens of millions" of Facebook users "without their permission." These are the same facts Shareholders use to claim Facebook deceived the public with more than two years later.

So, on their face, none of the 10-K risk factor statements are false or misleading. The statements advise that improper access to data *could* harm Facebook's reputation and business. And Shareholders have not sufficiently alleged that Facebook knew its reputation and business were *already* harmed at the time of the filing of the 10-K. Nor do they allege that Facebook was aware of government entities or users launching regulatory or legal actions based on the Cambridge Analytica scandal in February 2017.

While acknowledging these shortcomings in the Shareholders' complaint, the majority takes the sur-

<sup>&</sup>lt;sup>1</sup> See Harry Davies, Ted Cruz Using Firm that Harvested Data on Millions of Unwitting Facebook Users, The Guardian (Dec. 11, 2015), https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data.

prisingly broad view that it's irrelevant that "Facebook did not know whether its reputation was ... harmed" at the time of the 10-K filing. Maj. Op. 25. The majority instead asserts that it's enough that a breach had occurred, never mind whether the breach led to a discernible effect on Facebook's reputation or business at the time. *Id*. The majority goes so far as to say that a fraud occurs even if the harm caused by the breach was completely "unknown" to Facebook. Id. But if it was "unknown" whether the breach led to reputational or business harm, it's hard to see how the risk factor statements were untrue. Stating that harm could result from a breach is not falsified by some "unknown" possibility of harm from a breach. In other words. Facebook's risk factor statements could not "directly contradict what the defendant knew at that time" if any harm was unknown to Facebook at the time. Khoja, 899 F.3d at 1008.2

And *In re Alphabet, Inc. Securities Litigation*, 1 F.4th 687 (9th Cir. 2021), doesn't transform every risk statement into a false or misleading statement if a risk later comes to fruition. Nor does it create a new requirement that a company disclose every bad thing

<sup>&</sup>lt;sup>2</sup> Given the majority's analysis of these statements, it's difficult to see how Shareholders can ever satisfy the scienter requirement. Indeed, "[a] complaint will survive . . . only if a reasonable person would deem the inference of scienter cogent and at least as compelling as any opposing inference one could draw from the facts alleged." *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 324 (2007). Such a strong inference requires an "intent to deceive, manipulate, or defraud," or "deliberate recklessness"—which is "an *extreme* departure from the standards of ordinary care." *Schueneman v. Arena Pharmaceuticals, Inc.*, 840 F.3d 698, 705 (9th Cir. 2016). If the harm from Cambridge Analytica's breach was unknown at the time of the filing of the 10-K, it's doubtful this standard can be met.

that ever happened to it. In that case, Alphabet stated in two quarterly disclosure forms that certain risks "could adversely affect our business, financial condition, [and] results of operations," but that "[t]here have been no material changes to our risk factors since our [last] Annual Report on Form 10-K." 1 F.4th at 696 (simplified). What Alphabet didn't disclose is that, before the reports came out, its internal Google investigators had discovered a software glitch in one of its programs that allowed third parties to collect users' private data. Id. at 695. Google's legal and policy staff quickly recognized the problem and warned in an internal memorandum that these security issues would likely trigger an immediate regulatory response and cause its senior executives to testify before Congress. Id. at 696. When news inevitably broke six months later, Alphabet's shares plummeted in value and, sure enough, there were calls for government investigation. Id. at 697. We concluded that "[r]isk disclosures that speak entirely of as-yet-unrealized risks and contingencies and do not alert the reader that some of these risks may already have come to fruition can mislead reasonable investors." Id. at 703 (simplified). In Alphabet's case, the "warning in each [quarterly report] of risks that 'could' or 'may' occur [was] misleading to a reasonable investor [because] Alphabet knew that those risks had materialized." Id. at 704.

Contrary to the majority's assertion, this case is nothing like *Alphabet*. In *Alphabet*, the company knew a risk had come to fruition—set out as clear as day in an internal company memo—that a data bug would cause it greater regulatory scrutiny. *Id.* at 696. Rather than disclose its assessment, Alphabet chose to bury it and even stated that no material changes existed in its risk factors. *Id.* at 696–97, 703. Here,

Facebook might have known of breaches of its data even potentially serious breaches—when it gave its risk statements, but Shareholders don't allege that Facebook knew that those breaches would lead to immediate harm to its business or reputation. As the majority concedes, the harm from Cambridge Analytica's breach of Facebook's policies was "unknown" at the time of the 10-K filing. See Maj. Op. 25. Nor did Facebook lull investors into complacency by suggesting that nothing had changed on its risks front. These facts make all the difference here. Cf. Weston, 29 F.4th at 621 (dismissing fraud claims alleging that Twitter's risk warning statement—that its "product and services may contain undetected software errors, which could harm our business and operating results"—was misleading because the risk had materialized by then).

Because Facebook did not present false or misleading risk statements, and *Alphabet* did not modify a common-sense understanding of truthfulness and disclosure, we should have affirmed the dismissal of this claim.

## II.

## **User Control Statements**

The next category of alleged falsehoods concerns Facebook's representations that users control their data and information. During the relevant period for this lawsuit, Facebook and its executives made various statements emphasizing users' control over the data they shared with Facebook, such as—

"You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings." Facebook's

Statement of Rights and Responsibilities web page, ~ January 30, 2015 to May 25, 2018.

- "[W]hen you share on Facebook you need to know No one is going to get your data that shouldn't have it. That we're not going to make money in ways that you would feel uncomfortable with off your data. And that you're controlling who you share with. . . . Privacy for us is making sure that you feel secure, sharing on Facebook." Sheryl Sandberg, *Axios* interview, October 12, 2017.
- "Our apps have long been focused on giving people transparency and control...."
  Sheryl Sandberg, Facebook Gather Conference, January 23, 2018.

#### A.

Shareholders have adequately shown that these statements were misleading based on the allegation that Facebook "whitelisted" third parties. According to the Shareholders, at the same time these statements were made, Facebook continued to allow certain "whitelisted" third parties, mostly app developers and device manufacturers, to continue to access data against a user's wishes. Shareholders allege that Facebook overrode user privacy settings to allow these third parties access to the data of, not only the Facebook user, but that of the user's friends as well. In fact, Facebook paid the Federal Trade Commission \$5 billion to settle charges stemming from the "whitelisting" allegations.

These facts are enough to plead that the statements were false—the only question is whether the

statements caused Shareholders any loss. See Grigsby v. BofI Holding, Inc., 979 F.3d 1198, 1204 (9th Cir. 2020) (explaining that "investors must demonstrate that the defendant's deceptive conduct caused their claimed economic loss") (simplified). Facebook's "whitelisting" program became public on June 3, 2018, when the New York Times reported that Facebook shared users' and their friends' data with multiple "whitelisted" companies. When it comes to false statements, a plaintiff can usually show loss causation by pointing to an immediate stock drop after the falsity was uncovered. Id. at 1205 ("A plaintiff can satisfy the loss-causation pleading burden by alleging that a corrective disclosure revealed the truth of a defendant's misrepresentation and thereby caused the company's stock price to drop and investors to lose money.") (simplified). The wrinkle here is that Facebook's stock didn't drop immediately after the whitelisting became public. It wasn't until several weeks later—July 26, 2018, the day after Facebook announced slower growth than expected—that Facebook's stock dropped by almost 19%. Facebook contends that this temporal gap proves that its misleading user control statements didn't cause Shareholders any loss.

But sometimes it takes time for the full scope of a loss from a misrepresentation to materialize. As *In re Gilead Sciences Securities Litigation*, 536 F.3d 1049, 1058 (9th Cir. 2008) recognized, a "limited temporal gap between the time a misrepresentation is publicly revealed and the subsequent decline in stock value does not render a plaintiff's theory of loss causation per se implausible." Indeed, in that case, three months had passed between the disclosure of Gilead's alleged deceptive marketing practices and the stock drop after Gilead missed revenue targets. *Id.* at 1057–58. De-

spite this gap, we concluded the plaintiffs had plausibly alleged that the less-than-expected revenue was caused by lower end-user demand, which, in turn, was caused by disclosing the company's deceptive marketing. *Id.* at 1058. Thus, an "immediate market reaction" is not necessary when the market might "fail[] to appreciate [the] significance" of a disclosure right away. *Id.* at 1057–58.

So, we shouldn't be too quick to dismiss a claim based on a delay in the manifestation of loss. In my view, it's plausible that the whitelisting revelation made on June 18 caused user engagement and advertising revenue to diminish, which contributed to the lower earnings announced on July 25 and the immediate stock drop. Facebook counters that the European Union's new privacy regulations—not the whitelisting revelation—caused the lower July 25 earnings. That might be right. But, at the very least, Shareholders deserve some discovery to prove their theory of loss causation.

## В.

But the analysis of the user control statement must be different when it comes to the Cambridge Analytica scandal. Shareholders allege—and the majority agrees—that new revelations about Cambridge Analytica from March 2018 also proved Facebook's user control statements were false. As a reminder, in late 2015, Facebook discovered that Cambridge Analytica obtained personality score data harvested from Facebook data and demanded that Cambridge Analytica delete all such data. In response, Cambridge Analytica certified to Facebook that it would delete the data. On March 16, 2018, Facebook announced that it had received reports from the media that Cambridge

Analytica did not destroy the data and that it was suspending Cambridge Analytica from the platform. News reports then confirmed that Cambridge Analytica continued to possess and use harvested data from Facebook. Within a week of these disclosures, Facebook's shares dropped nearly 18%. Shareholders contend that these revelations prove the falsity of Facebook's user control statements.

These Cambridge Analytica disclosures did not make the user control statements materially false. To prevail, Shareholders must show that the Facebook user control statements "affirmatively create[d] an impression of a state of affairs that differ[ed] in a material way from the one that actually exist[ed]." *Brody*, 280 F.3d at 1006. But Cambridge Analytica's lies to Facebook and its continued violation of Facebook's privacy policies do not mean that Facebook's privacy protections do not actually exist. Aside from the whitelisting issue described above, Facebook seemingly described its privacy policies accurately. Cambridge Analytica's violation of those policies doesn't falsify them.

Imagine a bank. Say that the bank announces a range of security measures to protect its customers' money. Then consider if a bank robber defeats those measures, breaks in, and ultimately steals a bag of cash. Would anyone say that the bank lied about its security measures? Clearly, no. Here, a supposed bad actor violating Facebook's privacy controls to improperly access user data doesn't make the company's statements about its policies misleading.

What makes our ruling all the more odd is that much of the Cambridge Analytica scandal was already public by the time of the user control statements. The first article about it dropped in 2015. So it's hard to see how this new "revelation" added to the "total mix" of information available to Shareholders or "significantly altered" their decision-making. See Retail Wholesale & Dep't Store Union Loc. 338 Ret. Fund, 845 F.3d at 1274. We thus should have limited Facebook's liability for the user control statements to the "whitelisting" allegations.

## III.

For these reasons, I respectfully dissent from Part II.A of the majority opinion, from Part II.C as it relates to Cambridge Analytica, and from Part III.

#### APPENDIX C

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

IN RE

FACEBOOK, INC. SECURITIES LITIGATION Case No. 5:18-cv-01725-EJD

ORDER GRANTING DEFENDANTS' MOTION TO DISMISS THIRD AMENDED COMPLAINT WITHOUT LEAVE TO AMEND

Re: Dkt. No. 145

Dec. 20, 2021

Before the Court is Defendants' motion to dismiss Plaintiffs' third amended complaint. Plaintiffs are person who purchased shares of Facebook common stock between February 3, 2017 and July 25, 2018 ("the Class Period"), who believe that Defendant Facebook, Inc. and Executive Defendants Mark Zuckerberg, Sheryl K. Sandberg, and David W. Wehner made materially false and misleading statements and omissions in connection with the purchase and sale of Facebook stock. See Third Amended Complaint ("TAC") ¶ 1, Dkt. No. 142. Plaintiffs allege that Defendants violated Section 10(b), 20(a), and 20A of the Securities Exchange Act of 1934 (the "Exchange Act") and Rule 10b-5 promulgated thereunder because Defendants made guarantees that users had control over the sharing of their user data, while knowing that to not be true because of the Cambridge Analytica data breach and the practice of "whitelisting" certain applications. TAC ¶ 1 (focusing on Defendants' statements and omissions concerning Facebook's "privacy and data protection practices").

Defendants have filed a motion to dismiss, arguing that Plaintiffs have failed for a third time to meet Federal Rule of Civil Procedure 9(b)'s heightened pleading requirements for securities fraud. The Court agrees. Plaintiffs have failed to remedy the problems identified by the Court in its prior dismissal order. See Order Granting Defendants' Motion to Dismiss with Leave to Amend ("August 2020 Order"), Dkt. No. 137. The Court therefore **GRANTS** Defendants' motion to dismiss **without leave to amend.** 

## I. BACKGROUND

Rather than repeat the background of this case for a third time, the Court refers the Parties to its prior orders. To the extent the Parties ask the Court to alter its previous rulings, the Court declines and **AF-FIRMS** those rulings herein.

On October 15, 2018, Plaintiffs filed their Consolidated Class Action Complaint. See Dkt. No. 86. On September 25, 2019, this Court granted Defendants' motion to dismiss the consolidated complaint after finding that Plaintiffs had failed to carry their burden to plead falsity and scienter. The Court did not address reliance or loss causation in that order. Order Granting Defendants' Motion to Dismiss, Dkt. No. 118.

Plaintiffs filed their second amended complaint on November 15, 2019. See Dkt. No. 123 ("SAC"). On August 7, 2020, this Court again granted Defendants' motion to dismiss the complaint after finding that Plaintiffs failed to carry their burden to plead falsity, scienter, and loss causation. August 2020 Order. This

Court gave Plaintiffs one last opportunity to cure the deficiencies identified by the Court.

On October 16, 2020, Plaintiffs filed their third amended complaint. Defendants moved to dismiss the third amended complaint on December 18, 2020. Motion to Dismiss Third Amended Class Action Complaint ("Mot."), Dkt. No. 145. Plaintiffs filed an opposition. Lead Plaintiffs' Memorandum of Points and Authorities in Opposition ("Opp."), Dkt. No. 153. Defendants then filed a reply. Reply in Support of Defendants' Motion to Dismiss ("Reply"), Dkt. No. 158. On September 30, 2021, this Court granted Defendants' motion to strike portions of Plaintiffs' third amended complaint. See Dkt. No. 166. Pursuant to that order, this Court will not consider Dr. Cain's opinions set forth in paragraphs 722 through 724 of the TAC and any other portions of the TAC that rely on those opinions.

## II. DISCUSSION

## A. Legal Standard

To survive a Rule 12(b)(6) motion to dismiss, a complaint must contain sufficient factual matter to "state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009); Fed. R. Civ. Pro. 8(a). Threadbare recitals of the elements of a cause of action supported by mere conclusory statements do not suffice. *Ashcroft*, 556 U.S. at 678.

To show securities fraud under Section 10(b) and Rule 10b-5, plaintiffs must allege facts sufficient to establish (1) a material misrepresentation or omission, (2) made with scienter, *i.e.*, a wrongful state of mind, (3) a connection between the misrepresentation and the purchase or sale of a security; (4) reliance upon the

misrepresentation; (5) economic loss; and (6) loss causation. Loss v. Immersion Corp., 762 F.3d 880 (9th Cir. 2014), amended (Sept. 11, 2014). "To determine whether a private securities fraud complaint can survive a motion to dismiss for failure to state a claim, the court must determine whether particular facts in the complaint, taken as a whole, raise a strong inference that defendants intentionally or with deliberate recklessness made false or misleading statements to investors." In re LeapFrog Enter., Inc. Sec. Litig., 527 F. Supp. 2d 1033, 1039–40 (N.D. Cal. 2007).

The pleading standard in securities fraud cases is heightened. Complaints alleging securities fraud must meet the plausibility standard, the Private Securities Litigation Reform Act ("PSLRA"), and Federal Rule of Civil Procedure 9(b)'s higher pleading standard. See Tellabs, Inc. v. Makor Issues & Rights, Ltd., 551 U.S. 308, 319–22 (2007); Zucco Partners, LLC v. Digimarc, Corp., 552 F.3d 981, 991 (9th Cir. 2009). The PSLRA mandates that securities fraud complaints (1) specify each misleading statement, (2) set forth the facts "on which [a] belief" that a statement was misleading was "formed," (3) and "state with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind [i.e., scienter]." Dura Pharm., Inc. v. Broudo, 544 U.S. 336, 345 (2005) (quoting 15 U.S.C. §§ 78u–4(b)(1)–(2)). Plaintiffs bear the burden of proving that the defendant's misrepresentations "caused the loss for which the plaintiff seeks to recover." Id. In determining whether a "strong inference" of scienter has been sufficiently alleged, this Court must not only draw "inferences urged by the plaintiff," but must also engage in a "comparative evaluation," and examine and consider "competing inferences [in defendants' favor] drawn from the facts alleged." Tellabs, 551 U.S. at 314.

Hence, scienter must not only be "plausible or reasonable," it must also be "cogent or at least as compelling as any opposing inference of nonfraudulent intent." *Id.* at 324. Federal Rule of Civil Procedure 9(b) further requires a plaintiff pleading securities fraud to state, with particularity, the circumstances constituting fraud or mistake.

## B. Defendants' Motion to Dismiss

In their motion to dismiss, Defendants argue that Plaintiffs have not remedied the problems identified by the Court in its earlier orders.

In its August 2020 order, this Court identified two theories of securities fraud in Plaintiffs' SAC. First, Plaintiffs alleged that Executive Defendants knowingly made misleading statements regarding the Cambridge Analytica data breach. Plaintiffs argued that Executive Defendants knowingly made false statements regarding the Cambridge Analytica breach because Facebook knew Cambridge Analytica was still misusing the misappropriated data. This Court held that Plaintiffs had failed to allege falsity because the complaint indicated that Cambridge Analytica and Mr. Kogan certified to Facebook that they had deleted the misappropriated data and Plaintiffs had not shown a reason why Executive Defendants would know that the deletion certifications were false. Second, Plaintiffs alleged that Executive Defendants knowingly made misleading statements that users had complete control over their data. Plaintiffs maintained that these statements were false because of Facebook's whitelisting practice, a data-sharing reciprocity practice for certain "whitelisted applications" that was organized by Executive Defendants. The Court agreed that Plaintiffs had demonstrated falsity,

scienter, and reliance as to this theory of fraud, but held that Plaintiffs had failed to plead loss causation.

The Court must again dismiss Plaintiffs' two theories of securities fraud. While the amended complaint alleges that Facebook "embedded" employees in the Trump campaign, there are no allegations that demonstrate the employees knew that misappropriated data was being used or that the employees reported the misuse to Executive Defendants. Additionally, the amended complaint does not demonstrate loss causation as to the whitelisting theory of fraud. Because Plaintiffs have not cured the problems identified in this Court's August 2020 Order, the Court **GRANTS** Defendants' motion to dismiss Plaintiffs' third amended complaint **without leave to amend.** 

## C. Discussion

# 1. The Cambridge Analytica Data Breach

As discussed in the August 2020 Order, Plaintiffs argue that Executive Defendants made false or misleading statements about (1) the risks facing Facebook after the Cambridge Analytica data breach and (2) the results of Facebook's investigation into Cambridge Analytica's work on the Brexit and Trump campaigns. TAC ¶¶ 298–309. This Court previously determined that this theory of security fraud fails because at the time these statements were made, Facebook had reason to believe that Cambridge Analytica and Alexander Kogan had deleted the misappropriated data and that the misappropriated data was no longer being misused. See August 2020 Order at 33–35, 43. The Court determined that for Plaintiffs to cure this theory, they must demonstrate that Executive De-

fendants knew or should have known these certifications were false by "alleging, among other things, that Facebook "embedded" employees in the 2016 Trump campaign and thus knew that the deletion certifications were false." August 2020 Order at 66.

Like the SAC, Plaintiffs allege that Facebook made materially false and misleading statements about the risks facing the company by stating that business and reputation harm *could* occur if a third party were to improperly access and use sensitive user data. Plaintiffs allege that these "risk factor" statements were false when made because Cambridge Analytica was already using misappropriated user data. TAC ¶¶ 335–40. Plaintiffs also allege that Facebook misleadingly stated in March 2017 that its "investigation to date ha[d] not uncovered anything that suggests wrongdoing with respect to Cambridge Analytica's work on the [Brexit] and Trump campaigns." TAC ¶ 299. Plaintiffs maintain that these statements were false when made because Facebook had "embedded" employees in the two respective campaigns and thus Executive Defendants knew or should have known that the misappropriated data was still being misused and that Facebook was presently facing risks due to the continued use of misappropriated data. TAC ¶¶ 238–44.

## a. Legal Standard

As discussed above, to state a claim under Section 10(b) and Rule 10b-5, a complaint must plausibly allege: "(1) a material misrepresentation or omission by the defendant; (2) scienter; (3) a connection between the misrepresentation or omission and the purchase or sale of a security; (4) reliance upon the misrepresentation or omission; (5) economic loss; and (6) loss causation." *Halliburton Co. v. Erica P. John Fund*,

*Inc.*, 573 U.S. 258, 267 (2014) (citations omitted). A complaint must "satisfy the dual pleading requirements of Federal Rule of Civil Procedure 9(b) and the PSLRA" to state a securities fraud claim. Zucco Partners, 552 F.3d at 990. Federal Rule of Civil Procedure 9(b) requires a plaintiff to "state with particularity the circumstances constituting fraud," and the PSLRA extends this particularity requirement to allegations of scienter. See 15 U.S.C. § 78u-4(b)(2)(A) ("[T]he complaint shall, with respect to each act or omission alleged . . . , state with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind."); see also Kearns v. Ford Motor Co., 567 F.3d 1120, 1124 (9th Cir. 2009) ("Averments of fraud must be accompanied by the who, what, when, where, and how of the misconduct alleged." (citations and quotation marks omitted)).

To support a "strong inference" of scienter under the PSLRA, a complaint must allege that the defendant made false or misleading statements with an "intent to deceive, manipulate, or defraud" or with deliberate recklessness. City of Dearborn Heights Act 345 Police & Fire Ret. Sys. v. Align Tech., Inc., 856 F.3d 605, 619 (9th Cir. 2017) (citation omitted). Deliberate recklessness is an "extreme departure from the standards of ordinary care . . . which presents a danger of misleading buyers or sellers that is either known to the defendant or is so *obvious* that the actor must have been aware of it." Schueneman v. Arena Pharms., Inc., 840 F.3d 698, 705 (9th Cir. 2016). The "strong inference" standard "present[s] no small hurdle for the securities fraud plaintiff." Id. (citation omitted). When determining whether Plaintiff has alleged a "strong inference" of scienter, this court must "engage in a comparative evaluation [and] . . . consider, not only inferences urged by the plaintiff . . . but also competing

inferences rationally drawn from the facts alleged." *Tellabs*, 551 U.S. at 314. A complaint will survive a motion to dismiss "only if a reasonable person would deem the inference of scienter cogent and at least as compelling as any opposing inference one could draw from the facts alleged." *Id.* at 324.

## b. Analysis

In its August 2020 Order, this Court directed Plaintiffs to plead "specific facts" showing that Defendants knew that GSR and Cambridge Analytica did not delete the relevant data or that Defendants should have known that the misappropriated data was not deleted. August 2020 Order at 35, 43–44. Plaintiffs attempt to meet this burden by alleging that because three Facebook employees worked with Cambridge Analytica on the Trump campaign, Executive Defendants knew or should have known that Cambridge Analytica continued to use the misappropriated data.

To accept Plaintiffs' theory of knowledge, this Court would have to find:

- The three employees "embedded" in the Trump campaign knew the contents of Cambridge Analytica's deletion certifications, even though those certifications were provided to other employees in another department more than six months earlier. TAC ¶ 32 (alleging in December 2017, Facebook had 25,105 employees).
- These three employees saw the "psychographic stuff" that was allegedly derived from the misappropriated data because they were "seated next to" Cambridge Analytica employees. TAC ¶ 235.

- After seeing the "psychographic stuff," the employees would have known that Cambridge Analytica was still using the misappropriated data, despite its certifications to the contrary. TAC ¶ 237 ("Thus, when they saw and heard discussions about 'psychographics,' they would have known Cambridge Analytica was still using the misappropriated data that violated Facebook's policies.").
- Once the employees figured out that Cambridge Analytica was still misusing the data, they would have reported Cambridge Analytica's wrongdoing up the chain to the Executive Defendants. TAC ¶¶ 273, 281 (alleging that top management knew about the "embedded" employees).

Problematically, the TAC pleads no facts (1) that the "embedded" employees knew that Cambridge Analytica had certified it was no longer using the misappropriated data and thus would have been alerted to the problematic nature of its use, (2) that the employees alerted Executive Defendants about any use of misappropriated data by the Trump campaign, or (3) that at the time the employees were "embedded" in the campaign, the Executive Defendants knew that Cambridge Analytica was working on a "gigantic dataset" such that they should have known that the deletion certifications were false. Plaintiffs' general allegations that the "embedded" employees "would have" known about the violations, that they "would have" reported the violations, or that Executive Defendants "would have" known about Cambridge Analytica's data use are too speculative and fail to demonstrate actual knowledge. See Metzler Inv. GMBH v. Corinthian Colls., Inc., 540 F.3d 1049, 1068 (9th Cir. 2008)

("[C]orporate management's general awareness of the day-to-day workings of the company's business does not establish scienter—at least absent some additional allegations of specific information conveyed to management and related to the fraud."); see also In re Northpoint Comme'ns Grp., Inc. Sec. Litig., 184 F. Supp. 2d 991, 1005 (N.D. Cal. 2001) ("The PSLRA clearly establishes a preference for facts over such inferential leaps.").

Plaintiffs attempt to show knowledge by alleging facts about an "investigation team" employed by Facebook. See Opp. at 9–12 (alleging that Facebook's investigation team was aware of Cambridge Analytica's misuse of data and that the team collected "additional facts" that Cambridge Analytica was continuing to misuse the user data). First, Plaintiffs claim that Executive Defendants were "involved in discussions" regarding the "Cambridge Analytica investigation," Opp. at 8, but the paragraphs of the TAC identified only speculate about Executive Defendants role in the investigation and do not demonstrate that it was unreasonable for Executive Defendants to rely on the deletion certifications. See ¶¶ 35 (Defendant Sandberg is the Chief Operating Officer), 161–63 (detailing public relations response to the 2015 The Guardian article broke to demonstrate that Defendant Sandberg was included in this response and would have known about any investigation into Cambridge Analytica), 203–04 (testimony by Defendant Zuckerberg that Cambridge Analytica told Facebook that they had deleted the misappropriated data), 249 n.262 (testimony from Defendant Zuckerberg that Cambridge Analytica certified deletion in both an email and in a full legal contract), 268 (alleging that the investigation team reviewed and circulated an article in *The Washington Post* about Kogan's use of social media on campaigns).<sup>1</sup>

Second, Plaintiffs contend that the temporal proximity between a meeting involving the Executive Defendants and certain conservative political operatives on May 18, 2016 and the employee "embedding" demonstrates that the Executive Defendants knew about Cambridge Analytica's continued use of the misappropriated data. Opp. at 7–8. Yet, there are no allegations that demonstrate that Executive Defendants discussed Cambridge Analytica, its use of the misappropriated data, or any plot to "embed" employees to aid Cambridge Analytica with using the misappropriated data. Indeed, there are no allegations connecting Cambridge Analytica to this meeting. Instead, the complaint alleges that Executive Defendants engaged with the Trump campaign as to advertisements

<sup>&</sup>lt;sup>1</sup> The Court does not reach Plaintiffs' "red flag" theories of scienter. See Opp. at 11–16. Because Plaintiffs have not pled sufficient facts that connect Executive Defendants to the "embedded" employees, it is irrelevant whether the "embedded" employees should have known that Cambridge Analytica's use of Facebook User IDs, though publicly available, and filenames demonstrated that Cambridge Analytica had not deleted the misappropriated data. Opp. at 13. Further, the 2016 Cambridge Analytica presentation and the 2016 The Washington Post article cited by Plaintiff do not focus on Facebook's role in Cambridge Analytica's data use. On the contrary, the article does not even mention Facebook and Facebook's logo appears on just one slide in the presentation, alongside 11 other technology companies. See TAC ¶¶ 265, 269. Thus, that Facebook discussed the article is not enough to demonstrate that Executive Defendants extrapolated from the article that Cambridge Analytica was still misusing the data (and it seems unlikely that Mr. Kogan would publicly admit to such misuse). TAC ¶ 268.

and considered the campaign to be important for advertisement revenue. See TAC ¶¶ 188–92, 223 (Defendant Sandberg stated that "the 2016 election is a big deal in terms of ad spend."). Moreover, the temporal proximity between the meeting and the embedding, without more, does not establish scienter. See Yourish v. Cal. Amplifier, 191 F.3d 983, 997 (9th Cir. 1999) ("We have allowed the temporal proximity of an allegedly fraudulent statement or omission and a later disclosure to bolster a complaint, but we have never allowed the temporal proximity between the two, without more, does not create an inference that the earlier statements were fraudulent." (cleaned up)); see also Fecht v. Price Co., 70 F.3d 1078, 1083–84 (9th Cir. 1995).

Third, Plaintiffs argue that the Executive Defendants must have known that Cambridge Analytica continued to use the misappropriated data because the Trump campaign was a "big deal" to Facebook. Opp. at 8; TAC ¶¶ 180-81, 223. But general allegations about the Trump campaign being a big deal for advertisement revenue fails to show that Executive Defendants knew that Cambridge Analytica was continuing to use the misappropriated data to aid the Trump campaign. See Prodanova v. H.C. Wainwright & Co., LLC, 993 F.3d 1097, 1109 (9th Cir. 2021) ("[G]eneralized allegations fail to show that that [the defendant] had direct involvement in the [alleged falsity]."); Metzler, 540 F.3d at 1068. Further, to the extent Plaintiffs are pursuing a "core operations" theory to argue that the Trump campaign was of "such prominence that it would be absurd to suggest that management was without knowledge of the matter," S. Ferry LP, No. 2. v. Killinger, 542 F.3d 776, 786 (9th Cir. 2008), Plaintiffs still must allege facts that demonstrate that Executive Defendants knew about Cambridge Analytica's involvement in the Trump campaign (and its use of the misappropriated data). See Police Ret. Sys. of St. Louis v. Intuitive Surgical, Inc., 759 F.3d 1051, 1062 (9th Cir. 2014) ("Proof under [the core operations] theory is not easy. A plaintiff must produce either specific admissions by one or more corporate executives of detailed involvement in the minutia of a company's operations, such as data monitoring; or witness accounts demonstrating that executives had actual involvement in creating false reports." (citations omitted)); cf. In re Quality Sys., Inc. Sec. Litig., 865 F.3d 1130, 1145 (9th Cir. 2017) (holding that scienter adequately pled where complaint included multiple statements from confidential witnesses that established that members of executive-level management, including the defendants, had access to and used reports documenting sales declines).

Finally, Plaintiffs allege that in January 2016, Facebook learned "more facts showing serious, continuing policy violations and wrongdoing," regarding Cambridge Analytica's work on the Trump campaign. TAC ¶¶ 300–09; Opp. at 5–6. Plaintiffs argue that this demonstrates that Facebook knowingly made false statements that it had not uncovered any evidence of wrongdoing on the Trump campaign. TAC ¶¶ 301–02. Problematically, the speaker of this statement is not an individual defendant. See Galzer Cap. Mgmt., LP v. Magistri, 549 F.3d 736, 745 (9th Cir. 2008) (declining to adopt the theory of collective scienter and holding that the PSLRA requires a plaintiff to "plead scienter with respect to those individuals who actually made the false statements"). However, to the extent the speaker of this statement can be connected to the Executive Defendants, Plaintiffs have failed to connect Executive Defendants to the investigation into

Cambridge Analytica or show that Executive Defendants knew that Cambridge Analytica continued to use the misappropriated data. TAC ¶¶ 161–79 (outlining investigation but failing to allege that Executive Defendants learned that Cambridge Analytica had not deleted the misappropriated data). Without such allegations, Plaintiffs have not shown that Executive Defendants acted with knowledge or deliberate recklessness in certifying that Facebook had not uncovered any wrongdoing. Prodanova, 993 F.3d at 1108 ("The SAC pleads no facts alleging that [Defendant] knew about the Offering when he authored the Report. There is thus no factual basis for the allegation that he acted with knowledge or deliberate recklessness." (emphasis added)); see also Declaration of Brian M. Lutz, Dkt. No. 146 at Exhibit 7 ¶¶ 42–43 ("Facebook had no specific mechanism to summarize or report violations of its Platform Policy . . . . As a result, Facebook senior management and relevant legal staff did not assess the scope, business impact, or legal implications of the researcher's improper transfer of data to Cambridge[.]" (emphasis added)).<sup>2</sup>

Accordingly, Plaintiffs have failed to establish that Defendants knew that Cambridge Analytica was using the misappropriated data *after* Facebook obtained deletion certifications. Plaintiffs therefore have not established scienter as to statements made by Defendants about the Cambridge Analytica data breach.

## 2. Whitelisting

The Court previously determined that Plaintiffs had pled falsity, scienter, materiality, and reliance as to their whitelisting theory of liability. See August

<sup>&</sup>lt;sup>2</sup> The Court **GRANTS** Defendants' request for judicial notice as to Exhibit 7. *See* Fed. R. Evid. 201(b).

2020 Order at 65. However, the court dismissed Plaintiffs' whitelisting claims because the SAC failed to allege loss causation. The Court instructed Plaintiffs to demonstrate that the stock price fell in June 2018, following the revelation that Facebook secretly allowed certain "whitelisted" app developers to continue to access user data. TAC ¶ 319.

In the loss causation analysis, "the ultimate issue is whether the defendant's misstatement, as opposed to some other fact, foreseeably caused the plaintiff's loss." *Lloyd v. CVB Fin. Corp.*, 811 F.3d 1200, 1210 (9th Cir. 2016). A plaintiff must show that the defendant's misrepresentation was a "substantial cause" of his or her financial loss. *Loos v. Immersion Corp.*, 762 F.3d 880, 887 (9th Cir. 2014). To survive a motion to dismiss, a plaintiff "need only allege that the decline in the defendant's stock price was proximately caused by a revelation of fraudulent activity rather than by changing market conditions, changing investor expectations, or other unrelated factors." *Id.* 

"Typically, to establish loss causation, a plaintiff must show that the defendants' alleged misstatements artificially inflated the price of stock and that, once the market learned of the deception, the value of the stock declined." *Irving Firemen's Relief & Ret. Fund v. Uber Techs., Inc.*, 998 F.3d 397, 407 (9th Cir. 2021) (collecting cases). Courts refer to this theory as "fraud-on-the market." *Id.* (citation omitted). In this scenario, "the plaintiff must show that after purchasing her shares and before selling, . . . (1) the truth became known, and (2) the revelation caused the fraudinduced inflation in the stock's price to be reduced or eliminated." *Id.* (citation and quotation marks omitted). The second element requires a showing that the revelation of the truth "caused the company's stock

price to decline and the inflation attributable to the misstatements to dissipate." In re Bofl Holding, Inc. Secs. Litig., 977 F.3d 781, 791 (9th Cir. 2020). This analysis "involves a temporal component." Irving Firemen's Relief, 988 F.3d at 407; see also Dura Pharms., Inc. v. Broudo, 544 U.S. 336, 343–44 (2005). "[A] disclosure followed by an immediate drop in stock price is more likely to have caused the decline—but timing is not dispositive." In re Bofl Holding, 977 F.3d at 790; see also In re Gilead Scis. Sec. Litig., 536 F.3d 1049, 1057–58 (9th Cir. 2008) (noting that there is not a "bright-line rule requiring an immediate market reaction").

In its August 2020 Order, this Court held that the user control statements were adequately alleged to have been misleading because of Facebook's "white-listing practices." August 2020 Order at 38. As the Court noted, the relevant time period is *after* the revelation of Facebook's whitelisting practices, which would be after June 3, 2018. TAC ¶ 703. Plaintiffs do not plead a loss until July 26, 2018, which is over a month after the whitelisting practice was revealed. *Cf. In re Gilead*, 536 F.3d at 1051–58 (allowing a delayed market reaction where the falsity of the alleged misstatements was revealed months later). Plaintiffs have not established a connection between the revelation of Facebook's whitelisting practice and a stockdrop, and thus have not plead loss causation.<sup>3</sup>

<sup>&</sup>lt;sup>3</sup> The Court declines to revisit its earlier ruling as to the drop of the stock prices following the 2Q18 Earnings Release. *See* August 2020 Order at 65–66. Additionally, because the Court has determined that Plaintiffs have not established scienter as to its Cambridge Analytica theory, it also declines to address loss causation as to this theory.

## 3. Section 20(a) and 20(A) Claims

Plaintiffs also bring claims for violations of Sections 20(a) and (A) of the Exchange Act. Both these claims, however, depend on a primary violation of Section 10(b) or Rule 10b-5. *Lipton v. Pathogenesis Corp.*, 284 F.3d 1027, 1035 n.15 (9th Cir. 2002) ("[T]o prevail on their claims for violations of § 20(a) and § 20A, plaintiffs must first allege a violation of § 10(b) or Rule 10b-5."). Because the Court determines Plaintiffs' claim under Section 10(b) and Rule 10b-5 fail, Defendants' motion to dismiss these claims is also **GRANTED**.

#### 4. Leave to Amend

When dismissing a complaint for failure to state a claim, a court should grant leave to amend "unless it determines that the pleading could not possibly be cured by the allegation of other facts." *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000). This Court has previously dismissed two other complaints, has provided Plaintiffs ample opportunity to cure the deficiencies identified in those Orders, and has warned Plaintiffs that failure to cure the identified deficiencies would result in dismissal with prejudice. Because Plaintiffs have not remedied those deficiencies, the Court finds that amendment would be futile, and Plaintiffs' claims are dismissed without leave to amend.

# 127a

# III. CONCLUSION

Defendants' motion to dismiss Plaintiffs' TAC in its entirety is  ${\bf GRANTED.}$ 

# IT IS SO ORDERED.

Dated: December 20, 2021

/s/ Edward J. Davila
EDWARD J. DAVILA
United States District Judge

#### APPENDIX D

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

Case No.

5:18-cv-01725-EJD

IN RE

FACEBOOK, INC. SECURITIES LITIGATION ORDER GRANTING DEFENDANTS' MOTION TO DISMISS WITH LEAVE TO AMEND

Re: Dkt. No. 126

Aug. 7, 2020

Before the Court is Defendants' motion to dismiss Plaintiffs' second amended complaint. Plaintiffs are persons who purchased shares of Facebook common stock between February 3, 2017 and July 25, 2018 ("the Class Period"), who believe that Defendant Facebook, Inc. and Executive Defendants Mark Zuckerberg, Sheryl K. Sandberg, and David W. Wehner made materially false and misleading statements and omissions in connection with the purchase and sale of Facebook stock. See Second Amended Complaint ("SAC") ¶ 1, Dkt. 123. Plaintiffs allege that Defendants violated Section 10(b), 20(a), and 20A of the Securities Exchange Act of 1934 (the "Exchange Act") and Rule 10b-5 promulgated thereunder because Defendants made guarantees that the Cambridge Analytica, and related data-privacy scandals, would not impact Facebook stock while knowing this to be false. Specifically, Plaintiffs focus on Defendants' statements and omissions concerning Facebook's "privacy and data protection practices" and their impact on Facebook's stock prices during the Class Period. *Id*.

Defendants have filed a motion to dismiss¹ arguing that Plaintiffs have failed to (for a second time) meet Federal Rule of Civil Procedure 9(b)'s heightened pleading requirements for securities fraud. The Court agrees; while Plaintiffs have plead sufficient facts to show actionable misstatements, scienter, and reliance, their SAC fails to plead facts showing causation. Thus, the Court **GRANTS** Defendants' motion to dismiss **with leave to amend**.

## I. BACKGROUND

## A. Factual Background

Defendant Facebook was founded by Defendant Mark Zuckerberg, who is the Chief Executive Office ("CEO") of the company and the Chairman of the Board of Directors. Id. ¶ 32. Defendant Sheryl Sandberg is the Chief Organization Officer ("COO") of the company and serves on the Board of Directors. Id. ¶ 34. Defendant David Wehner is the Chief Financial Officer ("CFO") of the company. Id. ¶ 35.

Facebook is the world's largest social networking company; its products and platforms are designed to facilitate connection and information sharing between users through mobile devices and personal computers. *Id.* ¶ 41. Plaintiffs allege that Facebook's business model depends on: monetizing user data, attracting new users, and engaging/retaining existing users. *Id.* 

<sup>&</sup>lt;sup>1</sup> Pursuant to N.D. Cal. Civ. L.R. 7-1(b) and General Order 72-5, this Court found this motion suitable for consideration without oral argument. *See* Dkt. 136.

¶¶ 43–48 ("Facebook's main asset is the vast treasure-trove of user personal data that it has amassed since its founding."). The platform formerly allowed third-party app developers' applications or websites ("apps") access to users' information and to users' friends' information. Id. ¶ 48. Despite Defendants guarantees to the contrary, access to user data (in contravention of user privacy settings) continued through the class period. Allegedly, certain "whitelisted" app developers and corporate giants like Amazon, Google, Samsung, Blackberry, Huawei (a Chinese technology company), and Mail.Ru Group (a Kremlin-connected technology conglomerate) were able to access users' friends' data through the class period. Id. ¶¶ 15, 16.

The Court briefly outlines the background of Plaintiffs' claims. Before April 2014, a user automatically consented to an app developer gaining access to their personal data and the personal data of his or her friends ("third-party consent"). Id.; see also Ex. 25, Dkt. 126-26. However, in April 2014, Defendant Zuckerberg informed users that this third-party consent would be changed. See Ex. 30, Dkt. 126-31 ("Second, we've heard from people that they're often surprised when a friend shares their information with an app. So we've updated Facebook Login so that each person decides what information they want to share about themselves, including their friend list."). After reading this announcement and considering Facebook's 2014, 2015, and 2016 Privacy Policies, the Court understands this to mean that users could still share their friend list with third-party app developers, but users and users' friends would have more control over the sharing of that list. This is to say, Facebook represented to consumers that they could control the privacy of their data by using desktop and mobile privacy settings to limit the information that Facebook could

share with app-developers. In actuality, users lacked such control. Indeed, Plaintiffs maintain that Facebook's representations were false and/or materially misleading because "whitelisted" app developers could still access users' data and users' friends' data in contravention of user privacy settings. See id. ¶¶ 54–64.

## 1. Relevant Agreements

Facebook-User Agreements. The use and sharing of data on Facebook are governed by agreements between Facebook and its users, including Facebook's Data Policy (formerly the "Data Use Policy" and the "Privacy Policy") and Facebook's Terms of Service (formerly "Statement of Rights and Responsibilities"). Id. ¶¶ 167, 170, 232, 276, 370, 462–64. These policies explain how users can control whether and how their data is shared with their Facebook friends, other Facebook users, and third parties. Id. ¶¶ 326, 469. For example, the September 2016 Data Policy informed users of the categories of information that third-party apps could access if users allowed (or "authorized") apps to do so. See Ex. 26 at 2, Dkt. 126-27. The policy also informed users how to control access to their data and cautioned users that use of third-party apps, websites, or other services that use, or are integrated with, the Facebook platform may result in the thirdparties receiving information about what users post or share. *Id.*; see also SAC ¶ 469.

Under the November 2013 Data Use Policy, Facebook's policies allowed users to share information about their friends with third-party app developers. *Id.* ¶¶ 48, 89. This policy stated that app developers could ask for certain information about users' friends and alerted users that their friends might choose to share some of their information with app developers.

Ex. 25, Dkt. 126-26. For example, the policy advised users that when using a music app, "[y]our friend might . . . want to share the music you 'like' on Facebook." *Id.* at 4 ("[I]f you've shared your likes with just your friends, the application could ask your friend for permission to share them."). Thus, under this November 2013 policy, a user's friend could re-share the user's likes with an app that the friend had downloaded, so long as the original user consented to such sharing by their friends. The converse was also true; if a user chose to turn off all Platform apps, that user's friends could *not* share the user's information with apps (at least, not without running afoul of the stated policy).

In 2014, however, Facebook announced that it would implement changes to its Platform that would "dramatically limit the Facebook information apps could access," and "shut off third parties' access to collect user friend data" to ensure that "everyone has to choose to share their own data with an app themselves." SAC ¶¶ 81–83, 186, 383, 434; see also Ex. 30, Dkt. 126-31 (disclosing that platform changes would be finalized one year later). The FTC interpreted this to mean that Facebook would stop allowing thirdparty developers to collect data [about friends]." Id. ¶ 83. The Court does not comment on whether that interpretation is correct. But see Ex. 26, Dkt. 126-27 (2016 data policy warned users that when they use third-party apps, you share your username, user ID, your age range and country/language, and your list of friends, as well as any information that you share with them); accord Ex. 27 at 2, Dkt. 126-28; see also id. ("We transfer information to vendors, service providers, and other partners who globally support our business . . . . ").

Facebook-App Developer Agreements ("Platform Policy"). Third-party app developers must agree to Facebook's Platform Policy before offering apps on the Facebook platform. SAC ¶¶ 275–76 & n. 265, 368–70. The Platform Policy, which was in place at all times relevant to the allegations in the SAC, limits the extent to which developers can collect and use Facebook user data, and requires developers to explain to users the categories of information they will collect and how it will be used. Id. ¶¶ 210, 275–76, 383–70. The Platform Policy prohibits developers from selling or transferring user data, and from using their customers' friend data outside of customer use of the app. Id. ¶ 468.

## 2. Alleged Events Relevant to Plaintiffs' Claims

Aleksandr Kogan and Cambridge Analytica. In 2013, Aleksandr Kogan, a professor and data researcher at Cambridge University, developed a personality quiz app called "This is Your Digital Life." *Id.* ¶¶ 87–88; see also September 2019 Order at 4 (Plaintiffs admitted in first complaint that Kogan developed app in 2013); Hakopian v. Mukasey, 551 F.3d 843, 846 (9th Cir. 2008) ("Allegations in a complaint are considered judicial admissions."). The app appeared on the Facebook Platform in 2014 and told users that the results of the guiz would be used for academic purposes. Id. ¶¶ 87–88. Approximately 270,000 people installed the app and consented to sharing their data, including some information about their Facebook friends, see id. ¶ 89, which at that time was permitted under Facebook's policies, subject to the friends' privacy and application settings, see Ex. 25, Dkt. 126-26.

The December 2015 Guardian Article and Facebook's Response. In December 2015, The Guardian reported that Kogan, through his company Global Science Research ("GSR"), sold some of the information collected through the "This Is Your Digital Life" app to Cambridge Analytica, in violation of Facebook's policies. Ex. 17, Dkt. 126-18; SAC ¶¶ 5, 86-89, 98, 468. According to the article, Cambridge Analytica developed psychological profiles of U.S. voters using the data of tens of millions of Facebook users (which had been harvested from Kogan's data) to support Ted Cruz's presidential campaign. Ex. 17, Dkt. 126-18;  $\P \P 5$ , 86–89. After the article was published, Facebook removed Kogan's app from Facebook, and privately asked GSR and Cambridge Analytica to delete the data and was told by the companies that the data had been deleted. ¶¶ 5, 93, 137–38, 150, 186, 210, 377.

The Cambridge Analytica Story Resurfaces in 2018. On March 17, 2018, three years after the original Cambridge Analytica story broke, The New York Times and The Guardian reported that Defendants (1) delayed in addressing the Cambridge Analytica data breach and that (2) the data had not been deleted (as reported by Defendants), but was used in connection with President Donald Trump's campaign. See id. ¶ 189. Cambridge Analytica had lied when it represented to Facebook in 2016 that it had deleted all user data. Id. ¶¶ 20, 189-190. Facebook then suspended Cambridge Analytica, its parent company, and certain related employees from the Facebook Platform. ¶ 186.

In response to the stories, Facebook's common stock dropped nearly 7% on Monday, March 19, 2018,

the first trading day after the news broke, and fell an additional 2.5% the next trading day. *Id.* ¶ 198.

Facebook's First Quarter 2018 Earnings Report ("1Q18") and the GDPR. On April 25, 2018, Defendants released a favorable first quarter earnings report, 1Q18, with quarterly revenue, earnings, and daily and monthly active user growth exceeding analyst expectations. Id. ¶¶ 25, 219, 221, 223, 427. Although a "handful" of advertisers had "paused spend" with Facebook after the Cambridge Analytica news, Facebook reported that this did not appear to reflect a "meaningful trend." Id. ¶ 429. During the earnings call, Facebook told investors that it anticipated expenses to increase due to its investments in data security programs and the 48% increase in the number of Facebook employees from the prior year. Id.; see also Ex. 9 at 7–8, Dkt. 126-10. The stock price climbed more than 9% following the release of this report. SAC ¶ 25. By July, Facebook's stock price was trading well above \$200 per share. *Id*.

On this earnings call, Facebook also addressed the possible impact of the General Data Protection Regulation, ("GDPR")² which took effect the month after 1Q18 results were released. *Id.* ¶¶ 430–31; *see also* Ex. 9 at 8, 11, 15–16, 18, 23, Dkt. 126-10. Facebook claimed that compliance with the GDPR would not be an issue because Facebook was already almost compliant. SAC ¶ 232. However, Facebook did note that it

 $<sup>^2\,</sup>$  The GDPR is a broad set of privacy regulations governing the collection and use of personal data. It is designed to protect the privacy of European Union ("EU") citizens. The GDPR has a host of disclosure and user-control requirements. For instance, (and notable here) the GDPR requires corporations to make their data collection and sharing policies opt-in, rather than opt-out. SAC  $\P$  229.

was "early and difficult to know . . . in advance" the business implications of Facebook's implementation of the GDPR. Indeed, Facebook anticipated that Facebook's European daily and monthly user base could be "flat to slightly down." Ex. 9 at 8, 23, Dkt. 126-10. Facebook also noted that while they did not anticipate the GDPR to significantly impacting advertising revenue, there was "certainly the potential for some impact." *Id.* at 8; *see also id.* at 18 ("[T]he amount of uncertainty [] for us and all the other companies in the digital advertising industry is reasonably higher than it's been [] because we're in the process of rolling out GDPR. We're going to all know a lot more after we rollout.").

Facebook's Second Quarter 2018 Earnings Report ("2Q18"). On July 25, 2018, Facebook announced its 2Q18 earnings, which reported lower than expected revenue growth, profitability, and user growth. SAC ¶¶ 243–44, 247–48. On July 26, 2018 the common stock price dropped nearly 19%, resulting in a single-day loss of approximately \$120 billion in market capitalization. Id. ¶ 249.

Following the 2Q18 earnings, the Pew Research Center issued a report that it conducted following the aftermath of the 2018 Cambridge Analytica scandal. The report—titled "Americans are changing their relationship with Facebook"—documented changes in Facebook user engagement. *Id.* ¶ 252. It revealed substantial disengagement by Facebook users during May 29 to July 11, 2018 (the study period). *Id.* Specifically, it stated that more than half (54%) of Facebook users had changed their privacy settings to share less with Facebook, 42% had taken extended breaks from engaging with Facebook, while more than a quarter (26%) had deleted the Facebook app from their cell

phones. *Id.* Disengagement was particularly pronounced among the younger users, who are more coveted by advertisers. *Id.* 

Facebook attributed the user growth slowdown to the effects of the "GDPR rollout, consistent with the outlook we gave on the Q1 call," but noted that the "vast majority of people [had continued] opting in to ... third-party data use." Ex. 10 at 7, 18, Dkt. 126-11. During the earnings call, one analyst remarked that Facebook had given an "accurate read into the June quarter" on the likely impact of the GDPR. Id. at 15 (You have—you gave us a—what turned out to be a pretty accurate read into the June quarter . . . . "); see also id. ("We had indicated . . . in the first quarter that we would expect to see a decline [in daily active users and monthly active users in Europe following implementation of the GDPR]."). Facebook also reported that its expenses were up "50%" year-over-year, which accorded with estimates made in the prior quarter. *Id*. at 8 ("There are several factors contributing to that deceleration. For example, we expect currency to be a slight headwind in the second half vs. the tailwinds we have experienced over the last several quarters. We plan to grow and promote certain engaging experiences like Stories that currently have lower levels of monetization. We are also giving people who use our services more choices around data privacy which may have an impact on our revenue growth.").

Executive Defendants' Sale of Facebook Stock. During the Class Period, Defendant Zuckerberg sold approximately 30,000 Facebook shares for proceeds of more than \$5.2 billion, while Defendant Sandberg sold \$389 million in Facebook shares and Defendant Wehner sold \$21 million worth in Facebook

shares. SAC ¶ 19. Plaintiffs use this to corroborate scienter.

## 3. Alleged Misstatements/Omissions

Plaintiffs allege that Defendants made a total of **83** materially misleading statements or omissions in press releases, U.S. Securities and Exchange Commission ("SEC") filings, earnings calls, and public remarks at conferences. The Court has arranged these statements by source and bolded/italicized the relevant portions of the statements.

# <u>Statements Concerning Facebook Users' "Control" Over Their Data</u>

## Statement 1

"You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings."

SAC ¶ 326 (stated in Facebook's Statement of Rights and Responsibilities)

## **Statement 2**

"[W]hen you share on Facebook, you need to know that no one's going to steal our data. *No one is going to get your data that shouldn't have it.* That we're not going to make money in ways that would make you feel uncomfortable . . . . And that *you're controlling who you share with*. . . . Privacy for us is making sure that you feel secure, sharing on Facebook."

SAC ¶ 327 (stated by Defendant Sandberg during 2017 Axios interview)

## **Statement 3**

"[T]he Facebook family of apps already applies the core principles in the [GDPR] framework because we

built our services around transparency and control."

SAC  $\P$  328 (stated by Defendant Sandberg during 3Q17 earnings call)

## Statement 4

"Our apps have long been focused on giving people *transparency and control*...."

SAC ¶ 329 (stated by Defendant Sandberg during Facebook Gather Conference in January 2018)

#### Statement 5

"[T]he Facebook family of apps *already applies* the core principles in the GDPR framework, which are *transparency and control.*"

SAC ¶ 330 (stated by Defendant Sandberg during 4Q17 earnings call)

### Statement 6

"So we think with transparency and *control*, we're set up well to be in a position where we're compliant with GDPR when the regulation goes into effect in May."

SAC ¶ 331 (stated by Defendant Wehner during 2018 Conference Call)

### Statement 7

"In 2014, after hearing feedback from the Facebook community, we made an update to ensure that each person decides what information they want to share about themselves, including their friend list. This is just one of the many ways we give people the tools to control their experience. Before you decide to use an app, you can review the permissions the developer is requesting and choose which information to share.

You can manage or revoke those permissions at any time."

SAC ¶ 332 (stated by Defendant Facebook in 2018 post after 2018 Cambridge Analytica scandal)

## **Statement 8**

"[T]he main principles are, you have control over everything you put on the service, and most of the content Facebook knows about you it [sic] because you chose to share that content with your friends and put it on your profile."

SAC  $\P$  333 (stated by Defendant Zuckerberg during 2018 phone conference)

## **Statement 9**

"You've been hearing a lot about Facebook lately and how your data is being used. While this information can sometimes be confusing and technical, it's important to know that **you are in control of your Facebook**, what you see, what you share, **and what people see about you**."

SAC ¶ 334 (stated by Defendant Facebook in April 2018 post)

## **Statement 10**

"We already show people what apps their accounts are connected to and *allow them to control what data they've permitted those apps to use.*"

SAC  $\P$  335 (stated by Defendant Facebook in June 2018 to U.S. House of Representatives)

#### Statement 11

"Privacy is at the core of everything we do, and our approach to privacy starts with *our commitment to transparency and control*. [...] Our approach to

control is based on the belief that people should be able to choose who can see what they share and how their data shapes their experience on Facebook. *People can control the audience for their posts and the apps that can receive their data.* 

SAC ¶ 336 (stated by Defendant Facebook in June 2018 to U.S. House of Representatives)

## **Statement 12**

"This is the most important principle for Facebook: Every piece of content that you share on Facebook, you own and you have *complete control* over who sees it and—and how you share it, and you can remove it at any time. That's why every day, about 100 billion times a day, people come to one of our services and either post a photo or send a message to someone, because *they know that they have that control and that who they say it's going to go to is going to be who sees the content*. And I think that that control is something that's important that I think should apply to—to every service."

SAC ¶ 337(a) (stated by Defendant Zuckerberg in April 2018 to Joint Commerce & Judiciary Committees of U.S. Senate)

#### Statement 13

"That's what the [Facebook] service is, right? It's that you can connect with the people that you want, and you can share whatever content matters to you, whether that's photos or links or posts, and you get control over it."

SAC ¶ 337(b) (stated by Defendant Zuckerberg in April 2018 to Joint Commerce & Judiciary Committees of U.S. Senate)

#### Statement 14

"The two broad categories that I think about are content that a person is [sic] chosen to share and that they have complete control over, they get to control when they put into the service, when they take it down, who sees it. And then the other category are data that are connected to making the ads relevant. You have complete control over both."

SAC ¶ 337(c) (stated by Defendant Zuckerberg in April 2018 to Joint Commerce & Judiciary Committees of U.S. Senate)

### Statement 15

"Every person gets to control who gets to see their content."

SAC ¶ 337(d) (stated by Defendant Zuckerberg in April 2018 to Joint Commerce & Judiciary Committees of U.S. Senate)

#### Statement 16

"But, Senator, the—your point about surveillance, I think that there's a very important distinction to draw here, which is that when—when organizations do surveillance[,] people don't have control over that. But on Facebook, everything that you share there[,] you have control over."

SAC ¶ 337(e) (stated by Defendant Zuckerberg in April 2018 to Joint Commerce & Judiciary Committees of U.S. Senate)

## **Statement 17**

"[O]n Facebook, **you have control over** your information."

SAC ¶ 338(a) (stated by Defendant Zuckerberg in April 2018 to U.S. House of Representatives' Energy and Commerce Committee)

#### Statement 18

"[E]very single time that you share something on Facebook or one of our services, right there is a control in line, where you control who—who you want to share with."

SAC ¶ 338(b) (stated by Defendant Zuckerberg in April 2018 to U.S. House of Representatives' Energy and Commerce Committee)

#### Statement 19

"Congresswoman, giving people control of their information and how they want to set their privacy is foundational to the whole service [on Facebook]. It's not just a—kind of an add-on feature, something we have to . . . comply with. . . . all the data that you put in, all the content that you share on Facebook is yours. You control how it's used."

SAC ¶ 338(c) (stated by Defendant Zuckerberg in April 2018 to U.S. House of Representatives' Energy and Commerce Committee)

#### **Statement 20**

"Privacy is at the core of everything we do, and our approach to privacy starts with our commitment to transparency and control. [...] Our approach to control is based on the belief that people should be able to choose who can see what they share and how their data shapes their experience on Facebook. *People can control the audience for their posts and the apps that can receive their data*."

SAC ¶ 339 (stated by Defendant Facebook in response to questions from the U.S. Senate)

### <u>Statement Concerning Users' Privacy Settings</u>

#### Statement 21

"We respected the privacy settings that people had in place. Privacy and data protections are fundamental to every decision we make."

SAC ¶ 344 (stated by Defendant Facebook in March 2018 to *The Washington Post*)

## Statements Concerning Risks to Facebook's Business

#### **Statement 22**

"Security breaches and improper access to or disclosure of our data or user data, or other hacking and phishing attacks on our systems, *could* harm our reputation and adversely affect our business."

SAC ¶ 350(a) (stated by Defendant Facebook in 2016 Form 10-K)

#### Statement 23

"Any failure to prevent or mitigate security breaches and improper access to or disclosure of our data or user data *could* result in the loss or misuse of such data, which could harm our business and reputation and diminish our competitive position."

SAC ¶ 350(b) (stated by Defendant Facebook in 2016 Form 10-K)

#### Statement 24

"We provide limited information to ... third parties based on the scope of services provided to us. However, *if* these third parties or developers fail to adopt or adhere to adequate data security practices ... our

data or our users' data *may be* improperly accessed, used, or disclosed."

SAC ¶ 350(c) (stated by Defendant Facebook in 2016 Form 10-K)

#### Statement 25

"Although we have developed systems and processes that are designed to protect our data and user data, to prevent data loss and to prevent or detect security breaches, we cannot assure you that such measures will provide absolute security."

SAC ¶ 355 (stated by Defendant Facebook in 2016 Form 10-K)

#### Statement 26

"If we fail to retain existing users or add new users, or if our users decrease their level of engagement with our products, our revenue, financial results, and business may be significantly harmed.

The size of our user base and our users' level of engagement are critical to our success. Our financial performance has been and will continue to be significantly determined by our success in adding, retaining, and engaging active users of our products, particularly for Facebook and Instagram. We anticipate that our active user growth rate will continue to decline over time as the size of our active user base increases, and as we achieve higher market penetration rates. If people do not perceive our products to be useful, reliable, and trustworthy, we may not be able to attract or retain users or otherwise maintain or increase the frequency and duration of their engagement....

Any number of factors could potentially negatively affect user retention, growth, and engagement, including if:

there are decreases in user sentiment about the quality or usefulness of our products or *concerns related to privacy and sharing, safety, security*, or other factors

SAC  $\P$  358 (stated by Defendant Facebook in 2016 Form 10-K)

### Statements Concerning the Results of Facebook's Investigation into Cambridge Analytica

#### Statement 27

"Our investigation to date *has not uncovered any*thing that suggests wrongdoing with respect to Cambridge Analytica's work on the [Brexit] and Trump campaigns."

SAC ¶ 362 (stated by Defendant Facebook to The Guardian in March 2017)

#### Statement 28

"Our investigation to date *has not uncovered anything that suggests wrongdoing* [with respect to Cambridge Analytica]."

SAC ¶ 363 (stated by Defendant Facebook to *The Intercept* in March 2017)

#### **Statement 29**

"Our investigation to date *has not uncovered any*thing that suggests wrongdoing [with respect to Cambridge Analytica]."

SAC ¶ 363 (stated by Defendant Facebook to *The Intercept* in March 2017)

## <u>Statements Concerning Facebook's Response</u> to Instances of Data Misuse

#### Statement 30

"Misleading people or misusing their information is a direct violation of our policies and we will take swift action against companies that do, including banning those companies from Facebook and requiring them to destroy all improperly collected data."

SAC ¶ 368 (stated by Defendant Facebook to BuzzFeed News in February 2017)

#### Statement 31

"Misleading people or misusing their information is a direct violation of our policies and we will take swift action against companies that do, including banning those companies from Facebook and requiring them to destroy all improperly collected data."

SAC ¶ 369 (stated by Defendant Facebook to Newsweek in June 2017)

#### Statement 32

"Enforcement is both automated and manual, and can include disabling your app, restricting you and your app's access to platform functionality, *requiring that you delete data*, terminating our agreements with you or any other action that we deem appropriate."

SAC ¶ 370 (stated by Defendant Facebook in Data Policy)

#### Statement 33

"We are committed to vigorously enforcing our policies to protect people's information. We will

take whatever steps are required to see that this happens. We will take legal action if necessary to hold them responsible and accountable for any unlawful behavior.

\* \* \*

On an ongoing basis, we also do a variety of manual and automated checks to ensure compliance with our policies and a positive experience for users. These include steps such as random audits of existing apps along with the regular and proactive monitoring of the fastest growing apps.

We enforce our policies in a variety of ways from working with developers to fix the problem, to suspending developers from our platform, to pursuing litigation."

SAC ¶ 376 (stated by Defendant Facebook in March 2018 in group entitled "Suspending Cambridge Analytica and SCL Group from Facebook")

# Statements About Facebook Users Consenting to/Knowingly Giving Information to Kogan

#### Statement 34

"The claim that this is a data breach is completely false. Aleksandr Kogan requested and gained access to information from users who chose to sign up to his app, and everyone involved gave their consent. People knowingly provided their information, no systems were infiltrated, and no passwords or sensitive pieces of information were stolen or hacked."

SAC ¶ 380 (stated by Defendant Facebook in March 2018 Facebook post)

#### Statement 35

"The good news is that the most important actions to prevent this from happening again today we have already taken years ago.... In 2014, to prevent abusive apps, we announced that we were changing the entire platform to dramatically limit the data apps could access.... In this case, we already took the most important steps a few years ago in 2014 to prevent bad actors from accessing people's information in this way."

SAC ¶ 383 (stated by Defendant Zuckerberg on March 2018 on personal Facebook page)

## Statements About Facebook's Compliance with 2012 FTC Consent Decree

#### Statement 36

"Violation of existing or future regulatory orders or **consent decrees** could subject us to substantial monetary fines and other penalties that could negatively affect our financial condition and results of operations."

SAC ¶ 389 (stated by Defendant Facebook in 2016 Form 10-K)

#### Statement 37

"[W]e respect local laws and regulations . . . Certainly, regulation is always an area of focus that we work hard to make sure that we are explaining our business clearly and making sure regulators know the steps we take to protect privacy as well as making sure that we're in compliance."

SAC  $\P$  391 (stated by Defendant Sandberg during 2Q17 Earnings Call)

#### Statement 38

"We reject any suggestion of violation of the consent decree."

SAC ¶ 392 (stated by Defendant Facebook to *The Washington Post* in March 2018)

#### Statement 39

"You asked about the *FTC consent order*. We've worked hard to make sure that we comply with it."

SAC ¶ 393 (stated by Defendant Zuckerberg in April 2018)

#### Statement 40

"We're in constant conversation with the FTC, and that consent decree was important, and we've taken every step we know how to make sure we're in accordance with it."

SAC  $\P$  394 (stated by Defendant Sandberg in April 2018 interview)

#### Statement 41

"Our view is that—is that we believe that *we are in compliance with the consent order*, but I think we have a broader responsibility to protect people's privacy even beyond that."

SAC ¶ 395 (stated by Defendant Zuckerberg in April 2018 to U.S. Senate)

#### Statement 42

"Affected users or government authorities could initiate legal or regulatory actions against us in connection with any security breaches or *improper disclosure of data*, which could cause us to incur signifi-

cant expense and liability or result in orders or *consent decrees forcing us to modify our business practices.* Any of these events could have a material and adverse effect on our business, reputation, or financial results.

SAC ¶ 401 (stated by Defendant Facebook in 2016 Form 10-K)

# Statements About Facebook Users Whose Accounts Were Compromised

#### **Statement 43**

"We notify our users with context around the status of their account and actionable recommendations if we assess they are at increased risk of future account compromise by sophisticated actors or when we have confirmed their accounts have been compromised."

SAC ¶ 405 (stated by Defendant Facebook in April 2017 on its corporate website)

#### Statement 44

Facebook stated that it would provide:

- "*Notifications to specific people* if they have been targeted by sophisticated attackers, with custom recommendations depending on the threat models"; and
- "Proactive notifications to people who have yet to be targeted, but whom we believe may be at risk based on the behavior of particular malicious actors."

SAC ¶ 405 (stated by Defendant Facebook in April 2017 on its corporate website)

### Statement About Facebook Compliance with GDPR

#### Statement 45

"Europe[] has passed a single privacy law [i.e., the GDPR] and **we are adhering to that**. But privacy is something we take really seriously."

SAC ¶ 411 (stated by Defendant Sandberg in October 2017)

# Statements About Use of Platform to Influence Elections

#### Statement 46

"Though the volume of these posts was a tiny fraction of the overall content on Facebook, any amount is too much. Those accounts and Pages violated Facebook's policies—which is why we removed them, as we do with all fake or malicious activity we find."

SAC ¶ 414 (stated by Facebook's General Counsel [Mr. Strech] to U.S. Senate/U.S. House of Representatives)

#### Statement 47

SWALWELL: Can each of you assure the American people that you have fully searched your platforms and disclosed to this committee every Russian effort to influence the 2016 election? Mr. Edgett?

EDGETT: We've provided everything we have to date, and we're continuing to look at this. So there will be more information that we share.

SWALWELL: Mr. Stretch?

STRETCH: *The same is true*, particularly in connection with, as I mentioned earlier, some of the threat sharing that the companies are now engaged in.

SAC ¶ 415 (stated by Facebook's General Counsel [Mr. Stretch] to House subcommittee)

#### Statement 48

Feinstein QFR #4: Facebook confirmed in the House Intelligence committee hearing that they found no overlap in the groups targeted by the Trump campaign's advertisements, and the advertisements tied to the Russia-linked accounts identified thus far.... Does this assessment extend to both the content used and groups targeted by the companies associated with the campaign—like Cambridge Analytica—and Russian accounts?

Stretch: We have seen only what appears to be insignificant overlap between the targeting and content used by the IRA and that used by the Trump campaign (including its third-party vendors). We are happy to schedule a meeting with your staff to discuss our findings in more detail.

SAC ¶ 416 (stated by Facebook's General Counsel [Mr. Stretch] to Senator Feinstein)

# Statements About Daily Active Users ("DAU") and Monthly Active Users ("MAU") Metrics

#### Statement 49

May 3, 2017: "Daily active users (DAUs)—DAUs were 1.28 billion on average for March 2017, an increase of 18% year-over-year. **Monthly active users** (MAUs)—MAUs were 1.94 billion as of March 31, 2017, an increase of 17% year-over-year."

SAC ¶ 420(a) (stated by Defendant Facebook in press release)

#### Statement 50

"Our community now has more than 1.9 billion people, including almost 1.3 billion people active every day."

SAC ¶ 420(a) (stated by Defendant Zuckerberg in May 2017)

#### Statement 51

July 26, 2017: "Daily active users (DAUs)—DAUs were 1.32 billion on average for June 2017, an increase of 17% year-over-year. Monthly active users (MAUs)—MAUs were 2.01 billion as of June 30, 2017, an increase of 17% year-over-year."

SAC ¶ 420(b) (stated by Defendant Facebook in press release)

#### Statement 52

"Our community is now more than 2 billion people, including more than 1.3 billion people who use Facebook every day."

SAC  $\P$  420(b) (stated by Defendant Zuckerberg in June 2017)

#### Statement 53

November 1, 2017: "Daily active users (DAUs)—DAUs were 1.37 billion on average for September 2017, an increase of 16% year-over-year. Monthly active users (MAUs)—MAUs were 2.07 billion as of September 30, 2017, an increase of 16% year-over-year."

SAC ¶ 420(c) (stated by Defendant Facebook in press release)

#### Statement 54

"Our community continues to grow, now with nearly 2.1 billion people using Facebook every month, and nearly 1.4 billion people using it daily. Instagram also

hit a big milestone this quarter, now with 500 million daily actives."

SAC ¶ 420(c) (stated by Defendant Zuckerberg in November 2017)

#### Statement 55

January 31, 2018: "Daily active users (DAUs)—DAUs were 1.40 billion on average for December 2017, an increase of 14% year-over-year. **Monthly active users (MAUs)**—MAUs were 2.13 billion as of December 31, 2017, an increase of 14% year-over-year.

SAC ¶ 420(d) (stated by Defendant Facebook in press release)

#### Statement 56

"Our community continues to grow with more than 2.1 billion people now using Facebook every month and 1.4 billion people using it daily. Our business grew 47% year-over-year to \$40 billion."

SAC  $\P$  420(d) (stated by Defendant Zuckerberg in January 2018)

#### Statement 57

"We monitor the sentiment and engagement of people engaging in News Feed. We're really pleased with the strength of sentiment and engagement as we've ramped up News Feed ads."

SAC ¶ 421(a) (stated by Defendant Wehner)

#### Statement 58

"Because your experience on Facebook or Instagram is about the quality of what you see . . . what we do is **we monitor it carefully.** We ramp slowly. We monitor engagement sentiment, quality of ads. **We get a** 

lot of feedback directly from people who use Facebook. . . . And we just continue to monitor the metrics."

SAC ¶ 421(b) (stated by Defendant Sandberg)

#### Statement 59

"Improving the quality and the relevance of the ads has enabled us to show more of them, without harming the experience. And, our focus really remains on the experience. So, we'll continue to monitor engagement and sentiment very carefully."

SAC ¶ 421(c) (stated by Defendant Wehner)

#### Statement 60

"When we introduce ads into feed and continue to increase the ad load, we monitor really carefully. We're looking at user engagement on the platform. We also look at the quality of ads."

SAC  $\P$  421(d) (stated by Defendant Sandberg)

#### Statement 61

Analyst: "Can you just talk about some of the biggest trends you're monitoring?

Wehner: "Yes, I can start with the stats. So on—yes, Mark, on the engagement front, we're seeing time spent growth per DAU across the Facebook family of apps and that includes Facebook itself."

SAC ¶ 421(e)

#### Statement 62

"We have also increased our estimate for inauthentic accounts to approximately 2% to 3% of worldwide MAUs.... *We continuously monitor* and aggressively take down those accounts. These accounts tend

to be less active and thus, we believe, impact DAU less than MAU."

SAC ¶ 421(f) (stated by Defendant Wehner)

#### **Statements About 1Q18 Financial Results**

#### Statement 63

Facebook Reports First Quarter 2018 Results: "Daily active users (DAUs)—DAUs were 1.45 billion on average for March 2018, an increase of 13% year-overyear. Monthly active users (MAUs)—MAUs were 2.20 billion as of March 31, 2018, an increase of 13% year-over-year."

SAC ¶ 427.

#### Statement 64

"Despite facing important challenges, our community continues to grow. More than 2.2 billion people now use Facebook every month and more than 1.4 billion people use it daily."

SAC ¶ 428 (stated by Defendant Zuckerberg)

#### Statement 65

"Before going through our results, I want to take a minute to talk about ads and privacy. [...]

We also believe that people should control their advertising experience. For every ad we show, there's an option to find out why you're seeing that ad and to turn off ads from that advertiser entirely. And you can opt out of being targeted based on certain information like the websites you visit or your relationship status.

Advertising and protecting people's information are not at odds. We do both. Targeted ads that respect people's privacy are better ads. They show people things that they're more likely to be interested in. We regularly hear from people who use Facebook that they prefer to see ads that are relevant to them and their lives.

Effective advertising is also critical to helping businesses grow.

\* \* \*

In the coming months, GDPR will give us another opportunity to make sure people fully understand how their information is used by our services. It's an EU regulation, but as Mark said a few weeks ago, we're going to extend these controls to everyone who uses Facebook, regardless of where in the world they live. Our commitment to you is that we will continue to improve our ads model by strengthening privacy and choice while giving businesses of all sizes new and better tools to help them grow.

\* \* \*

Going forward, we will continue to focus on these 3 priorities and ensure that people's privacy is protected on Facebook."

SAC ¶ 430 (stated by Defendant Sandberg on 1Q18 earnings call)

#### Statement 66

"The changes that Mark and Sheryl described will, we believe, benefit our community and our business and will serve to strengthen Facebook overall. At the highest level, we believe that we can continue to build a great ads business while protecting people's privacy.

\* \* \*

So on GDPR, I think fundamentally, we believe we can continue to build a great ads business while protecting the privacy of the people that use Facebook. As part of the rollout of GDPR, we're providing a lot of control to people around their ad settings. And we're committed, as Sheryl and Mark mentioned, to providing the same controls worldwide. And while we don't expect these changes will significantly impact advertising revenue, there's certainly potential for some impact. Any change of our—of the ability for us and our advertisers to use data can impact our optimizational potential at the margin, which could impact our ability to drive price improvements in the long run. So we'll just have to watch how that plays out over time. I think it's important to note that GDPR is affecting the entire online advertising industry. And so what's really most important in winning budgets is our relative performance versus other opportunities presented to marketers, and that's why it will be important to watch kind of how this plays out at the industry level.

\* \* \*

I don't know that we really see a doomsday scenario here. I think what we think is that depending on how people react to the controls and the ad settings, there could be some limitations to data usage. We believe that those will be relatively minor. But depending on how broadly the controls are adopted and set, there is a potential to impact targeting for our advertisers. Obviously, if they are less able to target effectively, they'll get a lower ROI on their advertising campaigns. They'll then bid differently into the auction. That ultimately will flow through into how we can realize price on the im-

pressions that we're selling. So I think that's the mitigating issue that we could see, depending on how GDPR and our broader commitment to providing these same controls worldwide could play out. We think that there is a great case for not just our business but also for the user experience on Facebook to have targeting because we think it's a better experience for the people who use Facebook to have targeted ads. We think we can do that in a privacy-protected way, and it's just a better experience. You get more relevant ads, and it's—and I think overall benefits that only the advertisers but also the people who use Facebook. So I don't think see a real doomsday scenario here. We see an opportunity to really make the case."

SAC ¶ 431 (stated by Defendant Wehner on 1Q18 Earnings Call)

#### Statement 67

"I also want to talk about data privacy. And what happened with Cambridge Analytica was a major breach of trust. An app developer took data that people had shared with them and sold it. So we need to make sure that this never happens again, so we're taking a number of steps here.

First, as you all know we're restricting the data that developers will be able to request from people. Now the good news here is that back in 2014, we already made a major change to how the platform works to prevent people from sharing a lot of their friends' information. So this specific situation could not happen again today."

SAC  $\P$  434 (stated by Defendant Zuckerberg)

#### Statement 68

"So we recently went through this process of rolling out our flows and settings for GDPR compliance, first, in Europe, and we're going to do it around the world. And one of the settings that we ask people proactively to make a decision on is, do you want your ads, for how we do ad targeting, to be informed by the other apps and websites that you use? **People have to proac**tively make a decision. Yes or no. Do they want that data used? And the majority, I think we can even say vast majority of people say, yes, they want that data used. Because if they're going to see ads, you want to see good ads, right? So I think that this is one of the core questions that society faces and individuals face across the different services that we use, are how do we want our data to be used and where? . . . This is going to be a core thing that we need to think about going forward, but we think about it very deeply as this is a—just a core part of the value that we're trying to provide."

SAC ¶ 437 (stated by Defendant Zuckerberg)

#### Statement 69

"Privacy is at the core of everything we do, and our approach to privacy starts with our commitment to transparency and control. Our threefold approach to transparency includes, first, whenever possible, providing information on the data we collect and use and how people can control it in context and in our products. Second, we provide information about how we collect and use data in our user agreements and related educational materials. And third, we enable people to learn more about the specific data we have about them through interactive tools such as Download Your Information, which lets

people download a file containing data that they may want to take to another service, and Access Your Information, a tool we are launching that will let people more easily access and manage their data on Facebook.

Our approach to control is based on the belief that people should be able to choose who can see what they share and how their data shapes their experience on Facebook. People can control the audience for their posts and the apps that can receive their data. They can see and delete the history of their activities on Facebook, and, if they no longer want to use Facebook, they can delete their account and the data associated with it. Of course, we recognize that controls are only useful if people know how to find and use them. That is why we continuously deliver in-product educational videos in people's News Feeds on important privacy topics. We are also inviting people to take our Privacy Checkup—which prompts people to review key data controls—and we are sharing privacy tips in education campaigns off of Facebook, including through ads on other websites. To make our privacy controls easier to find, we are launching a new settings menu that features core privacy settings in a single place. We are always working to help people understand and control how their data shapes their experience on Facebook.

\* \* \*

Like many other free online services, we sell advertising space to third parties. Doing so enables us to offer our services to consumers for free. This is part of our mission to give people the power to build community and bring the world closer together.

\* \* \*

We maintain our commitment to privacy by not telling advertisers who users are or selling people's information to anyone. That has always been true. We think relevant advertising and privacy are not in conflict, and we're committed to doing both well.

We believe targeted advertising creates value for people and advertisers who use Facebook. Being able to target ads to the people most likely to be interested in the products, service or causes being advertised enables businesses and other organizations to run effective campaigns at reasonable prices.

\* \* \*

We do not have a "business reason" to compromise the personal data of users; we have a business reason to protect that information.

\* \* \*

We believe that everyone has the right to expect strong protections for their information, and that we also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations."

SAC ¶ 440 (stated by Defendant Facebook in June 2018 in response to questions from the U.S. Senate)

### **Statements About Selling User Data**

#### Statement 70

"We don't sell your data. We don't sell personal information like your name, Facebook posts, email address, or phone number to anyone. Protecting people's privacy is central to how we've designed our ad system."

SAC ¶ 445 (stated by Defendant Facebook in November 27)

#### Statement 71

"These principles are our commitment to the people who use our services. They are: We build for people first. **We don't sell your data**."

SAC ¶ 446 (stated by Defendant Facebook in January 2018)

#### Statement 72

"We provide a free service that's an ad-based business model, and in order to do that, we do not sell your data."

SAC ¶ 447 (stated by Defendant Sandberg in March 2018)

#### Statement 73

"There are other internet companies or data brokers or folks that might try to track and sell data, but we don't buy and sell. [...] The second point, which I touched on briefly there: for some reason we haven't been able to kick this notion for years that people think we will sell data to advertisers. We don't. That's not been a thing that we do. Actually it just goes counter to our own incentives... And we're going to use data to make those services better ... but we're never going to sell your information."

SAC ¶ 448 (stated by Defendant Zuckerberg in April 2018)

#### Statement 74

"What we share: We will never sell your information to anyone. We have a responsibility to keep people's information safe and secure, and we impose strict restrictions on how our partners can use and disclose data."

SAC ¶ 449 (stated by Defendant Facebook)

#### Statement 75

"It's a good opportunity to remind everyone what we say all the time, but we need to keep saying so people understand it—which is that **we don't sell data**, **period**, . . . And again, we do not sell data, ever."

SAC ¶ 450 (stated by Defendant Sandberg during April 2018 NPR interview)

#### Statement 76

"We do not sell data or give your personal data to advertisers, period."

SAC ¶ 451 (stated by Defendant Sandberg during April 2018 NPR interview)

#### Statement 77

"I want to be clear. We don't sell information. So regardless of whether we could get permission to do that, that's just not a thing we're going to go do." 418 Zuckerberg further stated, "Well, Senator, once again, we don't sell any data to anyone. We don't sell it to advertisers, and we don't sell it to developers."

SAC ¶ 452 (stated by Defendant Zuckerberg before U.S. Senate Committees)

#### Statement 78

"Mr. Chairman, you're right that we don't sell any data.... There is a common misperception, as you say, that is just reported—often keeps on being reported, that, for some reason, we sell data. I can't be

clearer on this topic. We don't sell data.... Congressman, we don't sell people's data. So I think that's an important thing to clarify up front."

SAC ¶ 453 (stated by Defendant Zuckerberg before U.S. House of Representatives Committee)

#### Statement 79

"We use the information you provide and that we receive from websites to target ads for advertisers, but we don't tell them who you are. We don't sell your information to advertisers or anyone else."

SAC ¶ 454(a) (stated by Defendant Zuckerberg during 1Q18 Earnings Call)

#### Statement 80

"At Facebook, we have always built privacy protection into our ads system. [...] We don't sell your information to advertisers or anyone else."

SAC ¶ 454(b) (stated by Defendant Sandberg during 1Q18 Earnings Call)

#### Statement 81

"We don't tell advertisers who you are; and **we don't sell your data**."

SAC ¶ 455 (stated by Defendant Facebook in May 2018)

#### Statement 82

"Facebook does not sell people's information to anyone, and we never will. When the individual is a Facebook user, we are also able to use this information to personalize their experiences on Facebook, whether or not they are logged out, but we will not target ads to users relying on this information unless the user allows this in their privacy settings. We don't sell or share this information with third parties."

SAC ¶ 456 (stated by Defendant Facebook in June 2018 to U.S. House of Representatives)

#### **Statement 83**

"We don't sell data.... So while it may seem like a small difference to you, this distinction on 'selling data,' I actually think to people it's like the whole game, right? So we don't sell data, we don't give the data to anyone else, but overwhelmingly people do tell us that if they're going to see ads on Facebook, they want the ads to be relevant; they don't want bad ads."

SAC ¶ 457 (stated by Defendant Zuckerberg in a July 2018 interview with Recode)

#### **B.** Procedural History

On October 15, 2018, Plaintiffs filed their Consolidated Class Action Complaint. See Dkt. 86. On September 25, 2019, this Court granted Defendants' motion to dismiss the consolidated complaint after finding that Plaintiffs had failed to carry their burden to plead with particularity falsity and scienter—the Court did not address reliance or loss causation in that order. Order Granting Defendants' Motion to Dismiss ("September 2019 Order"), Dkt. 118.

Plaintiffs filed their second amended consolidated complaint on November 15, 2019. See Dkt. 123. Thereafter, Defendants filed a motion to dismiss the second amended consolidated class action complaint. Motion to Dismiss Second Amended Consolidated Class Action Complaint ("Mot."), Dkt. 126. Plaintiffs filed an opposition. Lead Plaintiffs' Memorandum of Points and Authorities in Opposition to Defendants' Motion

to Dismiss ("Opp."), Dkt. 130. Defendants then filed a reply. Reply in Support of Defendants' Motion to Dismiss ("Reply"), Dkt. 132.

#### II. JUDICIAL NOTICE

Defendants ask this Court to take judicial notice of Exhibits 1 through 30, which are attached to the Declaration of Brian M. Lutz in Support of Defendant's Motion to Dismiss. See Request for Judicial Notice in Support of Defendants' Motion to Dismiss Second Amended Consolidated Class Action Complaint ("RJN re MTD"), Dkt. 127. Defendants also ask this Court to take judicial notice of Exhibit 31, which is attached to the Declaration of Brian M. Lutz in Support of Defendants' Reply ("RJN Reply"), Dkt. 133. Plaintiffs do not oppose this request and also ask the Court to take judicial notice of Exhibits A-K. Plaintiffs' Request for Judicial Notice and Response to Defendants' Request for Judicial Notice ("P RJN"), Dkt. 131.

Generally, district courts may not consider material outside the pleadings when assessing the sufficiency of a complaint under Federal Rule of Civil Procedure 12(b)(6). Lee v. City of L.A., 250 F.3d 668, 688 (9th Cir. 2001). When matters outside the pleadings are considered, the 12(b)(6) motion typically must convert into a motion for summary judgment. Khoja v. Orexigen Therapeutics, Inc., 899 F.3d 988, 998 (9th Cir. 2018); see also Fed. R. Civ. P. 12(d). This rule, however, does not apply to the incorporation by reference doctrine or judicial notice. Khoja, 899 F.3d at 998.

Federal Rule of Evidence 201 permits a court to take judicial notice of an adjudicative fact "not subject to reasonable dispute," that is "generally known" or "can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." Fed. R. Evid. 201(b). Specifically, a court may take judicial notice: (1) of matters of public record, *Khoja*, 899 F.3d at 999, (2) that the market was aware of information contained in news articles, *Heliotrope Gen., Inc. v. Ford Motor Co.*, 189 F.3d 971, 981 n.18 (9th Cir. 1999), and (3) publicly accessible websites whose accuracy and authenticity are not subject to dispute, *Daniels-Hall v. Nat'l Educ. Ass'n*, 629 F.3d 992, 998–99 (9th Cir. 2010). A court may consider the facts contained in the noticed materials. *Barron v. Reich*, 13 F.3d 1370, 1377 (9th Cir. 1994).

Incorporation by reference treats certain documents as though they are part of the complaint itself. *Daniels-Hall*, 629 F.3d at 998. These are situations where the complaint "necessarily relies" upon a document or where the complaint alleges the contents of the document and the document's authenticity and relevance is not disputed. *Coto Settlement v. Eisenberg*, 593 F.3d 1031, 1038 (9th Cir. 2010).

For the following reasons, Defendants' Exhibits 1–31 are subject to judicial notice.

• Exhibits 1–5 and 7–8 are SEC filings and Exhibit 6 is a table Defendants created that summarizes the forms contained in Exhibit 5. Judicial notice of these exhibits is appropriate because they are public filings made by Facebook with the SEC (or summaries of such public filings), and are therefore matters of public record not subject to reasonable dispute. See Fed. R. Evid. 201(b); see also Weller v. Scout Analytics, Inc., 230 F. Supp. 3d 1085, 1094 n.5 (N.D. Cal. 2017) (taking judicial notice of SEC filings).

- Exhibits 9–11 are transcripts of Defendants' earnings calls and shareholder meetings. Judicial notice of Exhibits 9 through 11 is appropriate—these exhibits are publicly available documents and are thus matters of public record not subject to reasonable dispute. See Fed. R. Evid. 201(b); see also In re Energy Recovery Inc. Sec. Litig., 2016 WL 324150, at \*3 (N.D. Cal. Jan. 27, 2016).
- Exhibit 12 is a transcript of a November 27, 2018 witness examination before the Digital, Culture, Media, and Sport Committee of the House of Commons of the United Kingdom. Exhibit 13 is a February 2019 report from the Information Commissioner's Office of the Parliament of the United Kingdom. Judicial notice of Exhibits 12 and 13 is appropriate because they are matters of public record not subject to reasonable dispute. See Fed. R. Evid. 201(b); Khoja, 899 F.3d at 999.
- Exhibits 14–16 are court filings. Judicial notice is appropriate because these exhibits are matters of public record not subject to reasonable dispute. See Fed. R. Evid. 201(b). "Materials from a proceeding in another tribunal are appropriate for judicial notice." Biggs v. Terhune, 334 F.3d 910, 915 n.3 (9th Cir. 2003); Foster Poultry Farms v. Alkar-Rapidpak-MP Equip., Inc., 868 F. Supp. 2d 983, 990 (E.D. Cal. 2012) ("Courts routinely take judicial notice of publicly available records . . . from other court proceedings.").
- Exhibits 17–24 are news articles. Exhibits 17 through 24 are publicly available documents, available on publicly accessible websites, they

are capable of accurate and ready determination from sources whose accuracy cannot reasonably be questioned, and are thus subject to judicial notice. Fed. R. Evid. 201(b); *Daniels-Hall*, 629 F.3d at 999.

- Exhibits 25–27 are versions of Facebook's Data Policy, which were in effect during the time period covered by Plaintiffs' allegations. The exhibits are subject to judicial notice because they are capable of accurate and ready determination from sources whose accuracy cannot reasonably be questioned. Fed. R. Evid. 201(b). It is common for courts to take judicial notice of a company's historical privacy policies. See, e.g., Matera v. Google Inc., 2016 WL 8200619, at \*5 (N.D. Cal. Aug. 12, 2016) (taking judicial notice of multiple versions of Google's privacy policy, including archived versions); Oracle Am., Inc. v. CedarCrestone, Inc., 938 F. Supp. 2d 895, 901 (N.D. Cal. 2013) (same).
- Exhibit 28 is Facebook's white paper, which is referenced and relied on in paragraphs 405 through 407 of the SAC. Because it is referenced and relied on in the SAC, the Court may consider it under the incorporation by reference doctrine. See Coto, 593 F.3d at 1038.
- Exhibit 29 is a Bloomberg stock table showing the historical stock prices of Facebook from January 2, 2018 to December 11, 2018. The Court may take judicial notice of Facebook's stock prices. See Lloyd v. CVB Fin. Corp., 2012 WL 12883522, at \*13 (C.D. Cal. Jan 12, 2012) (collecting cases); Metzler Inv. GMBH v. Corinthian Colls., Inc., 540 F.3d 1049, 1064 n.7

(9th Cir. 2008); In re Copper Mountain Sec. Litig., 311 F. Supp. 2d 857, 864 (N.D. Cal. 2004) ("Information about the stock price of publicly traded companies [is] the proper subject of judicial notice.").

- Exhibit 30 is an April 30, 2014 Facebook blog post entitled "The New Facebook Login and Graph API 2.0." Because Exhibit 30 is a publicly available document, available on a publicly accessible website, it is capable of accurate and ready determination from sources whose accuracy cannot reasonably be questioned, and it is thus subject to judicial notice. Fed. R. Evid. 201(b); see also Daniels-Hall, 629 F.3d at 999; Diaz, 2018 WL 2215790, at \*3 ("Publically accessible websites and news articles are proper subjects of judicial notice.").
- Exhibit 31 is Facebook's February 3, 2017 Annual Report on Form 10-K. Judicial notice is appropriate because it is a public filing made by Facebook with the SEC and is thus a matter of public record, not subject to reasonable dispute. See Weller, 230 F. Supp. 3d at 1094 n.5.

Plaintiffs' Exhibits A-K are also subject to judicial notice. These exhibits are either news articles, court filings, or other matters of public record. For the same reasons above, the Court finds them suitable for judicial notice. Accordingly, the Court **GRANTS** both Plaintiffs' and Defendants' requests for judicial notice.

#### III. DISCUSSION

#### A. Legal Standard

To survive a Rule 12(b)(6) motion to dismiss, a complaint must contain sufficient factual matter to "state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009); Fed. R. Civ. Pro. 8(a). Threadbare recitals of the elements of a cause of action supported by mere conclusory statements "do not suffice." *Ashcroft*, 556 U.S. at 678.

Securities fraud cases, however, must meet Rule 8's plausibility standard, the Private Securities Litigation Reform Act ("PSLRA"), and Rule 9(b)'s higher pleading standard. See Tellabs, Inc. v. Makor Issues & Rights, Ltd., 551 U.S. 308, 319–22 (2007); Zucco Partners, LLC v. Digimarc, Corp., 552 F.3d 981, 991 (9th Cir. 2009).

The PSLRA mandates that securities fraud complaints "specify" each misleading statement, set forth the facts "on which [a] belief" that a statement is misleading was "formed," and "state with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind [scienter]." Dura Pharm., Inc. v. Broudo, 544 U.S. 336, 345 (2005) (quoting 15 U.S.C. §§ 78u–4(b)(1)–(2)); see also Metzler, 540 F.3d at 1070 ("The PSLRA has exacting requirements for pleading 'falsity.""). Plaintiffs bear the burden of proving that the defendant's misrepresentations "caused the loss for which the plaintiff seeks to recover." Dura Pharm., 544 U.S. at 345–46 (quoting § 78u-4(b)(4)). In determining whether a "strong inference" of scienter has been sufficiently alleged, this Court must not only draw "inferences urged by the plaintiff," but also engage in a "comparative evaluation," and examine and consider "competing inferences [in defendants' favor] drawn from the facts alleged." *Tellabs*, 551 U.S. at 314. Hence, scienter must not only be "plausible or reasonable," it must also be "cogent and at least as compelling as any opposing inference of nonfraudulent intent." *Id.* at 324.

Federal Rule of Civil Procedure 9(b) further requires a plaintiff pleading securities fraud to state, with particularity, the circumstances constituting fraud or mistake.

#### B. Defendants' Motion to Dismiss

To show securities fraud under Section 10(b) and Rule 10b-5, plaintiffs must allege facts sufficient to establish (1) a material misrepresentation or omission; (2) made with scienter, *i.e.*, a wrongful state of mind; (3) a connection between the misrepresentation and the purchase or sale of a security; (4) reliance upon the misrepresentation; (5) economic loss; and (6) loss causation. Loos v. Immersion Corp., 762 F.3d 880 (9th. Cir. 2014), amended (Sept. 11, 2014). "To determine whether a private securities fraud complaint can survive a motion to dismiss for failure to state a claim, the court must determine whether particular facts in the complaint, taken as a whole, raise a strong inference that defendants intentionally or with deliberate recklessness made false or misleading statements to investors." In re LeapFrog Enter., Inc. Sec. Litig., 527 F. Supp. 2d. 1033, 1039–40 (N.D. Cal. 2007).

In their motion to dismiss, Defendants challenge the sufficiency of Plaintiffs' Section 10b and Rule 10b-5 claim as to (1) misrepresentation, (2) scienter, (3) reliance, and (4) causation. *First*, Defendants argue that Plaintiffs fail to plead actual misrepresentations—that is, statements by Defendants that are actually

false and/or omit material facts. The Court agrees that some of the alleged misrepresentations are not actionable or that Plaintiffs have failed to plead with particularity the circumstances that make the alleged misrepresentations actionable. However, for the below reasons, the Court finds a number of the alleged misrepresentations actionable. Second, Defendants argue that Plaintiffs have failed to plead scienter. The Court disagrees; Plaintiffs have alleged sufficient facts to connect the alleged misrepresentations with a wrongful state of mind. Third, Defendants argue that Plaintiffs have failed to plead reliance. The Court disagrees, Plaintiffs have established the presumption of reliance. Finally, Defendants argue that Plaintiffs have failed to plead loss causation. The Court agrees. Plaintiffs have not connected the alleged loss with alleged misrepresentations. For that reason, the Court must dismiss Plaintiffs' SAC.

#### C. Discussion

#### 1. Misrepresentation

For a misstatement to be actionable, the statement must be both false and material. See Basic Inc. v. Levinson, 485 U.S. 224, 238 (1988) ("It is not enough that a statement is false or incomplete, if the misrepresented fact is otherwise insignificant."). To survive a motion to dismiss, a complaint must "specify each statement alleged to have been misleading, [and] the reason or reasons why the statement is misleading." Metzler, 540 F. 3d at 1070 (quoting 15 U.S.C. § 78u–4(b)(1)).

Statements are misleading only if they "affirmatively create an impression of a state of affairs that differs in a material way from the one that actually exists." *Brody v. Transitional Hosp. Corp.*, 280 F.3d

997, 1006 (9th Cir. 2002). Rule 10b-5 prohibits "only misleading and untrue statements, not statements that are incomplete." *Id.* Silence, absent a duty to disclose, "is not misleading under Rule 10b-5." *Basic*, 485 U.S. at 239 n.17. "Often a statement will not mislead even if it is incomplete or does not include all relevant facts." *Brody*, 280 F.3d at 1006.

Not all material adverse events must be disclosed to investors. See In re Rigel Pharm., Inc. Sec. Litig., 697 F.3d 869, 880 n.8 (9th Cir. 2012) (discussing Matrixx Initiatives, Inc. v. Siracusano, 563 U.S. 27, 38-45 (2011)). Information that a reasonable investor might consider material need not always be disclosed; companies can control "what they have to disclose [per § 10(b)] by controlling what they say to the market." *Matrixx*, 563 U.S. at 45. Consequently, omissions are only actionable if a defendant has a duty to disclose information and fails to do so. Basic, 485 U.S. at 239 n.17. Hence, if the omission does not "make the actual statement[] misleading," a company need not supplement the statement "even if investors would consider the omitted information significant." Rigel, 697 F.3d at 880 n.8.

Finally, an actionable statement must also "be capable of objective verification." Retail Wholesale & Dep't Store Union Local 338 Ret. Fund v. Hewlett-Packard Co., 845 F.3d 1268, 1275 (9th Cir. 2017). For example, business puffery or opinion statements—i.e., vague, optimistic statements—are not actionable because they do not "induce the reliance of a reasonable investor." Or. Pub. Emps. Ret. Fund v. Apollo Grp. Inc., 774 F.3d 598, 606 (9th Cir. 2014).

In their SAC, Plaintiffs allege thirteen categories of allegedly misleading statements: (1) statements about control; (2) statements about respecting users'

privacy; (3) statements about risk factors; (4) statements about the Cambridge Analytica investigation; (5) statements about data misuse; (6) statements about user consent; (7) statements about compliance with the FTC consent decree; (8) statements about user notification; (8) statements about GDPR compliance; (9) statements about Russian interference in U.S. elections; (10) statements about user metrics; (11) statements about 1Q18 results; and (12) statements about the sale of user data. The Court addresses the alleged misstatements by category.

#### a. Deletion Certifications

An overarching issue through the alleged misrepresentations is whether or not Facebook knew that Kogan, GSR, and Cambridge Analytica did not delete the misappropriated data in 2015. Plaintiffs' main theory of securities fraud is that Defendants knew that Cambridge Analytica had sensitive user information and was using that information for improper purposes, which created a significant risk of business, reputational, and/or economic harm to Facebook. And, despite this knowledge, represented the risks posed by Cambridge Analytica as "hypothetical." See, e.g., SAC ¶¶ 135, 136.

The Parties each agree that Defendants did not know about Kogan's connections with Cambridge Analytica until December 2015—when *The Guardian* article broke. *Id.* ¶ 137. Once the article broke, Facebook learned that Kogan had used GSR to collect user data from Facebook and create personality scores for Facebook users. *Id.* Facebook also discovered that GSR, through Kogan, had transferred these personality scores (and not the underlying data) to Cambridge Analytica. *Id.* Both Parties also agree that Kogan's

**transfer** of personality scores to a third-party violated Facebook's Platform Policy (Kogan's retention of users' friends' data is another matter). *Id.* ¶ 138. Thereafter, Facebook privately asked GSR and Cambridge Analytica—the entities with illicit access to the data—to delete the personality scores. *Id.* Both GSR and Cambridge Analytica represented that the scores had been deleted. *Id.* 

Plaintiffs belabor the point that Facebook did "nothing else to confirm that the data had been deleted." *Id.* ¶ 139. This misses the mark; this is not a tort action. The relevant inquiry is not whether Defendants had a "duty" to do more. That question is already before Judge Chhabria. See In re Facebook, Inc., Consumer Privacy User Profile Litig., 402 F. Supp. 3d 767, 800 (N.D. Cal. 2019). Rather, the question is whether Facebook misrepresented its efforts to contain the Cambridge Analytica "breach." Thus, that Facebook did nothing else to confirm that the data had been deleted is only relevant if Facebook represented that it would confirm such deletion. Plaintiffs maintain that Facebook made such representations in their data use policy. Yet, nowhere in Facebook's data policy is there any representation that Facebook would confirm deletion. To the contrary, the data policy only represents that it would "require" data to be deleted. See **Statement 32.** It makes no guarantees about how Facebook would enforce that requirement.

Perhaps recognizing that their "lack of confirmation" argument essentially boils into a duty argument, Plaintiffs argue that "Facebook did not believe the oral statements from GSR and Cambridge Analytica that the data had been deleted." SAC ¶ 140. This is closer; with this theory, Plaintiffs can argue that Facebook knew GSR and Cambridge Analytica still could

access the data and that representations to the contrary were false. But, Plaintiffs encounter another problem—they fail to provide the Court with any reason why Facebook's belief would be misplaced. Instead, Plaintiffs use speculation to argue that Facebook should have known that Cambridge Analytica was still involved in data mining. For instance, Plaintiffs highlight February 2016 reports that a group supporting Brexit signed up Cambridge Analytica. *Id*. ¶ 141. From this, Defendants were supposed to deduce that Cambridge Analytica was using the misappropriated personality scores. Id. ¶ 42. Of course, Plaintiffs do not explain why the equally likely inference—that Cambridge Analytica was using data other than the misappropriated Facebook data—is overcome.

More damning is Plaintiffs' admission that after the June 2016 Brexit vote, Facebook contacted Cambridge Analytica to confirm deletion. *Id.* ¶ 142. Plaintiffs argue that this shows a "guilty conscience" by Facebook. The converse is true; it *also* shows that Defendants wanted to ensure their policies had been followed and that the data had been deleted. Again, Plaintiffs provide no reason as to why this inference is not also possible.

Next, Plaintiffs point the Court toward the "Confidential Settlement Agreement and Mutual Release" agreement Facebook signed with Kogan following the June 2016 Brexit vote. *Id.* ¶ 143. Two important things occurred in this agreement: first, Kogan certified that he and GSR had deleted the data. *Id.* ¶ 144. Second, the agreement revealed that the data Kogan transferred to Cambridge Analytica was not just personality scores, but also included highly sensitive user

information like name, birthdays, page likes, and locations. Id. Plaintiffs focus on this later revelation and show that it "revealed beyond doubt" that GSR and Cambridge Analytica had lied when initially describing the types of user data they had misappropriated. This is **literally** true. But, the inference Plaintiffs draw from it is mere speculation. Plaintiffs argue that this second revelation showed Facebook that Cambridge Analytica had not deleted the data and that the company was still misusing the data. *Id.* ¶ 146. Plaintiffs, however, provide no specific facts to support this inference. Instead, Plaintiffs point the Court toward vague evidence about Cambridge Analytica use of personality profiles—which they could have compiled with non-Facebook data—to target political advertising. Id. The significance of these "red flags" is never explained. The Court, rather, is supposed to draw inferences in Plaintiffs' favor, on the sole basis that the SEC identified these facts as "red flags." This is not enough. See In re UBS Auction Rate Secs. Litig., 2010 WL 2541166, at \*19 n.11 (S.D.N.Y. June 10, 2010); see also Vess v. Ciba-Geigy Corp. USA, 317 F.3d 1097, 1107 (9th Cir. 2003) ("[T]he circumstances constituting the alleged fraud [must] be specific enough to give the defendants notice of the particular misconduct . . . . Averments of fraud must be accompanied by the who, what, when, where, and how of the misconduct charged." (quotation marks and citations omitted)).

Finally, Plaintiffs focus on Roger McNamee's warnings to Defendants about bad actors using Facebook data to "harm innocent people." *Id.* ¶¶ 147, 148. These warnings, however, fail to establish that McNamee told Defendants that Cambridge Analytica did *not* delete the data or that he would even have such personal knowledge about Cambridge Analytica's data use.

This is all to say, the SAC does not have sufficient allegations from which the Court can infer that Defendants knew that GSR and Cambridge Analytica did not delete the relevant data. This undercuts many of Plaintiffs' theories of falsity because it demonstrates that Defendants' representations about the Cambridge Analytica scandal were not false and/or made with scienter. The Court will not re-analyze this in each below section, but it should be noted, that this is in the background of the below analysis.

#### **b.** Statements About Control

Statements 1-20 concern Facebook users' ability to control their data and information. See SAC ¶ 325. Importantly, this Court held in its September 2019 Order that **Statement 2** was plead with adequate falsity. Plaintiffs have now presented the Court with every statement by Defendants using the word "control" and have attempted to lump together any statement that references control. This is incorrect. Metzler, 540 F. 3d at 1070 (noting that plaintiff must allege why each statement is false). Simply stating that users have control over their experience does not render the statement inaccurate. Rather, the relevant inquiry is whether Plaintiffs have alleged particular facts showing that the alleged misstatements were false when made. See Ronconi v. Larkin, 253 F.3d 423, 430 (9th Cir. 2001).

Three sub-categories emerge. There are statements like **Statements 2**, **8**, and **12–19**, where an Executive Defendant pledges that users "control what they share" and how the data is used. These statements are of the type that the Court previously found actionable. There are statements like **Statements 1**, **7**, **9–11**, and **20**, where Defendant Facebook pledges that users can control the audience for their posts and

the apps that receive their data via the privacy settings. These statements are of the type previously found inactionable.<sup>3</sup> And then, there are statements like **Statements 3–6**, which focus on "transparency and control." These statements have not been previously analyzed. Plaintiffs argue the statements (irrespective of the sub-category) are false by their literal terms and because they omit material facts necessary to make them not misleading. But see supra III.C.1.a. (finding that Plaintiffs have not alleged sufficient facts to show Defendants omitted information about the Cambridge Analytica data deletion, or mislead investors about deletion and access to data). Specifically, Plaintiffs argue that the statements are false because users did not have control over their data since (i) Facebook continued to give whitelisted parties users' friend's data (and overrode user privacy settings to do so), (ii) bad actors (like Cambridge Analytica) could still access Facebook data, and (iii) Facebook could not control the data once it was given to thirdparties. SAC ¶¶ 340, 343.

In **Statements 2, 8, and 12–19**, an Executive Defendant (either Defendant Sandberg or Defendant Zuckerberg) made assurances like "you have complete control over who sees your content," "no one is going to get your data that shouldn't have it," "you are controlling who you share with," and "you have control

<sup>&</sup>lt;sup>3</sup> Specifically, the Court previously held **Statements 1 & 7** inactionable. In their Consolidated Class Action Complaint, Plaintiffs alleged that these statements were false because (1) Defendants' privacy policies were deliberately confusing to users and (2) they were meant to cast doubt on new reports about Facebook's failure to address data breaches. *See* September 2019 Order at 33, 41. Plaintiffs' theory of falsity has changed in this action and the Court finds this new theory, coupled with the factual background, sufficient to show falsity. *See infra* III.C.1.b.

over everything you put on the service." Plaintiffs have alleged that the contrary was true—that is, that users did not control their data as whitelisted developers could override privacy controls. See, e.g., id.  $\P$  3. More concerning, once data was in the hands of app developers, developers could share the data with "bad actors" or other third-parties without Facebook's knowledge. As demonstrated by the Cambridge Analytica data scandal, Facebook had limited control over the data once it "left" Facebook's servers. Id.  $\P$  9 (noting that the data Kogan misappropriated was not deleted despite certifications to the contrary). This is to say, users did not have control over their data; white-listed developers could still access, use, and potentially abuse user data, much like Kogan did in 2015.

Plaintiffs have plead sufficient, particular facts which show that **Statements 2, 8, and 12–19** were false when made. In April 2014, Facebook issued a press release promising to shut-off third party access to user-friend data to ensure that "everyone has to choose to share their own data with an app themselves." *Id.* ¶ 82; *see also* Ex. 30, Dkt. 126-31. This announcement established two timelines: new apps would be immediately confined to the new privacy terms, while existing apps would have a full year to upgrade. Ex. 30, Dkt. 126-31. This "transition period" ended April 30, 2015. During this transition period, existing developers could continue to access friends' data, subject to a users' privacy and application setting. Ex. 30, Dkt. 126-31.

Plaintiffs allege that new-whitelisted app developers were able to access user data and users' friends' data in contravention of the April 2014 announcement. More concerning, **Statements 2, 8, and 12–19** were made in 2018, which is *long* after the "transition"

period" discussed in the April 2014 announcement. Thus, at the time **Statements 2, 8, and 12–19** were made, there was no notification to users that their data or their friends' data could still be accessed by whitelisted developers (whether such developers were using new or existing apps). It was thus false for Defendants to say users "controlled" their data since whitelisted app-developers could access user-data in contravention of user privacy settings. See SAC ¶¶ 111–25 (alleging the specifics of whitelisting, including that whitelisted apps could override privacy settings through to nearly the end of the Class Period); see also ¶ 116 (investigation by The New York Times revealed that during the Class Period, Facebook allowed at least 60 phone and other device makers continued access to users' friends' data without consent). Two such third-party developers were Huawei, a Chinese telecom company, with ties to the Chinese government and Mail.Ru Group, a Kremlinconnected technology conglomerate. Id. ¶¶ 16, 125. After Cambridge Analytica, and especially after the 2018 The Guardian story, Defendants knew or should have known that once data is released to third-party app developers, it is near-impossible for Facebook to control the sharing or deletion of that data. See id.  $\P$  86–106, 171–72. Hence, it was false for Defendants to state that users had "complete control" over their data when they knew that user data was released to whitelisted developers with little to no oversight. For these reasons, the Court holds that Plaintiffs have adequately plead falsity as required by the PSLRA for **Statements 2, 8, and 12–19.** 

Statements 1, 7, 9–11, and 20 pertain to statements made by Defendant Facebook about user control on the platform. For instance, **Statement 1** told

users that they could control the sharing of their content and information via privacy and application settings. Likewise, **Statement 7** told users that they were being given "tools to control their experience." And, **Statement 9** stated that users were told they could "control what data . . . apps [could] use." Defendants argue that these statements are "indisputably true," see Mot. at 11, because these statements describe how Facebook's platform functions, see Reply at 4. But, these statements do not fully describe how Facebook's platform functions. Take **Statement 20**, where Defendant Facebook stated: "People can control the audience for their posts and the apps that can receive their data." Accepting Plaintiffs' allegations that, despite Defendant Facebook's assurances of control, certain whitelisted developers and phone companies were able to access user data and circumvent user privacy settings, renders Statement 20 false. Indeed, the issue is not what users chose to post, but whether Defendants' promises of control were true. By default, if a third-party can access a users' data, without permission and in contravention of Facebook's stated policy, a user does not have control over their content. Hence, Statements 1, 7, 9–11, and 20 are misleading because they indicate that users could control who accessed their data, when whitelisted developers and certain phone companies could still access user information. Users thus did not have "control" over their content and the Court holds that Plaintiffs have adequately plead falsity as to these statements.

In **Statements 3–6**, Plaintiffs challenge Defendants' representations that Facebook "built [its] services around transparency and control." Defendants argue that these statements are too vague to be actionable. Reply at 5. In the alternative, Defendants argue that these statements are true.

To be misleading, a statement must be "capable of objective verification." Hewlett-Packard Co., 845 F.3d at 1275. For example, "puffing"—expressing an opinion rather than a knowingly false statement of fact is not misleading. Id. The Court finds that Statements 3-6 are capable of objective verification. These statements are not the "soft statements," "loose predictions," or "aspirational goals" typically found to be puffery. See id. at 1049. Paradigm examples of puffery include "business remained strong," "consolidation would be very positive," or "we want to be a company known for its ethical leadership." An investor cannot quantify terms like "strong," "very positive," or "wants." Such statements are too vague to impact an investors investment decisions and are thus inactionable. In contrast, these statements can be verified—if Plaintiffs' allegations are true, Facebook was *not* built around transparency and control. The secret whitelisting practice is antithetical to Defendants' statements that Facebook is built around "transparency and control." In other words, if Facebook shared user data, as is alleged, then the service is neither transparent nor focused on user control. For these reasons, Plaintiffs have adequately plead falsity as to **State**ments 3-6 and Defendants' motion to dismiss Statements 1–20 on falsity grounds is **DENIED**.

# c. Statement About Respecting Users' Privacy

Plaintiffs claim that **Statement 21**—"We respected the privacy settings that people had in place"—was false and misleading because Facebook continued to give whitelisted third-parties and others access to users' friends' data after April 2014. SAC ¶ 345. For the reasons detailed above, *see* III.C.1.b., the Court finds that Plaintiffs have adequately plead

falsity as to **Statement 21** and **DENIES** Defendants' motion to dismiss this statement on falsity grounds.

### d. Statements About Risk Factors

**Statements 22–26** refer to Defendant Facebook's 10-K SEC risk disclosure statements. Plaintiffs again argue that these statements are materially false and misleading because the risks warned of had already materialized and were not disclosed. Opp. at 9 ("The above statements were materially misleading because they presented the risk of improper access, disclosure, and use of user data as merely hypothetical ...."). Plaintiffs first allege that it was misleading for Facebook to state that, "[a]ny failure to prevent or mitigate security breaches and improper access to or disclosure of our data could result in the loss or misuse of such data, which could harm our business and reputation and diminish our competitive position." (Statement 23). Plaintiffs next allege that it was misleading for Facebook to warn that if "third parties or developers fail to adopt or adhere to adequate data security practices, or in the event of a breach of their networks, our data or our users' data may be improperly accessed, used, or disclosed." (Statement 24). In Plaintiffs' view, these statements are misleading because Defendants knew that Kogan had already improperly disclosed the data of tens of millions of Facebook users to Cambridge Analytica and that the data was still in use by Cambridge Analytica. Opp. at 9<sup>4</sup>; but see supra III.C.1.a.

<sup>&</sup>lt;sup>4</sup> Plaintiff relies on the SEC's Complaint, which alleges that Facebook's risk factor statements were misleading. This reliance is misplaced. Defendant Facebook did not admit to this charge. Ex. 16 at  $\P$  2, Dkt. 126-17 ("Without admitting or denying the

For a risk disclosure to be false or misleading, a plaintiff must allege facts indicating that, when the risk factor was made, the risk warned of was "already affecting" the defendant. Lloyd v. CVB Fin. Corp., 2012 WL 12883522, at \*19 (C.D. Cal. Jan. 12, 2012); see also Baker v. Seaworld Entm't, Inc., 2016 WL 2993481, at \*12 (S.D. Cal. Mar. 31, 2016) (holding that risk disclosure statements not materially false or misleading because "[p]laintiffs . . . fail to plausibly allege Defendants knew that [warned-of risks] were having any impact on attendance"); Kim v. Advanced Micro Devices, Inc., 2019 WL 2232545, at \*7-8 (N.D. Cal. May 23, 2019) ("An omission is misleading where it 'affirmatively create[s] an impression of a state of affairs that differs in a material way from the one that actually exists." (quoting *Brody*, 280 F.3d at 1006).

Williams v. Globus Medical Inc., 869 F.3d 235 (3d Cir. 2017) is instructive. There, the relevant risk disclosure warned that "if any of our independent distributors were to cease to do business with us, our sales could be adversely affected." Id. at 242. The plaintiffs argued that this statement was misleading because the defendants failed to warn investors that they had in fact lost an independent distributor. Id. at 241. The court disagreed. The risk warned of was the risk of adverse effects on sales, not the loss of independent distributors generally. Id. The risk at issue thus only materialized if sales were adversely affected at the time the risk disclosures were made. Id. Accordingly,

allegations of the complaint . . . . "). Statements made by the SEC in settlement documents are not law, they are "untested assertions by litigants" and the position articulated by the SEC is "not binding on this Court." *In re UBS Auction Rate Secs. Litig.*, 2010 WL 2541166, at \*19 n.11.

because the plaintiffs failed to allege that the company's sales were adversely affected by the decision to terminate the distributor, the risk disclosure was not misleading and the defendants' duty to disclose was not triggered. *Id.* at 243; *see also Kim*, 2019 WL 2232545, at \*7–8 (finding risk factors statements not misleading because "the potential risks disclosed in the SEC filings had not come to fruition when Defendants filed the challenged risk disclosures").

The same analysis applies here. The relevant risks discussed in **Statements 22, 23, 25, and 26** are reputation, business, or competitive harm, not improper access to or the disclosure of user data. Plaintiffs do not allege that, at the time the risk disclosure was made, the Cambridge Analytica scandal was harming Facebook's reputation, business, or competitive position. Nor can they. At the time these risk disclosures were made in February 2017, both Kogan's and Cambridge Analytica's misuse of user data were matters of public knowledge (with no alleged harm to Facebook's business, reputation, or competitive positions). See Ex. 17, Dkt. 126-18 (Guardian story published in December 2015). Accordingly, **Statements** 22, 23, 25, and 26 were not misleading because the potential risks presented therein were not yet "affecting" Facebook.

**Statement 24** presents a different scenario. There, the risk identified is the improper use or disclosure of user data. This is what Plaintiffs allege occurred (see *supra* for more discussion on whitelisting). However, Plaintiffs have a chronology problem.<sup>5</sup>

<sup>&</sup>lt;sup>5</sup> The Court also notes that Plaintiffs have not overcome Defendants' argument that Facebook reasonably believed that the

When Defendants identified data misuse and disclosure as relevant risks in 2016, Kogan's and Cambridge Analytica's misuse of Facebook user data was already public knowledge, and had been so for more than a year. See SAC ¶ 5 n.3 (citing Harry Davies, Ted Cruz Using Firm that Harvested Data on Millions of Unwitting Facebook Users, The Guardian (Dec. 11, https://www.theguardian.com/usnews/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data). Thus, as of December 2015, investors knew that Kogan had collected user data through his app and then sold that data to Cambridge Analytica in violation of Facebook's policies. and that Cambridge Analytica in turn used Kogan's data to create psychological profiles of voters for the purpose of assisting political campaigns. SAC ¶¶ 5, 86–92, 232, 280. Investors therefore had all of the information they needed to evaluate Statement 24 because the risk of data misuse and loss had already been realized, investors would not have been misled as to this risk. See Paskowitz v. Arnall, 2019 WL 3841999, at \*9 (W.D.N.C. Aug. 15, 2019) ("At the same time the Company disclosed the 'risks' of attracting and retaining key personnel[,] the Company also disclosed the identities of the key personnel and the numbers of investment professionals working in the business. Therefore, investors would not have been misled concerning the degree to which the 'risk' of employee departures had been realized ...."); cf. Sgarlata v. PayPal Holdings, Inc., 2018 WL 6592771, at \*2 (N.D. Cal. Dec. 13, 2018) (finding material misstatement where statement failed to fully disclose an unknown-

data had been deleted and thus that there was no risk of improper access.

risk because that created a false impression of reality); see also Brody, 280 F.3d at 1006 ("[An omission] must affirmatively create an impression of a state of affairs that differs in a material way from the one that actually exists.").<sup>6</sup>

For these reasons, the Court holds that Plaintiffs have failed to plead falsity as required by the PSLRA for **Statements 22–26** and the Court **GRANTS** Defendants' motion to dismiss as to those statements.

## e. Statements About Cambridge Analytica Investigation

Plaintiffs next argue that Defendants' statements about "the results of Facebook's investigation into Cambridge Analytica's data misuse" were false and/or misleading. SAC ¶¶ 361–66 (Statements 27–29). Plaintiffs claim it was misleading for Defendant Facebook to state in March 2017 that its "investigation to date ha[d] not uncovered anything that suggests wrongdoing with respect to Cambridge Analytica's work on the [Brexit] and Trump campaigns" because Facebook had found evidence of wrongdoing by Cambridge Analytica in or before December 2015—namely, that Cambridge Analytica had improperly accessed the data of Facebook users, had misused it during campaigns, and that Kogan had violated Facebook

<sup>&</sup>lt;sup>6</sup> For this reason, Plaintiffs reliance on *Berson v. Applied Signal Technology, Inc.*, 527 F.3d 982 (9th Cir. 2008) is misplaced. There, the company failed to disclose information that rendered its risk disclosures misleading. *Id.* at 987. In contrast, the events that Plaintiffs claim render Facebook's risk disclosures misleading were fully disclosed in 2015 (*i.e.*, before Defendant Facebook's risk disclosure statements were submitted to the SEC).

<sup>&</sup>lt;sup>7</sup> Importantly, these statements focus on Cambridge Analytica's use of misappropriated Facebook user-data on political campaigns only.

policies by transferring user data to Cambridge Analytica. Id. ¶¶ 97–100, 136–38, 141–49, 152, 365–66.

Defendants argue that the SAC lacks contemporaneous facts from which the Court can infer that, as of March 2017, Facebook had determined that the misappropriated data was still being used in connection with the Brexit and Trump campaigns. Id.; see also Reply at 13. The Court agrees. In their Opposition, for the first time, Plaintiffs allege that top management knew about Cambridge Analytica's involvement with the Trump campaign because around June 2016, Facebook embedded three employees in the Trump campaign, where the employees worked sideby-side with Cambridge Analytica people on a gigantic dataset that "was obviously the same one that had been misappropriated by Cambridge Analytica two years earlier." Opp. at 15. Yet, the SAC mentions Trump's campaign and Brexit only in passing. See SAC ¶ 164 ("Facebook [had] repeatedly lied to journalists about the severity of the Cambridge Analytica scandal as part of an alleged coverup of a privacy breach that gave up to 87 million users' personal data to the Trump-linked political firm."); Id. ¶¶ 140–43 (stating only that Facebook knew of Cambridge Analytica's involvement in Brexit, but failing to plead specific factual allegations to that effect).8

<sup>&</sup>lt;sup>8</sup> The Court cautions Plaintiffs about misrepresenting the context of an alleged misrepresentation. In their opposition, Plaintiffs contend that **Statement 28** was not limited to the Trump/Brexit campaign. Opp. at 21. By the statement's terms, this might be true. However, in context of the article in which it is quoted, it is obvious from the *title of that article alone* that **Statement 28** relates to Facebook's investigation into wrongdo-

It is well established that a complaint may not be amended by briefs in opposition to a motion to dismiss. See Diamond S.J. Enter. v. City of San Jose, 395 F. Supp. 3d 1202, 1231 (N.D. Cal. 2019). Given the dearth of allegations in the SAC linking Cambridge Analytica's privacy violations to the Brexit and Trump campaigns, there is no factual basis for this Court to conclude that Defendant Facebook made a material misrepresentation when it stated that its investigation "had not uncovered anything that suggests wrongdoing with respect to Cambridge Analytica's work on the [Brexit] and Trump campaigns." See Metzler, 540 F.3d at 1070 ("The PSLRA has exacting requirements for pleading 'falsity.' . . . A litany of alleged false statements, unaccompanied by the pleading of specific facts indicating why those statements were false, does not meet this standard."). Although the SAC includes voluminous allegations which tend to show that Facebook's investigation revealed wrongdoing by Kogan and Cambridge Analytica, the SAC fails to connect that wrongdoing to either the Brexit or Trump campaign. For that reason, the Court cannot conclude that **Statements 27–29** are actionable

ing during the Trump campaign. See Mattathias Schwartz, Facebook Failed to Protect 30 Million Users from Having Their Data Harvested by Trump Campaign Affiliate, Intercept (Mar. 30, 2017), https://theintercept.com/2017/03/ 30/facebook-failed-to-protect-30-million-users-from-having-their-data-harvested-by-trump-campaign-affiliate/ (discussing the models or algorithms used by the Trump campaign and stating that Facebook "continues to maintain that whatever happened during the run-up to the election was business as usual" (emphasis added)). This is to say, Statements 27–29 are all confined to Facebook's investigation of data misuse by Cambridge Analytica during the Trump and Brexit campaigns.

and the Court **GRANTS** Defendants' motion to dismiss as to these statements.<sup>9</sup>

### f. Statements About Response to Data Misuse

Statements 30–33 concern statements about Facebook's "responses to instances of data misuse." In January, February and June 2017, Defendants stated that they would take "swift action" against companies that mislead people or misuse their information and would require such companies to destroy improperly collected data. SAC ¶¶ 368–70 (Statements 30–32). In March 2018, Defendants stated that they were "committed to vigorously enforcing their policies to protect people's information" and would take necessary steps against third-parties who had misused data. *Id.* ¶ 376 (Statement 33). Plaintiffs argue that

<sup>&</sup>lt;sup>9</sup> Plaintiffs again rely on the SEC Complaint to show falsity as to **Statements 27–29**. A closer look at the SEC Complaint, however, reveals that the SEC's complaint contains no allegations linking Cambridge Analytica's policy violation to the Brexit or Trump campaign; in fact, the complaint omits that portion of the challenged statement all together. Ex. 15, Dkt. 126-16.

Secondly, the SAC includes a footnote, see ¶ 152 n.131, which references an article in which Roger McNamee, a Facebook investor and mentor of Defendant Zuckerberg, discusses how Facebook had three employees infiltrate President Trump's campaign. Pursuant to the incorporation by reference doctrine, the Court can consider this article. However, Plaintiffs do not argue that this footnote alone meets the PSLRA's specificity requirements and the Court cannot find any precedent stating that the PSLRA's requirements can be met through the incorporation by reference doctrine. For that reason, the Court finds that this footnote does not show "specific facts" demonstrating falsity. See Irving Firemen's Relief & Ret. Fund v. Uber Techs., 2018 WL 4181954, at \*6 (N.D. Cal. Aug. 31, 2018) (noting that, in this district, courts have rejected the "laborious deconstruction and reconstruction of a great web of . . . allegations").

these statements were misleading because Facebook did not: (1) take swift action against third parties who had misused information; (2) require data misusers to destroy or delete improperly collected data; or (3) vigorously enforce its policies. *Id.* ¶¶ 375, 379.

The Court previously dismissed these statements. The analysis underlying that dismissal has not changed. When **Statements 30-32** were made in 2017, Facebook "[had] investigate[d] the alleged data misuse, [had] remove[d] Kogan's app from Facebook, and [had] obtain[ed] certifications and confirmations that all user data had been destroyed." September 2019 Order at 30; see also SAC ¶¶ 137–38; supra III.C.1.a. Likewise, Facebook never made a promise that it would "automatically" require improperly collected data to be destroyed. Facebook only promised that it would require the data to be destroyed; it did not specify the means it would use to ensure such deletion. Thus, relying on certifications of deletion however unverified and self-serving those certifications may have been—was permissible. See SAC ¶¶ 138, 144, 171-80. This Court thus cannot say that **Statement 33** was false when made because it is not clear that Facebook was neither committed "to vigorously enforcing [its] policies to protect people's information" nor taking "whatever steps [were] required" (whatever those might be) against third parties who had misused user information. 10 For these reasons,

<sup>&</sup>lt;sup>10</sup> Moreover, **Statement 33** is seemingly inactionable puffery. "[S]tatements projecting 'excellent results,' a 'blowout winner' product, 'significant sales gains,' and '10% to 30% growth rate over the next several years" have been held not actionable as mere puffery. *In re Fusion-io*, 2015 WL 661869, at \*14 (citing *In re Cornerstone Propane Partners, L.P. Sec. Litig.*, 355 F. Supp.

the Court holds that Plaintiffs have failed to plead falsity as required by the PSLRA for **Statements 30–33** and the Court **GRANTS** Defendants' motion to dismiss as to these statements.

### g. Statements About User Consent

**Statement 34** pertains to the issue of consent, specifically whether users knowingly provided Kogan with their data. This Court previously held that these statements were not actionable. Plaintiffs allege three main theories of misconduct regarding consent: (i) third-party consent (*i.e.*, allowing a user to give share information about their friends with third-party app developers), (ii) whitelisting, and (iii) sharing of data with third-parties contrary to stated policy. At issue here is (i) and (ii). See *id.* ¶ 89 (admitting that specific users who took Kogan's quiz consented to Kogan's app's use of their personal data, but arguing that the app's access of the personal data of users' friends' violated the then-existing privacy policy).

Under the first consolidated complaint **Statement 34** was not "false," because the operative privacy policy in 2014 (which is when users allegedly took the quiz) allowed for third-party consent. *See* September 2019 Order at 43. In their SAC, Plaintiffs allege that the user data obtained by Cambridge Analytica was taken *after* the April 2014 announcement in which Defendant Zuckerberg pledged to shut off third-party access. SAC ¶¶ 89, 101. Allegedly, in the summer and early fall of 2014—after the April 2014 announcement—GSR (controlled by Kogan) retained

<sup>2</sup>d 1069, 1087 (N.D. Cal. 2005)). A promise to "vigorously enforce" privacy policies or "take whatever steps necessary" is comparable to the vague, generalized statements of corporate optimism discussed in *In re Fusion-io*.

a surveying firm to recruit and pay approximately 270,000 Facebook users to download Kogan's app and take his personality quiz. From this, Kogan collected the Facebook data of the 270,000 takers and many app users' friends. Id. ¶ 104. This is how Kogan was able to harvest the data from 50 million people. Id. ¶ 106. And, this is the data that was later sold to Cambridge Analytica.

Plaintiffs maintain that the above timeline resolves the issue of third-party consent. In their view, because Facebook announced in April 2014 that it would change its policy of allowing third-party consent, Defendant Zuckerberg falsely stated in 2018 that "everyone gave their consent." A closer look at the April 2014 announcement reveals a different story. According to the April 2014 announcement, "existing apps [had] a full year to upgrade." Ex. 30, Dkt. 126-31. Importantly, GSR's collection method relied on a "pre-existing application functioning under Facebook's old terms of service." SAC ¶ 103. The "This Is Your Digital Life" app thus predated the April 2014 announcement; indeed, as Plaintiffs admitted in their earlier complaint, the app was developed in 2013. September 2019 Order at 4. So, when GSR collected user data in June 2014, pursuant to the privacy policy in place, everyone did give their "consent." Accordingly, it is irrelevant that GSR harvested the data after the April 2014 announcement. The dispositive inquiry is when was the application that allowed such data harvesting authorized. Pursuant to Plaintiffs' own pleadings, the app was authorized before the April 2014 announcement and thus third-party consent was permissible until April 30, 2015. Ex. 30, Dkt. 126-31. For these reasons, Plaintiffs still have not shown that **Statement 34** was false when made and the Court **GRANTS** Defendants' motion to dismiss as to this statement.

Statement 35 discusses actions allegedly taken by Facebook to make the platform "safer." Specifically, in 2014, the platform was changed to "dramatically limit the data apps could access." SAC ¶ 383. Plaintiffs have plead falsity as to this statement. When Statement 35 was made, Facebook allegedly continued to provide user data to "whitelisted" app developers, mobile device makers, and others, often in contravention of users' privacy settings. *Id.* ¶¶ 384, 387. Accordingly, in light of the alleged secret whitelisting, it was not the case that Facebook had "limit[ed] the data apps could access" or that a Cambridge Analytica-type event would not occur again, see *supra* III.C.1.b. For this reason, the Court **DENIES** Defendants' motion to dismiss as to this statement.

# h. Statements About Compliance with FTC Consent Decree

**Statements 36–42** pertain to statements made by Defendants about Facebook's compliance with the 2012 FTC consent decree. *See id.* ¶¶ 388–403.

In the Ninth Circuit, "vague, generalized assertions of corporate optimism or statements of 'mere puffing' are not actionable material misrepresentations under federal securities laws" because no reasonable investor would rely on such statements. *In re Fusion-io*, 2015 WL 661869, at \*14 (collecting cases). When valuing corporations, investors do not "rely on vague statements of optimism like 'good,' 'well-regarded,' or other feel good monikers." *In re Cutera*, 610 F.3d at 1111. Statements like "[w]e are very pleased with the learning from our pilot launch," "so far we're getting really great feedback," and "we are very

pleased with our progress to date," are inactionable puffery. Wozniak v. Align Tech., Inc., 2012 WL 368366, at \*4–5 (N.D. Cal. Feb. 3, 2012). Likewise, "statements projecting 'excellent results,' a 'blowout winner' product, 'significant sales gains,' and '10% to 30% growth rate over the next several years" have been held not actionable as mere puffery. In re Fusionio, 2015 WL 661869, at \*14 (citing In re Cornerstone Propane Partners, 355 F. Supp. 2d at 1087).

In **Statement 39** Defendant Zuckerberg stated that Facebook "worked hard to make sure that" it was in compliance with the FTC consent decree. SAC  $\P$  39. Plaintiffs argue that this statement was misleading because Defendants were violating the FTC consent decree by allowing third-parties to access user data, in contravention of user privacy settings. *Id.*  $\P$  396. Defendants argue that this statement is too vague to be actionable. The Court previously held that this statement was too vague to be actionable. That opinion has not changed.

First, courts often hold that statements regarding general compliance are too vague to be actionable misrepresentations or omissions. See, e.g., Lomingkit v. Apollo Educ. Grp. Inc., 2017 WL 633148, at \*23 (D. Ariz. Feb. 16, 2017). Plaintiffs argue that **Statement 39** was not a "general" statement of corporate compliance, but rather was a specific representation about a specific consent decree. As support, Plaintiffs rely on Hefler v. Wells Fargo & Co., 2018 WL 1070116, at \*8 (N.D. Cal. Feb. 27, 2018). There, the defendant (Wells Fargo) was under investigation following improper sales activities. An executive stated that the company was having a "terrific reaction from our regulators from a compliance standpoint." Id. The court determined that this was an actionable misrepresentation

because a reasonable investor would not consider a regulatory investigation a "terrific reaction." Plaintiffs argue that like *Hefler*, **Statement 39** is actionable because it creates a contrary impression of the existing state of affairs. The Court disagrees. First, unlike in *Hefler*, there was no ongoing regulatory investigation. Second, Defendant Zuckerberg did not value Facebook's compliance efforts—that is, he did not state that Facebook was doing a "terrific" job complying. He only stated that Facebook was working "very hard" to ensure that they were compliant. This is the exact type of vague, unverifiable statement that courts routinely hold inactionable. See Wozniak, 2012 WL 368366, at \*4-5. For this reason, the Court **GRANTS** Defendants' motion to dismiss as to **State**ment 39.

In **Statements 37–38 and 40–41**, Defendants made representations about following and/or trying to follow the 2012 FTC consent decree. In **Statements 36 and 42**, Defendants discuss the risks of non-compliance. Plaintiffs maintain that **Statements 36–38** and 40–42 are material misrepresentations because, at the time the statements were made, Defendants knew that they were violating aspects of the FTC consent decree and failed to disclose such violations and/or presented violations as hypothetical risks. SAC ¶¶ 400, 402–03. Defendants, however, had no obligation to tell investors that they *might* not be in compliance with the FTC consent decree. Indeed, companies are not required to engage in "self-flagellation" by disclosing unproven allegations. Haberland v. Bulkeley, 896 F. Supp. 2d 410, 426 (E.D.N.C. 2012); In re Paypal Holdings, Inc., 2018 WL 466527, at \*3 (N.D. Cal. Jan. 18, 2018) ("Federal securities laws do not impose upon companies a 'duty to disclose uncharged, unadjudicated wrongdoing." (citing City of Pontiac Policemen & Firemen Ret. Sys. v. UBS AG, 752 F.3d 173, 184 (2d Cir. 2014)). Defendants thus had no duty to disclose unproven allegations.

Despite recognizing the absence of a duty to disclose alleged FTC-violations, Plaintiffs argue that because Defendants "chose to speak on [the FTC consent decree]," they had an obligation not to make material misrepresentations about it. This is of course true. See Hefler, 2018 WL 1070116, at \*8. But, Plaintiffs invert this obligation and predicate the material misrepresentations on Defendants' failure to discuss the alleged FTC violations. This is perplexing—the law is clear that Defendants had no duty to disclose unproven violations.

At the time **Statements 36–38 and 40–42** were made, the FTC only stated an *intent* to investigate Facebook, but had not made any formal findings that Facebook violated the 2012 decree order. September 2019 Order at 27. Defendants had no obligation or requirement to elaborate on any alleged non-compliance because they had not yet been found to be noncompliant. Hence, at the time of these statements (specifically, at the time of the risk disclosures) the risk of being found non-compliant was hypothetical. See In re Teledyne Defense Contracting Deriv. Litig., 849 F. Supp. 1369, 1382 (C.D. Cal. 1993) (dismissing securities violation claim because directors need not disclose alleged wrongdoing "when such charges have not yet been brought, let alone proven"). For these reasons, the Court **GRANTS** Defendants' motion to dismiss as to Statements 36-38 and 40-42.

### i. Statements About User Notification

Statements 43 & 44 refer to statements made by Defendant Facebook in an April 2017 white paper. SAC ¶¶ 405–06. In the white paper, Defendants stated they would "notify specific people" targeted by sophisticated attackers and "proactively" notify people they believed would be targeted. Id. Plaintiffs argue that these statements are materially false and misleading because Defendants did not "notify" Facebook users whose accounts were compromised or at risk of being compromised; did not provide "notifications to specific people" whose accounts or data had been targeted or compromised; and did not provide "proactive notifications to people" whose data may be at risk. Id. ¶ 407. As support, Plaintiffs point to Defendant Zuckerberg's Senate testimony, in which he confirms that "there was a decision made" not to notify the tens of millions of users whose data was compromised pursuant to the Cambridge Analytica datascandal, see id. ¶ 408, and to Defendant Sandberg's admission that Facebook has "the responsibility to disclose to people when problems occur, see id.  $\P$  409.

The Court previously considered these statements and found them not to be false. Again, "Plaintiffs seem to ignore that these statements refer to 'targeted' data collection and theft." September 2019 Order at 38; see also Ex. 28, Dkt. 126-29 (emphasis added). Specifically, this page advised users about protecting their

accounts from data collection by methods like "phishing<sup>11</sup> with malware to infect a person's computer and credential theft to gain access to . . . online accounts." Ex. 28, Dkt. 126-29. The portion of the white paper that Plaintiffs cite expressly focuses on bad actors who "steal" user data using methods like phishing. Moreover, notification is limited to persons targeted by "sophisticated attackers," or persons "suspected of working on behalf of a nation-state." Id. at n.5. The SAC does not allege that Cambridge Analytica or any of the whitelisted developers used methodologies like phishing to gain access to user data or that such actors were suspected of working on behalf of a nation-state (the closest allegation is about Huawei and Mail.Ru Group, but Plaintiffs only allege that Huawei has "deep ties" to the Chinese government and that Mail.Ru is connected to the Kremlin). See SAC ¶ 16. Thus, the factual background of this action does not render **Statements 43 & 44** false because Plaintiffs' SAC focuses on situations where app developers had valid access to the Facebook platform. See Hong v. Extreme Networks, Inc., 2017 WL 1508991, at \*15 (N.D. Cal. Apr. 27, 2017) (holding that the plaintiffs' allegations of falsity were insufficient because "the reasons Plaintiffs offer as to why the statements are false or misleading bear no connection to the substance of the statements themselves").

<sup>&</sup>lt;sup>11</sup> As noted in the Court's earlier order, phishing is "a cybercrime in which a target or targets are contacted by email, telephone, or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords." *What Is Phishing?*, Phising.org, https://www.phishing.org/what-is-phishing (last visited July 27, 2020).

Defendant Sandberg and Zuckerberg's 2018 statements do not change this analysis. Even while Executive Defendants expressed that they "should have" informed users and that they "got [it] wrong" by withholding notice from Cambridge Analytica victims, Defendants statements of regret over how the Cambridge Analytica scandal was handled do not render unrelated statements false. For these reasons, the Court **GRANTS** Defendants' motion to dismiss as to **Statements 43 and 44.** 

# j. Statement About GDPR Compliance

**Statement 45** is about Defendant Facebook's compliance with the GDPR. SAC ¶¶ 411–13. During an October 2017 interview, Defendant Sandberg stated that "Europe[] has passed a single privacy law [i.e., the GDPR] and **we are adhering to that**. But privacy is something we take really seriously." *Id.* ¶ 411. Plaintiffs maintain that this statement was materially false and misleading because at the time of the statement Defendant Facebook was not "adhering to" the GDPR, as demonstrated by Facebook overriding users' privacy settings to allow whitelisted developers access to user data. *Id.* ¶ 412.

The Court previously considered this statement and found that Plaintiffs failed to allege falsity. That analysis has not changed. September 2019 Order at 43–44. As the Court previously held, **Statement 45** expressed an intention to adhere to the GDPR; it is not a profession of being fully compliant. Indeed, GDPR did not become effective until May 25, 2018. SAC ¶ 229. Thus, **Statement 45** cannot be rendered false by Facebook's alleged failure to fully comply with the GDPR, which was not even in effect at the time the statement was made. For this reason, the Court holds

that Plaintiffs failed to plead falsity as required by the PSLRA for **Statement 45** and the Court thus **GRANTS** Defendants' motion to dismiss as to this statement.

## k. Statements About Use of Platform to Influence Elections

**Statements 46–48** pertain to statements made by Defendants about Russian interference in the U.S. elections. Id. ¶¶ 414–19. Plaintiffs allege that it was false for Facebook's then-general counsel (Mr. Stretch) to state that the Company had provided "everything we have to date" regarding Russian efforts to influence the 2016 election, and that it was false for Mr. Stretch to say that Facebook had seen "only what appear[ed] to be insignificant overlap between the targeting and content used by the [Russian Internet Research Agency] and that used by the Trump campaign." Id. ¶¶ 414–15. Plaintiffs argue that these statements were materially false and misleading when made because the statements do not to include information about the results of Facebook's Cambridge Analytica investigation, which should have revealed that user data had repeatedly been used to design effective political advertising for the 2016 Trump campaign. Id. ¶¶ 416–18.

Plaintiffs, however, have failed to allege facts that show that **Statements 46–48** were false when made. That is, Plaintiffs have not plead specific facts from which the Court can infer that Facebook *had not* provided complete information about Russian efforts to influence the 2016 election or that Facebook *had seen* significant overlap between the targeting and content used by the Russian IRA and the Trump campaign. See Brody, 280 F.3d at 1006 (statements are only misleading if they "affirmatively create an impression of

a state of affairs that differs in a material way from the one that actually exists").

Plaintiffs further argue that **Statement 48** was misleading because there was a significant risk that Kogan's data (and thus Cambridge Analytica's data) was similar to the Russian IRA's data since "Kogan had worked closely with Russian operatives in the past, giving rise to a heightened risk that data provided to Cambridge Analytica had been obtained by Russian agents either before or after the [Cambridge Analytica data scandal was originally reported." *Id*. ¶ 419. But, this is mere speculation—the Court cannot infer that Facebook had seen "significant overlap" between the user data used by Russian IRA and the Trump campaign based on Plaintiffs' bare allegation that "Kogan worked closely with Russian operatives." See In re Stratosphere Corp. Sec. Litig., 1997 WL 581032, at \*13 (D. Nev. May 20, 1997) (circumstantial evidence to show falsity must be plead with particularity). Accordingly, the Court cannot conclude that **Statements 46–48** are false because Plaintiffs have not met their burden of showing particular facts from which this Court can infer falsity. The Court thus **GRANTS** Defendants' motion to dismiss as to these statements.

#### l. Statements About User Metrics

Statements 49–62 pertain to statements by Defendants about Facebook's Daily Active User ("DAU") and Monthly Active User ("MAU") metrics. SAC ¶¶ 420–21. Plaintiffs argue that these statements were misleading because at the time the DAU and MAU figures were collected in 2017, Facebook was using an "incorrect methodology to calculate duplicate accounts," which caused Facebook to overstate its

user-figures. Id. ¶ 423 ("Facebook admitted to this reality on November 1, 2017, when it implemented a 'new methodology for duplicate accounts that included improvements to the data signals we rely on to help identify such accounts."). Plaintiffs further argue that the statements are materially false and misleading because Defendants failed to account for the number of fake accounts on Facebook. Id. ¶ 424 ("In May 15, 2018, Facebook announced for the first time that it had deleted a total of 1.277 billion fake accounts during the period from Q4 2017 to Q2 2018."). Lastly, Plaintiffs argue that the statements are materially false and misleading because Defendants omitted to include information about (1) their whitelisting privacy practices and (2) how the active user engagement metrics were not reliable indicators of the health or strength of Facebooks business. *Id.* ¶ 425.

As this Court noted in its earlier order, simply using a new methodology to count accounts is not misleading. See Ironworkers Local 580—Joint Funds v. Linn Energy, LLC, 29 F. Supp. 3d 400, 426 (S.D.N.Y. 2014) (rejecting claim that changed formula for calculating financial metrics amounted to "some sort of admission that statements made in prior reporting periods were false or materially misleading"). There is no requirement that companies like Facebook use specific methods to calculate user engagement (or at least Plaintiffs have not identified such a requirement). Plaintiffs' effort to transform Defendants' business decision to change its methodologies into some sort of admission that its prior statements were false and materially misleading is misguided and rejected.

Likewise, Plaintiffs' omission arguments are rejected. The necessary predicate to any action under

the securities laws is either (1) making a "misstatement" or (2) omitting to say something that is needed in order for the full truth to be told. *Id.* at 426. Thus, in order for **Statements 49-62** to contain omissions. Plaintiffs must plead specific facts that tend to show that the statement only told "half" the truth or that a defendant had a "duty to disclose" information but failed to do so. Basic, 485 U.S. at 239 n.17; see also supra III.C.1.a. Plaintiffs have not met this burden. First, Plaintiffs argue that Defendants omitted information about their whitelisting practices. Yet, nowhere in **Statements 49–62** do Defendants make any qualitative comment about user growth. Rather, each statement is quantitative—Defendants thus cannot be said to have told a "half-truth" by not discussing their whitelist policy because they never promised any results. Perhaps if Defendants had made guarantees about continued user growth, this Court could find that they made a material omission by failing to include information about whitelisting (which, as Plaintiffs note, would be likely to affect user engagement). But, that is not the case—simply stating the relevant data and promising to "continue to monitor" user engagement makes no promise about future results.

Second, Plaintiffs argue that Defendants omitted information about the reliability of their user metrics. Again, nowhere in **Statements 49–62** do Defendants make any promises about the reliability of their metrics, nor is there any identifiable requirement for Defendants to do so. *See Basic*, 485 U.S. at 239 n.17. It thus cannot be said that Defendants presented a "half" truth by presenting their data.

For these reasons, the Court holds that Plaintiffs have failed to plead falsity as required by the PSLRA for **Statements 49–62** and the Court **GRANTS** Defendants' motion to dismiss as to those statements.

## m. Statements About 1Q18 Results

**Statements 65 and 66**<sup>12</sup> relate to statements made by Defendants during Facebook's 1Q18 Earnings Call. SAC ¶¶ 427–43. In these statements, Defendants discussed Facebook's 1Q18 financial results and the anticipated impact of GDPR on Facebook. Plaintiffs claim that these statements were false or misleading because they were meant to "assure investors that the Cambridge Analytica data scandal had not, and would not, have a meaningful financial impact on the business" and that "data breaches like Cambridge Analytica scandal were behind the company." Id. ¶ 432.

Under the PSLRA "Safe Harbor" Provision, "forward-looking statements are not actionable as a matter of law if they are identified as such and accompanied by "meaningful cautionary statements identifying important facts that could cause actual results to differ materially from those in the forward looking statement." 15 U.S.C. § 78u-5(c)(1)(A)(i). A forward-looking statement is "any statement regarding (1) financial projections, (2) plans and objectives of management for future operations, (3) future economic performance, or (4) the assumptions 'underlying or related to' any of these issues." No. 84 Emp'r Teamster Joint Council Pension Trust Fund v. Am. W. Holding Corp., 320 F.3d 920, 936 (9th Cir. 2003) (citing 15 U.S.C. § 78u5 (i)). "[I]f a forward-looking statement is

<sup>&</sup>lt;sup>12</sup> For the reasons discussed in III.C.1.k, **Statements 63 & 64** are not plead with sufficient falsity. These statements pertain to statements about DAU and MAU data. The Court **GRANTS** Defendants' motion to dismiss as to those statements.

identified as such and accompanied by meaningful cautionary statements, then the state of mind of the individual making the statement is irrelevant, and the statement is not actionable regardless of the plaintiff's showing of scienter." *In re Cutera Sec. Litig.*, 610 F.3d 1103, 1112 (9th Cir. 2010).

Here, Defendants argue Statements 65 and 66 are forward-looking statements protected by the PSLRA's Safe Harbor. 13 The Court agrees. Statement 65 is a statement about Facebook's intent to use GDPR to strengthen its privacy policies and its commitment to improving its ads model. Management's plans or objectives for future operations and predictions of future economic performance are protected forward-looking statements. 15 U.S.C. 5(i)(1)(A)–(C). At bottom, **Statement 65** concerns Executive Defendants' objectives for future Facebook operations. See SAC ¶ 430 ("Going forward, we will continue to focus on [GDPR, ad improvement, and choicel." (emphasis added)). Because **Statement 65** is an inactionable forward-looking statement accompanied by meaningful cautionary language, see n.11, the Court **GRANTS** Defendants' motion to dismiss as to this statement.

**Statement 66** is also a forward looking statement; it concerns predictions of the impact of the GDPR on ad revenue. *See* September 2019 Order at 26 (holding comparable statement inactionable). Specifically, Defendant Wehner stated that he did not "ex-

<sup>&</sup>lt;sup>13</sup> Importantly, at the start of the earnings call, Defendants reminded investors that the remarks may "include forward-looking statements" and that "[a]ctual results may differ." Ex. 10, Dkt. 126-11.

pect [GDPR to] significantly impact advertising revenue" and that Defendants believed any effect to be "relatively minor." SAC ¶ 431. This statement plainly concerns Facebook's future economic performance in light of GDPR. See 15 U.S.C. § 78u–5(i)(1)(A)–(C). The statement is accompanied by meaningful cautionary language. See supra n. 11; see also SAC ¶ 431 (Defendant Wehner acknowledged that there was potential "for some impact"). Because **Statement 66** is an inactionable forward-looking statement accompanied by meaningful cautionary language, the Court **GRANTS** Defendants' motion to dismiss as to this statement.

In **Statement 68**, Defendant Zuckerberg stated that he believed the vast majority of people "want their data used." SAC ¶ 437. Plaintiffs claim that this statement was false and/or misleading because it was meant to assure investors that GDPR would not cause (and had not caused) a decline in active use of Facebook's platform and portrayed Facebook as GDPRcompliant. *Id.* ¶ 438. Plaintiffs further claim that the statement omitted information about Defendants' privacy misconduct. Plaintiffs have not sufficiently alleged falsity—they do not allege facts tending to show that people did *not* want their data used. Moreover, the statement says nothing about GDPR compliance or the costs associated with compliance. See Hong, 2017 WL 1508991, at \*15. Moreover, Defendants' alleged privacy misconduct has no bearing on this statement. Plaintiffs allege no reason why users' decision to opt-in to data sharing would be effected by any alleged privacy misconduct. For these reasons, Plaintiffs have not alleged falsity as to **Statement 68** and the Court **GRANTS** Defendants' motion to dismiss as to this statement.

Plaintiffs have plead sufficient falsity as to **State**ments 67 and 69. In Statement 67, Defendant Zuckerberg stated that situations "like" the Cambridge Analytica scandal would not occur again. Id. ¶ 434. But, accepting Plaintiffs' whitelisting allegations as true, "Facebook had not been protecting privacy" and so there was a risk that a Cambridge Analytica-type scandal could occur again. *Id.* ¶ 435. **Statement 69** is materially misleading for the same reason—the statement assures users and investors that users' control their data and that Facebook has "strong protections" in place for user information. Id. ¶ 440. However, Plaintiffs' whitelisting allegations render this statement misleading. For these reasons, Defendants' motion to dismiss Statements 67 and 69 on falsity grounds is **DENIED**.

## n. Statements About the Sale of User Data

**Statements 70–83** concern comments made by Facebook that it does not "sell data." SAC ¶¶ 444–60. Plaintiffs maintain that these statements were materially misleading because Facebook used user friend data "as consideration for a reciprocal exchange of value with third-party app developers and other companies who were 'whitelisted' for secret access to user friend data." *Id.* However, Plaintiffs (as they admit in their Opposition) do not allege that Facebook did sell data. To the contrary, Plaintiffs maintain that "selling" data includes data-bartering. Opp. at 27. Not so. "Selling" user data contemplates a cash-for-data transaction. Indeed, this is the type of transaction contemplated by Defendants when **Statements 70**-83 were made. See, e.g., SAC ¶ 448 ("[W]e don't buy and sell [data]." (emphasis added)). Plaintiffs do not allege any facts from which this Court can plausibly infer that Defendants did sell (i.e., for cash) user data. The closest Plaintiffs get is by pointing the court to a September 2013 email chain, which shows Facebook Directors discussing the fact that Facebook was requiring third-party app developers to "spend on [advertising at Facebook at least \$250,000 a year to maintain access to the data." Id. ¶ 72. There are no allegations, however, about which advertisers were required to do this, whether all advertisers were required to do this, or if Facebook actually required such spending to maintain data-access. See id. ¶ 459; see also Metzler, 540 F. 3d at 1070. Plaintiffs thus have not plead specific facts showing that Defendants sold data and thus have not alleged falsity for **Statements** 70-81. The Court **GRANTS** Defendants' motion to dismiss as to these statements.

Parts of **Statements 82 & 83** are actionable. For the above reasons, the Court holds that the portions of these statements that refer to selling of information are not actionable. However, the portions of the statements that state Facebook does not "share" or "give" user information to "third parties" are actionable. As discussed above, Plaintiffs have plead sufficient facts to show falsity—Plaintiffs have demonstrated that, despite guarantees to the contrary, Facebook was sharing user data (including user friend data) to third-parties via whitelisting. See SAC ¶¶ 16, 63–80, 444–60. Accordingly, the portions of **Statements 82** and 83 that refer to sharing—but not selling—of data are actionable.

#### 2. Scienter

Having determined that **Statements 1–21, 35, 67, 69, and parts of Statements 82 and 83** are actionable, the next issue is whether Plaintiffs have adequately pled a strong inference of scienter.

Scienter is required under the PSLRA and plaintiffs must plead "with particularity facts giving rise to a strong inference that the defendant acted with the requisite state of mind" regarding "each act or omission alleged." 15 U.S.C. § 78u-4(b)(2)(A). It can be established by intent, knowledge, or certain levels of recklessness. In re Verifone Holdings, Inc. Sec. Litig., 704 F.3d 694, 702 (9th Cir. 2012). Recklessness must be deliberate. Schueneman v. Arena Pharma., Inc., 840 F.3d 698, 705 (9th Cir. 2016) ("[S]cienter—a mental state that not only covers 'intent to deceive, manipulate, or defraud,' but also 'deliberate recklessness." (citations omitted)). Deliberate recklessness is an "extreme departure from the standards of ordinary care ... which presents a danger of misleading buyers or sellers that is either known to the defendant or is so obvious that the actor must have been aware of it." *Id.* Thus, recklessness only satisfies scienter under § 10(b) to the extent it reflects some degree of intentional or conscious misconduct. In re NVIDIA Corp. Sec. Litig., 768 F.3d 1046, 1053 (9th Cir. 2014).

A "strong inference" of scienter exists "only if a reasonable person would deem the inference of scienter cogent and at least as compelling as any opposing inference one could draw from the facts alleged." *Tellabs*, 551 U.S. at 324. In reviewing a complaint under this standard, the court must consider "all reasonable inferences to be drawn from the allegations, including inferences unfavorable to the plaintiffs." *Metzler*, 540 F.3d at 1061. To plead a strong inference of scienter, plaintiffs must plead particularized facts demonstrating that the individual defendants knew the supposedly false statements challenged by the plaintiffs were false or misleading when made or had access to information demonstrating that the individual defendants

were deliberately reckless in allowing the false statements to be made. See id. at 1068.

In **Statements 1–21**, Defendants claimed that users could "completely control" their data, that users could use "privacy and application setting" to control their data, that the platform was focused on "transparency and control," and that Facebook "respected the privacy settings that people had in place." The Court found above that Plaintiffs adequately alleged falsity as to these statements because of Defendants' "whitelisting" practices.

To establish scienter for Executive Defendants Zuckerberg and Sandberg, <sup>14</sup> Plaintiffs rely on Facebook's internal documents, which show that Defendants knowingly supplied user friend data to white-listed developers. SAC  $\P$  70. An internal memo, from 2013/2014 states that "during app review, we examine the APIs [Application Programming Interfaces] that the app uses in order to determine what [is] the appropriate level of reciprocity." *Id.* The guideline for review is "take data, give data." *Id.* Facebook emails dating from September 2013 note that "the capability will remain to *give access features* which are *publicly* 

<sup>&</sup>lt;sup>14</sup> Defendants do not argue that Plaintiffs have failed to plead scienter as to Defendant Facebook. The Court finds that Plaintiffs have pled sufficient information to support a strong inference of scienter. A corporation can only act through its employees and agents, and can thus only have scienter through them. *In re ChinaCast Educ. Corp. Sec. Litig.*, 809 F.3d 471, 475 (9th Cir. 2015). Thus, to show Defendant Facebook's scienter, Plaintiffs must show scienter as to any of Facebook's senior executives. *See Cheung v. Keyuan Petrochemicals, Inc.*, 2012 WL 5834894, at \*3 (C.D. Cal. Nov. 1, 2012). Plaintiffs have met that burden. *See* III.C.2.

deprecated [i.e., discontinued] but available to white-listed apps." *Id.* ¶ 71 (emphasis added) (alteration in original).

Defendants Zuckerberg and Sandberg were involved in the decision to exchange user friends' data for reciprocal value from third parties. *Id.* ¶ 73. Internal Facebook documents show that Defendants Zuckerberg and Sandberg were actively involved in discussions about whitelist access. See id. ¶¶ 74–79. Indeed, these documents demonstrate that Defendants Zuckerberg and Sandberg were the original architects of Facebook's "full reciprocity" business model, in which Facebook gave access to user data and user friend data to certain whitelisted parties who, in a reciprocal exchange, would give Facebook data, ad revenues, or access to new users. Id. ¶¶70–80 ("Facebook employees pointed to Zuckerberg as being intimately involved in the discussions and decision-making around [whitelisting]."). These allegations show that Defendants Zuckerberg and Sandberg were actively involved in the whitelisting process and thus support an inference that Defendants Zuckerberg and Sandberg knew of Facebook's illicit whitelisting practices. Cf. Fleming v. Impax Labs. Inc., 2018 WL 4616291, at \*4 (N.D. Cal. Sept. 7, 2018) ("Even when viewed as a whole, the factual allegations in the amended complaint do not plausibly suggest that individual Defendants directly engaged in unlawful pricefixing ...." (emphasis added)).

Likewise, Plaintiffs have plead sufficient facts showing that Defendants knew that Facebook had little control over the deletion of misappropriated data and that the risk of a Cambridge Analytica type scandal could again occur due to its whitelisting practices. See Metzler, 540 F.3d at 1061. Because **Statements** 

35, 67, 69, and the relevant portions of 82 and 83 rely on the same theory of falsity, Plaintiffs have shown scienter as to these statements also.

For these reasons, the Court holds that Plaintiffs have plead scienter as to **Statements 1–5, 7–21, 35, 67, 69, and the relevant portions of 82 and 83.** The Court thus **DENIES** Defendants' motion to dismiss these statements on scienter grounds.

**Statement 6** was made by Defendant Wehner. Plaintiffs do not allege that he knew of the above emails or was involved in whitelisting. Instead, Plaintiffs argue that the Court can infer scienter through Defendant Wehner's stock sales. The Court disagrees. "Insider stock sales are not inherently suspicious; they become so only when the level of trading is dramatically out of line with prior trading practices at times calculated to maximize the personal benefit from undisclosed information." In re Vantive Corp. Sec. Litig., 283 F.3d 1079, 1093 (9th Cir. 2002), abrogated on other grounds by Gebhart v. SEC, 595 F.3d 1034 (9th Cir. 2010) (quotation marks and citation omitted). Absent from the SAC are allegations regarding Executive Defendants' holdings of Facebook stock before the sale. SAC ¶¶ 490–91, 496, 502–03; see also In re Vantive Corp. Sec. Litig., 283 F.3d at 1093 ("[B]y themselves, large numbers do not necessarily create a strong inference of fraud."). Hence, Plaintiffs have not provided "sufficient context of insider trading" to support an inference of fraud. Ronconi, 253 F.3d at 436. And, the Court cannot say that Defendant Wehner's sales are suspicious in light of his trading history. This is the only other grounds for scienter alleged as to Defendant Wehner. Because Plaintiffs have provided no particularized facts from which this Court can infer that Defendant Wehner consciously lied, the Court finds that Plaintiffs fail to plead scienter as to **Statement 6** as required by the PSLRA and so this Court **GRANTS** Defendants' motion to dismiss as to this statement.

#### 3. Reliance

Plaintiffs must plead facts showing that they relied on the allegedly false or misleading statements in purchasing Facebook stock. See ScripsAmerica, Inc. v. Ironridge Glob. LLC, 119 F. Supp. 3d 1213, 1252–53 (C.D. Cal. 2015); Matrixx Initiatives, Inc., 563 U.S. at 37–38. The reliance element "ensures that there is a proper connection between a defendant's misrepresentation and a plaintiff's injury." Halliburton Co. v. Erica P. John Fund, Inc., 573 U.S. 258, 268 (2014) (citation and quotation marks omitted). "The traditional (and most direct) way a plaintiff can demonstrate reliance is by showing that he was aware of a company's statement and engaged in a relevant transactione.g., purchasing common stock—based on that specific misrepresentation." *Id.* (citation and quotation marks omitted).

In *Basic*, the Supreme Court recognized that requiring such direct proof of reliance "would place an unnecessarily unrealistic evidentiary burden on the Rule 10b-5 plaintiff who has traded on an impersonal market." 485 U.S. at 245. To address this concern, *Basic* held that securities fraud plaintiffs can, in certain circumstances, satisfy the reliance element of a Rule 10b-5 action by invoking a rebuttable presumption of reliance, rather than proving direct reliance. *Halliburton*, 573 U.S. at 268. This "fraud-on-the-market" theory of reliance holds that "the market price of shares traded on well-developed markets reflects all publicly available information, and, hence, any mate-

rial misrepresentations." Basic, 485 U.S. at 246. Indeed, rather than scrutinize every piece of public information about a company for himself, the typical "investor who buys or sells stock at the price set by the market does so in reliance on the integrity of that price." Id. at 247. Thus, whenever the investor buys or sells stock at the market price, his "reliance on any public material misrepresentations ... may be presumed for purposes of a Rule 10b-5 action." Id.; see also In re Apple Computer Sec. Litig., 886 F.2d 1109, 1114 (9th Cir. 1989) ("In a fraud on the market case, the plaintiff claims that he was induced to trade stock not by particular representations made by corporate insiders, but by the artificial stock price set by the market in light of statements made by the insiders as well as all other material public information.").

A plaintiff relying on the fraud-on-the-market theory must make the following showings to demonstrate that the presumption of reliance applies: (1) that the alleged misrepresentations were publicly known; (2) that they were material; (3) that the stock traded in an efficient market; and (4) that the plaintiff traded the stock between the time the misrepresentations were made and when the truth was revealed. Halliburton, 573 U.S. at 268. This showing establishes a presumptive—not conclusive—showing of reliance. Hence, "[a]ny showing that severs the link between the alleged misrepresentation and either the price received (or paid) by the plaintiff, or his decision to trade at a fair market price, will be sufficient to rebut the presumption of reliance." Basic, 485 U.S. at 248. So, for example, if a defendant could show that the alleged misrepresentation did not, for whatever reason, actually affect the market price, or that a plaintiff would have bought or sold the stock even had he been aware that the stock's price was tainted by fraud, then the presumption of reliance would not apply. *Id.* at 248–49; *see also id.* at 284 ("[D]efendants must be afforded an opportunity before class certification to defeat the presumption through evidence that an alleged misrepresentation did not actually affect the market price of the stock."); *In re Kalobios Pharm., Inc. Sec. Litig.*, 258 F. Supp. 3d 999, 1008 (N.D. Cal. 2017) ("[T]he presumption may be rebutted where a defendant can show that *the truth had actually been made available* to the market through a different source." (emphasis added)); *In re Convergent Techs. Sec. Litig.*, 948 F.2d 507, 513 (9th Cir. 1991) ("[A]n omission is materially misleading only if the information has not already entered the market.").

Plaintiffs rely on the fraud-on-the-market theory to establish reliance. SAC ¶¶ 533–34. Defendants argue that Plaintiffs cannot rely on the fraud-on-themarket's presumption of reliance because the market was already aware of the core information that Plaintiffs claim was omitted—namely, that Facebook "knowingly and recklessly allowed third-party app developers to harvest and misuse user data without their knowledge and consent, including, for example, Cambridge Analytica and its affiliated companies." Mot. at 34 (citing SAC ¶ 471). Defendants are correct; as the Court noted, in December 2015, The Guardian article disclosed that Kogan collected and sold data to Cambridge Analytica and that Cambridge Analytica had used that data to create psychological profiles of voters for the purpose of assisting political campaigns. SAC ¶¶ 5, 86–92, 232, 280. Mainstream news sources reported additional details about Cambridge Analytica's misuse of Facebook user data. Id. ¶¶ 141, 146 (describing The Wall Street Journal and The Washington Post articles). Based on the content of these articles, and the credibility and wide circulation of the respective sources, the Court agrees that the market was aware of Cambridge Analytica's data misuse. *See Kalobios*, 258 F. Supp. 3d at 1009.

Of course, the market was not aware of Cambridge Analytica's *continued* misuse until the March 2018 *The Guardian* article. In March 2018, the market learned that Cambridge Analytica had not deleted the misappropriated data and had used the data in connection with President Donald Trump's campaign. Importantly, Defendants had received assurances to the contrary from Cambridge Analytica, and Plaintiffs have failed to plead facts showing that Defendants knew or should have known that these assurances were false. Thus, this theory of reliance is not viable. *See supra* III.C.1.a.

An alternative theory of reliance exists. On June 3, 2018, The New York Times revealed that Facebook allowed whitelisted developers to access user data. See Gabriel J.X. Dance et al., Facebook's Device Partnerships Explained, The New York Times (June 4, 2018), https://www.nytimes.com/2018/06/04/technology/facebook-device-partnerships.html ("Facebook continued to allow that kind of access to dozens of the world's biggest tech and hardware companies—and only began shutting down the data-sharing partnerships after the Cambridge Analytica scandal erupted in March [2018]."). Plaintiffs have shown that Defendants' statements about users "controlling" their data were false and made with scienter. See supra. Because alleged misrepresentations were publicly known; material; Facebook stock traded in an efficient market; and Plaintiffs' traded the stock between the time the misrepresentations were made and when the truth was revealed, see Halliburton, 573 U.S. at 268,

Plaintiffs have established a presumption of reliance. Defendants have not presented evidence rebutting this presumption and so the Court presumes investors relied on **Statements 1–5**, **7–21**, **35**, **67**, **69**, and the relevant portions of **82** and **83**.

#### 4. Causation

Even when deceptive conduct is properly plead, a securities fraud complaint must also adequately allege "loss causation." Lloyd v. Fin. Corp., 811 F.3d 1200, 1210 (9th Cir. 2016). Loss causation is shorthand for the requirement that "investors must demonstrate that the defendant's deceptive conduct caused their claimed economic loss." Id. Thus, like a plaintiff claiming deceit at common law, the plaintiff in a securities fraud action must demonstrate that an economic loss was caused by the defendant's misrepresentations, rather than some intervening event. Dura Pharm., 544 U.S. at 343–44. Loss causation is a "context-dependent" inquiry. Miller v. Thane Int'l, Inc., 615 F.3d 1095, 1102 (9th Cir. 2010). It is a variant of proximate cause; and so, the ultimate issue is whether the defendant's misstatement, as opposed to some other fact, foreseeably caused the plaintiff's loss. Lloyd, 811 F.3d at 1210.

Plaintiffs have not adequately plead loss causation. Having determined that the only viable theory of falsity plead in the SAC is that Defendants mislead investors as to their privacy policies based on their alleged whitelisting practices, the relevant timeframe is stock sales from February 3, 2017 to June 3, 2018 (which is when the whitelisting was revealed). Plaintiffs allege *no* facts from which the Court can infer the stock price fell in June 2018. See SAC ¶ 512. The only point that Plaintiffs' identify after the June 2018 revelations is July 26, 2018 (i.e., following Defendants

2Q18 Earnings Release). While the Court could find that the whitelisting practices affected the stock prices following the 2Q18 Earnings Release, it is unclear if this is the ultimate reason for the drop. See, e.g., SAC ¶¶ 520, 522, 526–27 (noting that stock-drop was attributed to Cambridge Analytica scandal, decline in user engagement, advertising revenues, and "related privacy concerns," including GDPR); see also supra I.A.2 (discussing 2Q18 earnings call). The Court thus cannot conclude that information about white-listing was the "ultimate reason" for a stock decline. For this reason, the Court **GRANTS** Defendant's motion to dismiss.

## 5. Plaintiffs' Section 20(a) and 20(A) Claims

Plaintiffs also bring claims for violations of Sections 20(a) and (A) of the Exchange Act. Both these claims, however, depend on a primary violation of Section 10(b) or Rule 10b-5. *Lipton v. Pathogenesis Corp.*, 284 F.3d 1027, 1035 n.15 (9th Cir. 2002) ("[T]o prevail on their claims for violations of § 20(a) and § 20A, plaintiffs must first allege a violation of § 10(b) or Rule 10b-5."). Because the Court determines Plaintiffs' claim under Section 10(b) and Rule 10b-5 fail, Defendants motion to dismiss these claims is also **GRANTED**.

#### 6. Leave to Amend

When dismissing a complaint for failure to state a claim, a court should grant leave to amend "unless it determines that the pleading could not possibly be cured by the allegation of other facts." *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000). Although the Court has determined that Plaintiffs fail to state a

claim, it is possible Plaintiffs can cure their allegations by alleging, among other things, that Facebook embedded employees in the 2016 Trump campaign and thus knew that the deletion certifications were false and by alleging more facts about the stock price following the June 3, 2018 whitelisting revelation. Accordingly, because Plaintiffs may salvage their Complaint, the Court finds amendment would not be futile. Plaintiffs' claims are therefore dismissed with leave to amend. Plaintiffs are advised that this will be their final opportunity to amend.

### IV. CONCLUSION

Defendants' motion to dismiss Plaintiffs' SAC in its entirety is **GRANTED** with leave to amend. Should Plaintiffs choose to file an amended complaint, they must do so by **September 23, 2020**. Failure to do so, or failure to cure the deficiencies addressed in this Order, will result in dismissal of Plaintiffs' claims with prejudice. Plaintiffs may not add new claims or parties without leave of the Court or stipulation by the parties pursuant to Federal Rule of Civil Procedure 15.

### IT IS SO ORDERED.

Dated: August 7, 2020

/s/ Edward J. Davila
EDWARD J. DAVILA
United States District Judge

### APPENDIX E

## STATUTORY AND REGULATORY PROVISIONS INVOLVED

## 15 U.S.C. § 78j. Manipulative and deceptive devices

It shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce or of the mails, or of any facility of any national securities exchange—

- (a)(1) To effect a short sale, or to use or employ any stop-loss order in connection with the purchase or sale, of any security other than a government security, in contravention of such rules and regulations as the Commission may prescribe as necessary or appropriate in the public interest or for the protection of investors.
- (2) Paragraph (1) of this subsection shall not apply to security futures products.
- (b) To use or employ, in connection with the purchase or sale of any security registered on a national securities exchange or any security not so registered, or any securities-based swap agreement<sup>1</sup> any manipulative or deceptive device or contrivance in contravention of such rules and regulations as the Commission may prescribe as necessary or appropriate in the public interest or for the protection of investors.
- (c)(1) To effect, accept, or facilitate a transaction involving the loan or borrowing of securities in contravention of such rules and regulations as

<sup>&</sup>lt;sup>1</sup> So in original. Probably should be followed by a comma.

the Commission may prescribe as necessary or appropriate in the public interest or for the protection of investors.

(2) Nothing in paragraph (1) may be construed to limit the authority of the appropriate Federal banking agency (as defined in section 1813(q) of title 12), the National Credit Union Administration, or any other Federal department or agency having a responsibility under Federal law to prescribe rules or regulations restricting transactions involving the loan or borrowing of securities in order to protect the safety and soundness of a financial institution or to protect the financial system from systemic risk.

Rules promulgated under subsection (b) that prohibit fraud, manipulation, or insider trading (but not rules imposing or specifying reporting or recordkeeping requirements, procedures, or standards as prophylactic measures against fraud, manipulation, or insider trading), and judicial precedents decided under subsection (b) and rules promulgated thereunder that prohibit fraud, manipulation, or insider trading, shall apply to security-based swap agreements to the same extent as they apply to securities. Judicial precedents decided under section 77q(a) of this title and sections 78i, 78o, 78p, 78t, and 78u-1 of this title, and judicial precedents decided under applicable rules promulgated under such sections, shall apply to securitybased swap agreements to the same extent as they apply to securities.

# 17 C.F.R. § 240.10b-5. Employment of manipulative and deceptive devices

It shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce, or of the mails or of any facility of any national securities exchange,

- (a) To employ any device, scheme, or artifice to defraud,
- (b) To make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading, or
- (c) To engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person,

in connection with the purchase or sale of any security.