**FOR PUBLICATION**

# UNITED STATES COURT OF APPEALS
# FOR THE NINTH CIRCUIT

| | |
|---|---|
| IN RE ALPHABET, INC. SECURITIES LITIGATION,<br><br>STATE OF RHODE ISLAND, Office of the Rhode Island Treasurer on behalf of the Employees' Retirement System of Rhode Island; Lead Plaintiff, Individually and On Behalf of All Others Similarly Situated,<br>*Plaintiff-Appellant*,<br><br>v.<br><br>ALPHABET, INC.; LAWRENCE E. PAGE; SUNDAR PICHAI; RUTH M. PORAT; GOOGLE LLC; KEITH P. ENRIGHT; JOHN KENT WALKER, JR.,<br>*Defendants-Appellees.* | No. 20-15638<br><br>D.C. No. 4:18-cv-06245-JSW<br><br>OPINION |

Appeal from the United States District Court
for the Northern District of California
Jeffrey S. White, District Judge, Presiding

Argued and Submitted February 4, 2021
San Francisco, California

Filed June 16, 2021

Before: Sidney R. Thomas, Chief Judge, and Sandra S. Ikuta and Jacqueline H. Nguyen, Circuit Judges.

Opinion by Judge Ikuta

## SUMMARY*

### Securities Fraud

The panel affirmed in part and reversed in part the district court's dismissal of a securities fraud action for failure to state a claim, vacated the district court's judgment, and remanded for further proceedings.

The State of Rhode Island filed a private securities fraud action under §§ 10(b) and 20(a) of the Securities Exchange Act of 1934 and SEC Rule 10b-5 against Google LLC, its holding company Alphabet, Inc., and individual defendants. The consolidated amended complaint alleged that defendants omitted to disclose security problems with the Google+ social network. The complaint referred to the cybersecurity problems as the "Three-Year Bug" and the "Privacy Bug." The district court granted defendants' motion to dismiss on the grounds that Rhode Island failed to adequately allege a materially misleading misrepresentation or omission and that Rhode Island failed to adequately allege scienter.

The panel held that the complaint adequately alleged that two statements made by Alphabet in its quarterly reports filed

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

with the SEC on Form 10-Q omitted material facts necessary to make the statements not misleading. Applying an objective materiality standard to the 10-Qs, the panel held that Rhode Island's complaint plausibly alleged the materiality of the costs and consequences associated with the Privacy Bug, and its public disclosure, and how Alphabet's decision to omit information about the Privacy Bug in its 10-Qs significantly altered the total mix of information available for decisionmaking by a reasonable investor.

The panel next addressed whether the complaint adequately alleged scienter for the materially misleading omissions from the 10-Q statements. The panel held that the complaint was required to plausibly allege, with the particularity required by the Private Securities Litigation Reform Act, that the maker of the statements knew about the security vulnerabilities and intentionally or recklessly did not disclose them. The panel concluded that the complaint's specific allegations, taken as a whole, raised a strong inference that defendant Lawrence Page, and therefore Alphabet, knew about the Three-Year Bug, the Privacy Bug, and a Privacy Bug Memo, and that Alphabet intentionally did not disclose this information in its 10-Q statements.

The panel further held that Rhode Island adequately alleged falsity, materiality, and scienter for the 10-Q statements. The panel therefore reversed the district court's holdings to the contrary. The panel also reversed the district court's dismissal of the complaint's § 20(a) control-person claims based on the 10-Q statements.

As to ten additional statements identified in the complaint, the panel concluded that the complaint did not plausibly allege that these remaining statements were

misleading material misrepresentations. The panel therefore affirmed the district court's dismissal of claims based on these statements.

Rhode Island argued on appeal that the district court erred in dismissing its "scheme liability claim" under Rule 10b-5(a) and (c) when it dismissed the complaint in its entirety without addressing those claims. The panel held that because Alphabet's motion to dismiss did not target Rhode Island's Rule 10b-5(a) and (c) claims, Rhode Island did not waive those claims by failing to address them in opposition to the motion to dismiss. Reversing, the panel held that the district court erred in sua sponte dismissing the Rule 10b-5(a) and (c) claims when Alphabet had not targeted them in its motion to dismiss.

---

## COUNSEL

Jason A. Forge (argued), Michael Albert, J. Marco Janoski Gray, and Ting H. Liu, Robbins Geller Rudman & Dowd LLP, San Diego, California, for Plaintiff-Appellant.

Ignacio E. Salceda (argued), Benjamin M. Crosson, Cheryl W. Foung, Stephen B. Strain, and Emily Peterson, Wilson Sonsini Goodrich & Rosati, Palo Alto, California; Gideon A. Schor, Wilson Sonsini Goodrich & Rosati, New York, New York; for Defendants-Appellees.

**OPINION**

IKUTA, Circuit Judge:

In March 2018, amid the furor caused by news that Cambridge Analytica improperly harvested user data from Facebook's social network, Google discovered that a security glitch in its Google+ social network had left the private data of some hundreds of thousands of users (according to Google's estimate) exposed to third-party developers for three years and that Google+ was plagued by multiple other security vulnerabilities. Warned by its legal and policy staff that disclosure of these issues would result in immediate regulatory and governmental scrutiny, Google and its holding company, Alphabet, chose to conceal this discovery, made generic statements about how cybersecurity risks could affect their business, and stated that there had been no material changes to Alphabet's risk factors since 2017. This appeal raises the question whether, for purposes of a private securities fraud action, the complaint adequately alleged that Google, Alphabet, and individual defendants made materially misleading statements by omitting to disclose these security problems and that the defendants did so with sufficient scienter, meaning with an intent to deceive, manipulate, or defraud.

I

A

At the motion to dismiss stage, we start with the facts plausibly alleged in the complaint, documents incorporated into the complaint by reference, and matters of which a court may take judicial notice. *See Ashcroft v. Iqbal*, 556 U.S. 662,

678–79 (2009); *Tellabs, Inc. v. Makor Issues & Rts., Ltd.*, 551 U.S. 308, 322 (2007). The story begins in the 1990s when Lawrence Page and Sergey Brin, then students at Stanford University, developed Google, a web-based search engine. Over the next two decades, Google rapidly expanded beyond its search engine services into a range of other internet-related services and products, including advertising technology, cloud computing, and hardware.

Since its initial public offering prospectus in 2004 and throughout Google's continued rise, Google and its executives publicly recognized the importance of user privacy and user trust to Google's business. Google executives expressed their understanding that Google's "success is largely dependent on maintaining consumers' trust" so that "users will continue to entrust Google with their private data, which Google can then monetize." As one media outlet put it, "Google has a strong incentive to position itself as a trustworthy guardian of personal information because, like Facebook, its financial success hinges on its success to learn about the interests, habits and location[s] of its users in order to sell targeted ads." Google and its executives repeatedly emphasized that maintaining users' trust is essential and that a significant security failure "would be devastating." Google's public emphasis on user trust and user privacy remained central to its business when, in 2011, Google launched Google+ "in an attempt to make a social media network to rival that of Facebook and Twitter, and to join all users of Google services (*i.e.*, Search, Gmail, YouTube, Maps) into a single online identity."

In October 2015, Google restructured itself from Google, Inc. into Google LLC and created Alphabet, Inc. as its parent company, which is "essentially a holding company" whose

"lifeblood is Google." Page, who had been the CEO of Google, became the CEO of Alphabet. Sundar Pichai, a longtime Google senior executive, replaced Page as the CEO of Google. Page and Pichai both sat on Alphabet's Board of Directors and served on the board's three-person Executive Committee. Pichai directly reported to Page and maintained regular contact with him; Pichai was also directly accountable to Page. Pichai also participated in Alphabet's public earnings calls. Page received weekly reports of Google's operating results and continued to make "key operating decisions" at Google.

Google's corporate restructuring did not change the central importance of privacy and security. Google and Alphabet consistently indicated that Google's foremost competitive advantage against other companies was its sophistication in security. Thus, according to Alphabet's Chief Financial Officer in February 2018, security is "clearly what we've built Google on."

While highlighting expertise in security and data privacy, Google and Alphabet also acknowledged the substantial impact that a cybersecurity failure would have on their business. According to Alphabet's 2017 Annual Report on Form 10-K filed with the Securities and Exchange Commission (SEC), "[c]oncerns about our practices with regard to the collection, use, disclosure, or security of personal information or other privacy related matters, even if unfounded, could damage our reputation and adversely affect our operating results." Alphabet warned that "[i]f our security measures are breached resulting in the improper use and disclosure of user data" then Alphabet's "products and services may be perceived as not being secure, users and customers may curtail or stop using our products and

services, and we may incur significant legal and financial exposure." As Pichai explained in January 2018, "users use Google because they trust us and it is something easy to lose if you are not good stewards of it. So we work hard to earn the trust every day."

B

"By the spring of 2018, the trustworthiness of technology and those who control it were under unprecedented scrutiny." According to the complaint, a trigger for this scrutiny was the publication of reports that a research firm, Cambridge Analytica, "improperly harvested data from Facebook users' profiles" to be used for political advertising. The immediate effects of this reporting were "devastating to Facebook and its investors," including a 13% decline in Facebook's stock price, which amounted to a loss of approximately $75 billion of market capitalization.

This scandal quickly led to congressional hearings into Facebook's leak of user information to a third-party data collector. Facebook was not the only target of scrutiny, as the Senate Judiciary Committee, chaired by Senator Grassley, requested that Google and Twitter testify at these hearings about their data privacy and security practices. In a letter to Pichai, Senator Grassley outlined the committee's "significant concerns regarding the data security practices of large social media platforms and their interactions with third party developers and other commercial[] users of such data." According to Senator Grassley, Pichai declined to testify after "asserting that the problems surrounding Facebook and Cambridge Analytica did not involve Google."

At around the same time, in May 2018, the European Union implemented the General Data Protection Regulation (GDPR), a new framework for regulating data privacy protections in all member states. Among other things, the GDPR required prompt disclosure of personal data breaches, not later than 72 hours after learning of the breach. On its website, Google reaffirmed its commitment to complying with the GDPR across all its services and reaffirmed Google's aim "always to keep data private and safe."

C

While external scrutiny of data privacy and security grew in March and April 2018, internal Google investigators had discovered a software glitch in the Google+ social network that had existed since 2015 (referred to in the complaint as the "Three-Year Bug"). Because of a bug in an application programming interface for Google+, third-party developers could collect certain users' profile data even if those users had relied on Google's privacy settings to designate such data as nonpublic. The exposed private profile data included email addresses, birth dates, gender, profile photos, places lived, occupations, and relationship status.

Not only did Google's security protocols fail to detect the problem for three years, but Google also had a limited set of activity logs that could review only the two most recent weeks of user data access. Due to this record-keeping limitation, Google "had no way of determining how many third-parties had misused its users' personal private data." And Google "could only estimate that it exposed to third-parties the personal private data of hundreds of thousands of users" based on "less than 2% of the Three-Year Bug's lifespan." Despite the efforts of "over 100 of Google's best

and brightest," Google "could not confirm the damage from [the bug] or determine the number of other bugs." At the same time, this investigation into the Three-Year Bug detected other shortcomings in Google's security systems, including "previously unknown, or unappreciated, security vulnerabilities that made additional data exposures virtually inevitable." The complaint refers collectively to the Three-Year Bug and these additional vulnerabilities as the "Privacy Bug."

Around April 2018, Google's legal and policy staff prepared a memo detailing the Three-Year Bug and the additional vulnerabilities (referred to in the complaint as the "Privacy Bug Memo"). According to the complaint, the Privacy Bug Memo warned that the disclosure of these security issues "would likely trigger 'immediate regulatory interest' and result in defendants 'coming into the spotlight alongside or even instead of Facebook despite having stayed under the radar throughout the Cambridge Analytica scandal.'" The memo warned that "disclosure 'almost guarantees Sundar [Pichai] will testify before Congress.'"

According to the complaint, Pichai and other senior Google executives received and read the memo in early April 2018. The complaint alleges that key officers and directors, including Page and Pichai, chose a strategy of nondisclosure. Pichai approved a plan to conceal the existence of the Three-Year Bug and other security vulnerabilities described in the Privacy Bug Memo "to avoid any additional regulatory scrutiny, including having to testify before Congress." Further, despite Google+ having 395 million monthly active users, more than either Twitter or Snapchat, Pichai and Page approved a plan to shut down the Google+ consumer platform.

D

Despite the information in the Privacy Bug Memo, Alphabet and Google continued to give the public the same assurances about security and privacy as before. In particular, on April 23, 2018, Alphabet filed its quarterly report on Form 10-Q for the period ending March 31, 2018. The 10-Q incorporated the risk disclosures from Alphabet's 2017 10-K and made no disclosure about the Privacy Bug. It stated:

> Our operations and financial results are subject to various risks and uncertainties, including those described in Part I, Item 1A, "Risk Factors" in our Annual Report on Form 10-K for the year ended December 31, 2017, which could adversely affect our business, financial condition, results of operations, cash flows, and the trading price of our common and capital stock. *There have been no material changes to our risk factors since our Annual Report on Form 10-K for the year ended December 31, 2017*.

(emphasis added). Nor did Alphabet make any disclosure during an earnings call on the same day. Months later, in July 2018, Alphabet filed its Form 10-Q for the period ending June 30, 2018. This filing included a risk disclosure substantially identical to the one in the April 2018 filing; it likewise incorporated the 2017 Form 10-K risk factors and affirmed that no material changes occurred. Nor did

Alphabet make any disclosure of the problems during its July 2018 earnings call.[1]

The complaint identifies statements made by Alphabet, Google, and their employees between April and October 2018 that continued to reference user security and data privacy while making the same omission regarding any Google+ problems. According to the complaint, Alphabet thought that this "decision to buy time" would reduce the detrimental effects of eventual disclosure by avoiding disclosure at a time when Facebook was facing regulatory scrutiny, public criticism, and loss of consumer confidence as a result of the Cambridge Analytica scandal.

E

Six months after this decision to buy time, the *Wall Street Journal* exposed Google's discovery of Google+'s security vulnerabilities and its decision to conceal those vulnerabilities. In October 2018, the *Wall Street Journal* published a lengthy story on the events surrounding the Privacy Bug Memo. *See* Douglas MacMillan & Robert McMillan, *Google Exposed User Data, Feared Repercussions of Disclosing to Public*, Wall Street J. (Oct. 8, 2018). The story reported that "Google exposed the private data of hundreds of thousands of users of the Google+ social network and then opted not to disclose the issue this past spring, in part because of fears that doing so would draw regulatory scrutiny and cause reputational damage." It

[1] The complaint alleges that Page signed the 10-Qs and signed certifications, under SEC rules promulgated after the Sarbanes-Oxley Act, that vouched for the accuracy of the 10-Qs and the adequacy of controls for identifying cybersecurity risks.

walked the reader through the discovery of the privacy bug, explained how Google made "concerted efforts to avoid public scrutiny of how it handles user information, particularly at a time when regulators and consumer privacy groups are leading a charge to hold tech giants accountable for the vast power they wield over the personal data of billions of people," and reported that Pichai had been briefed on the plan not to notify users.

The day the news broke, Google published a blog post acknowledging the "significant challenges" regarding data security identified in the *Wall Street Journal* article. It finally admitted to exposing the private data of hundreds of thousands of users and announced it was shutting down the Google+ social network for consumers.

Condemnation from lawmakers soon followed. Two days after the *Wall Street Journal* article, Democratic senators wrote to demand an investigation by the Federal Trade Commission. This letter noted that, due to the limitations of Google's internal logs, "we may never know the full extent of the damage caused by the failure to provide adequate controls and protection to users." The letter likewise noted that the "awareness and approval by Google management to not disclose represents a culture of concealment and opacity set from the top of the company." Republican senators also wrote a letter to Pichai that questioned Google's decision "to withhold information about a relevant vulnerability for fear of public scrutiny" at the same time that Facebook was being questioned regarding the Cambridge Analytica scandal. In a second letter to Pichai, Senator Grassley complained that Google had assured him in April 2018 that it maintained robust protection for user data, despite Pichai's awareness that Google+ "had an almost identical feature to Facebook,

which allowed third party developers to access information from users."

Markets reacted to the news. Alphabet's publicly traded share price fell after the *Wall Street Journal* article. According to the complaint, Alphabet's share price fell $11.91 on October 8, $10.75 on October 9, and $53.01 on October 10. Financial news reports called Google's decision not to disclose the security breach a "cover-up" and predicted forthcoming regulatory scrutiny.

Just weeks later, in December 2018, Google disclosed the discovery of another Google+ bug that had exposed user data from 52.5 million accounts. Google also announced it was accelerating the shutdown of the consumer Google+ platform to occur four months earlier than planned.

F

Three days after the *Wall Street Journal* article, Rhode Island filed a securities fraud action, as did other plaintiffs.[2] After the cases were consolidated, Rhode Island was designated the lead plaintiff. It filed a consolidated amended complaint in April 2019, which now serves as the operative complaint. The complaint names Alphabet, Google, Page, Pichai, and two other Google senior executives as defendants (we refer to the defendants collectively as Alphabet, where

[2] Rhode Island refers to the State of Rhode Island, Office of the Rhode Island Treasurer on behalf of the Employees' Retirement System of Rhode Island.

appropriate, and otherwise by name).[3] The complaint alleges primary violations of Section 10(b) of the Securities Exchange Act of 1934, 15 U.S.C. § 78j(b), and SEC Rule 10b-5, 17 C.F.R. § 240.10b-5, for securities fraud, as well as violations of Section 20(a) of the Exchange Act, 15 U.S.C. § 78t(a), which imposes joint and several liability on persons in control of "any person liable under any provision" of securities law.

Alphabet moved to dismiss the complaint for failure to state a claim. The district court granted the motion after determining that the complaint failed to allege any material misrepresentation or omission and failed to allege scienter sufficiently. Further, the court held that because the Section 10(b) claim failed, the Section 20(a) claim for controlling-person liability "necessarily fails."

Although the district court granted leave to amend, Rhode Island notified the district court that it did not intend to amend, and the district court entered judgment. Rhode Island now appeals from that final judgment.

II

We have jurisdiction under 28 U.S.C. § 1291. We review the district court's dismissal of Rhode Island's complaint for failure to state a claim de novo. *In re NVIDIA Corp. Sec.*

[3] The other two individual defendants are Keith P. Enright, who served as Google's Legal Director of Privacy from 2016 until September 2018 when he became Google's Chief Privacy Officer, and John Kent Walker, Jr., who served as Google's Vice President and General Counsel from 2016 through August 2018 before becoming Senior Vice President for Global Affairs.

*Litig.*, 768 F.3d 1046, 1051 (9th Cir. 2014). "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Iqbal*, 556 U.S. at 678 (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "When there are well-pleaded factual allegations, a court should assume their veracity and then determine whether they plausibly give rise to an entitlement to relief." *Id.* at 679. As the Supreme Court has explained, "[d]etermining whether a complaint states a plausible claim for relief" is "a context-specific task that requires the reviewing court to draw on its judicial experience and common sense." *Id.* In the process, we may "disregard '[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements.'" *Telesaurus VPC, LLC v. Power*, 623 F.3d 998, 1003 (9th Cir. 2010) (quoting *Iqbal*, 556 U.S. at 678).

A complaint is plausible on its face "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678. The misconduct alleged here includes claims under two statutory sections: primary liability under Section 10(b) of the Exchange Act and controlling-person liability under Section 20(a) of the Exchange Act.

Section 10(b) of the Exchange Act prohibits using or employing, "in connection with the purchase or sale of any security . . . [,] any manipulative or deceptive device or contrivance in contravention of such rules and regulations as the [SEC] may prescribe as necessary or appropriate in the public interest or for the protection of investors." 15 U.S.C. § 78j(b). To implement Section 10(b), the SEC prescribed Rule 10b-5, which makes it unlawful

> (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.

17 C.F.R. § 240.10b-5.

The Supreme Court has interpreted Section 10(b) and Rule 10b-5 as providing an implied private cause of action. *Stoneridge Inv. Partners, LLC v. Scientific-Atlanta*, 552 U.S. 148, 157 (2008). "In a typical § 10(b) private action" based on material misrepresentations or omissions, a plaintiff must prove "(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." *Id.*

Under Section 10(b) and Rule 10b-5(b), "the maker of a statement is the person or entity with ultimate authority over the statement, including its content and whether and how to communicate it." *Janus Cap. Grp., Inc. v. First Derivative Traders*, 564 U.S. 135, 142 (2011). Persons "who do not 'make' statements (as *Janus* defined 'make'), but who

disseminate false or misleading statements to potential investors with the intent to defraud, can be found to have violated the *other* parts of Rule 10b-5, subsections (a) and (c), as well as related provisions of the securities laws" including Section 10(b). *Lorenzo v. SEC*, 139 S. Ct. 1094, 1099, 1100–03 (2019).

The first two elements of a typical Section 10(b) and Rule 10b-5(b) claim are at issue here. The first element is that a defendant omitted "to state a material fact necessary in order to make the statements made . . . not misleading," 17 C.F.R. § 240.10b-5(b). To meet this requirement, the plaintiff must prove both that the omission is misleading and that it is material. *Id.*

We apply the objective standard of a "reasonable investor" to determine whether a statement is misleading. *See In re VeriFone Sec. Litig.*, 11 F.3d 865, 869 (9th Cir. 1993). Section 10(b) and Rule 10b-5(b) "do not create an affirmative duty to disclose any and all material information" and instead require disclosure "only when necessary 'to make . . . statements made, in light of the circumstances under which they were made, not misleading.'" *Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. 27, 44 (2011) (quoting 17 C.F.R. § 240.10b-5(b)).

A misleading omission is material if "there is 'a substantial likelihood that [it] would have been viewed by the reasonable investor as having significantly altered the "total mix" of information made available' for the purpose of decisionmaking by stockholders concerning their investments." *Retail Wholesale & Dep't Store Union Loc. 338 Ret. Fund v. Hewlett-Packard Co.*, 845 F.3d 1268, 1274 (9th Cir. 2017) (quoting *Basic Inc. v. Levinson*, 485 U.S. 224,

231–32 (1988)). The inquiry into materiality is "fact-specific," *Matrixx Initiatives*, 563 U.S. at 43 (quoting *Basic*, 485 U.S. at 236), and "requires delicate assessments of the inferences a 'reasonable shareholder' would draw from a given set of facts and the significance of those inferences to him," *Fecht v. Price Co.*, 70 F.3d 1078, 1080 (9th Cir. 1995) (quoting *TSC Indus., Inc. v. Northway, Inc.*, 426 U.S. 438, 450 (1976)). "[T]hese assessments are peculiarly ones for the trier of fact." *Id.* (quoting *TSC Indus.*, 426 U.S. at 450). As a result, resolving materiality as a matter of law is generally appropriate "only if the adequacy of the disclosure or the materiality of the statement is so obvious that reasonable minds could not differ." *Id.* at 1081 (cleaned up); *see Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 1014 (9th Cir. 2018) (same).

In evaluating whether an omission relating to cybersecurity is materially misleading, we may consider the SEC's interpretive guidance regarding the adequacy of cybersecurity-related disclosures. *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Securities Act Release No. 33-10459, Exchange Act Release No. 34-82746, 83 Fed. Reg. 8166-01, 8167 (Feb. 26, 2018) ("*Cybersecurity Disclosures*"). Regardless of the degree of deference such interpretive guidance may merit, *see Kisor v. Wilkie*, 139 S. Ct. 2400, 2414–18 (2019), an SEC interpretive release can "shed further light" on regulatory disclosure requirements, *NVIDIA*, 768 F.3d at 1055. Agency interpretations, like the SEC interpretive release here, can provide "the judgments about the way the real world works" that "are precisely the kind that agencies are better equipped to make than are courts." *See Pension Benefit Guar. Corp. v. LTV Corp.*, 496 U.S. 633, 651 (1990); *see also Kisor*, 139 S. Ct. at 2413 ("[W]hen new issues demanding new policy calls

come up within that [statutory] scheme, Congress presumably wants the same agency, rather than any court, to take the laboring oar.").

We have held that "transparently aspirational" statements, *Hewlett-Packard*, 845 F.3d at 1278, as well as statements of "mere corporate puffery, vague statements of optimism like 'good,' 'well-regarded,' or other feel good monikers," are generally not actionable as a matter of law, because "professional investors, and most amateur investors as well, know how to devalue the optimism of corporate executives," *Police Ret. Sys. of St. Louis v. Intuitive Surgical, Inc.*, 759 F.3d 1051, 1060 (9th Cir. 2014) (quoting *In re Cutera Sec. Litig.*, 610 F.3d 1103, 1111 (9th Cir. 2010)). Such statements rise to the level of materially misleading statements only if they provide "concrete description of the past and present" that affirmatively create a plausibly misleading impression of a "state of affairs that differed in a material way from the one that actually existed." *See In re Quality Sys., Inc. Sec. Litig.* (*Quality Systems*), 865 F.3d 1130, 1144 (9th Cir. 2017) (cleaned up).

The second element of a typical Section 10(b) claim, scienter, is not set forth in the statute. Rather, the Supreme Court has determined that "[t]he words 'manipulative or deceptive' used in conjunction with 'device or contrivance' strongly suggest that § 10(b) was intended to proscribe knowing or intentional misconduct." *Ernst & Ernst v. Hochfelder*, 425 U.S. 185, 197 (1976). We have since held that "a reckless omission of material facts" satisfies the element of scienter, *Hollinger v. Titan Cap. Corp.*, 914 F.2d 1564, 1568–70 (9th Cir. 1990) (en banc) (quoting *Sundstrand Corp. v. Sun Chem. Corp.*, 553 F.2d 1033, 1044 (7th Cir. 1977)), provided that such recklessness "reflects some degree

of intentional or conscious misconduct," *In re Silicon Graphics Inc. Sec. Litig.*, 183 F.3d 970, 977 (9th Cir. 1999), *abrogated in part on other grounds*, *S. Ferry LP, No. 2 v. Killinger* (*South Ferry*), 542 F.3d 776, 783–84 (9th Cir. 2008). We refer to this standard as "deliberate recklessness" and define it as "'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.'" *Nguyen v. Endologix, Inc.*, 962 F.3d 405, 414 (9th Cir. 2020) (quoting *Schueneman v. Arena Pharm., Inc.*, 840 F.3d 698, 705 (9th Cir. 2016)).

In addition to these substantive elements, a plaintiff bringing a securities fraud action must also meet the heightened pleading standards imposed by the Private Securities Litigation Reform Act (PSLRA) for pleading, among other things, "[m]isleading statements and omissions" and "[r]equired state of mind." 15 U.S.C. § 78u-4(b)(1)–(2). Under these standards, if the plaintiff alleges that the defendant "omitted to state a material fact necessary in order to make the statements made, in the light of the circumstances in which they were made, not misleading," then

> the complaint shall 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.

15 U.S.C. § 78u-4(b)(1). Likewise, when a plaintiff must prove "that the defendant acted with a particular state of

mind," then "the complaint shall, with respect to each act or omission alleged to violate this chapter, state with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind." 15 U.S.C. § 78u-4(b)(2)(A); *see also* Fed. R. Civ. P. 9(b). For pleading scienter, we assess "all the allegations holistically" to determine whether the inference of scienter is "cogent and compelling." *Tellabs*, 551 U.S. at 324, 326. "[M]erely 'reasonable' or 'permissible'" inferences are insufficient. *Id.* at 324. As a result, courts must "take into account plausible opposing inferences" and determine that "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 323, 324.

Finally, in addition to alleging violations under Section 10(b), Rhode Island also alleges violations of Section 20(a) of the Exchange Act, 15 U.S.C. § 78t(a). Section 20(a) imposes liability on a person who is in control of the person who is directly responsible for a securities fraud violation:

> Every person who, directly or indirectly, controls any person liable under any provision of this chapter or of any rule or regulation thereunder shall also be liable jointly and severally with and to the same extent as such controlled person to any person to whom such controlled person is liable . . . , unless the controlling person acted in good faith and did not directly or indirectly induce the act or acts constituting the violation or cause of action.

15 U.S.C. § 78t(a). SEC regulations define "control" to mean "the possession, direct or indirect, of the power to direct or

cause the direction of the management and policies of a person, whether through the ownership of voting securities, by contract, or otherwise." 17 C.F.R. § 230.405. To establish a cause of action under Section 20(a), "a plaintiff must first prove a primary violation of underlying federal securities laws, such as Section 10(b) or Rule 10b-5, and then show that the defendant exercised actual power over the primary violator." *NVIDIA*, 768 F.3d at 1052. We have held that the inquiry into actual power or control "is normally an 'intensely factual question.'" *Zucco Partners, LLC v. Digimarc Corp.*, 552 F.3d 981, 990 (9th Cir. 2009) (quoting *Paracor Fin., Inc. v. Gen. Elec. Cap. Corp.*, 96 F.3d 1151, 1161 (9th Cir. 1996)). Nevertheless, "if a plaintiff fails to adequately plead a primary violation," then Section 20(a) claims "may be dismissed summarily." *Id.*

III

The district court granted Alphabet's motion to dismiss on the grounds that Rhode Island failed to adequately allege a materially misleading misrepresentation or omission and that Rhode Island failed to adequately allege scienter. We therefore focus on these two bases for the district court's decision.

A

The complaint identifies a dozen allegedly misleading statements, but we begin by considering two statements made by Alphabet in its quarterly reports filed with the SEC on Form 10-Q in April 2018 and July 2018. We conclude that the complaint adequately alleges that these two statements omitted material facts necessary to make the statements not misleading.

The April 2018 report for the period ending March 31, 2018, stated that Alphabet's "operations and financial results are subject to various risks and uncertainties," including those identified in Alphabet's Annual Report on Form 10-K for the year ended December 31, 2017, and asserted that "[t]here have been no material changes to our risk factors since our Annual Report on Form 10-K for the year ended December 31, 2017."[4] The 2017 10-K had warned, among other things, that even unfounded concerns about Alphabet's "practices with regard to the collection, use, disclosure, or security of personal information or other privacy related matters" could damage the company's "reputation and adversely affect [its] operating results." Alphabet's April and July 2018 10-Qs make no mention of the Three-Year Bug or other security vulnerabilities identified in the Privacy Bug Memo.

Given that the April 10-Q filing was made after the detection of Google's cybersecurity issues, after internal deliberation based on the Privacy Bug Memo, and during the growing scrutiny following the Cambridge Analytica scandal, the complaint plausibly alleges that the omission of any mention of the Three-Year Bug or the other security vulnerabilities made the statements in each Form 10-Q materially misleading to a reasonable investor and significantly altered the total mix of information available to investors.

The complaint plausibly alleges that Alphabet's omission was material. Among other allegations in the complaint, Alphabet's risk disclosures in the 2017 10-K warned of the harms that could follow from the detection and disclosure of

[4] Alphabet's July 2018 Form 10-Q, for the quarter ending June 30, 2018, is substantively identical.

security vulnerabilities, including public concerns about privacy and regulatory scrutiny. Public statements by Google and Alphabet executives similarly demonstrated the importance of user trust and public perceptions of security and privacy practices for the products and services central to Alphabet's business. The scale of the data-privacy and security-vulnerability problems identified in the Privacy Bug Memo further supports the allegations that these problems were material. Indeed, the Privacy Bug Memo itself warned of the significant consequences of the problems discovered and of their disclosure. The market reaction, increased regulatory and governmental scrutiny, both in the United States and abroad, and media coverage alleged by the complaint to have occurred after disclosure all support the materiality of the misleading omission.

Finally, the SEC's guidance on when companies should disclose "cybersecurity incidents" also supports the conclusion that Alphabet's omission was material. *See Cybersecurity Disclosures*, 83 Fed. Reg. at 8169.[5] In determining disclosure obligations and "[t]he materiality of cybersecurity risks and incidents," the SEC advises that companies should weigh, among other things, "harm to a company's reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-U.S. authorities." *Id.* at 8168–69. Here,

[5] The SEC defines a "cybersecurity incident" as an "occurrence that actually or potentially results in adverse consequences to an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences." *Cybersecurity Disclosures*, 83 Fed. Reg. at 8166 n.3 (cleaned up).

the complaint plausibly alleges that these risks of harm ripened into actual harm when the Privacy Bug was detected and created the new risk that this discovery would become public.

The complaint also plausibly alleges that Alphabet's omission was misleading. Risk 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. *See Berson v. Applied Signal Tech., Inc.*, 527 F.3d 982, 985–87 (9th Cir. 2008). In *Berson*, we held that the company's statement of anticipated revenues from its large backlog of work was misleading because it failed to disclose that a significant portion of the "backlogged" work was "substantially delayed and at serious risk of being cancelled altogether." *Id.* at 986. Similarly, we explained that a 10-Q statement that warned of "the risks of product liability claims in the abstract" was misleading because it failed to disclose that the risk had already come to fruition. *Siracusano v. Matrixx Initiatives, Inc.*, 585 F.3d 1167, 1181 (9th Cir. 2009) (citing *Berson*, 527 F.3d at 986), *aff'd*, 563 U.S. 27 (2011). Even more recently, we held that a company's warning in its Form 10-Q that share prices "might" be affected by announcements of study results that "may" be inconsistent with interim study results was misleading because the company "allegedly knew already that the 'new data' revealed exactly that." *Khoja*, 899 F.3d at 1015–16; *cf. Wochos v. Tesla, Inc.*, 985 F.3d 1180, 1195–96 (9th Cir. 2021) (rejecting the argument that a risk disclosure's forward-looking statements "constituted misleading omissions about current or past challenges" because the disclosure also acknowledged that the company had already experienced "the sort of 'challenges' that it would have to

overcome in order to achieve its stated objective").[6] As in these cases, the complaint plausibly alleges that Alphabet's warning in each Form 10-Q of risks that "could" or "may" occur is misleading to a reasonable investor when Alphabet knew that those risks had materialized.

Alphabet makes several arguments against this conclusion. First, Alphabet argues that any omission from the Form 10-Qs was not misleading because Google had already remediated the software glitch in Google+ before it made the 10-Q statements. Because the risks caused by the software glitch had been remediated, Alphabet argues, Rhode Island cannot rely on the cases holding that a company's warning of future risks is misleading if those risks have already materialized. This argument fails for several reasons. Given that Google's business model is based on trust, the material implications of a bug that improperly exposed user data for three years were not eliminated merely by plugging the hole in Google+'s security. The existence of the software glitch for a three-year period, which exposed the private information of hundreds of thousands of Google+ users, and the fact that Google was unable to determine the scope and impact of the glitch, indicated that there were significant problems with Google's security controls. Google had long recognized that in an industry based on security and privacy, the public disclosure of serious failings in this area would have wide-ranging effects, including erosion of consumer confidence and increased regulatory scrutiny. Further, the

[6] In light of our precedent, we decline to follow the Sixth Circuit's unpublished decision in *Bondali v. Yum! Brands, Inc.*, which held that a statement disclosing future harms generally would not mislead a reasonable investor about the current state of a corporation's operations. 620 F. App'x 483, 490–91 (6th Cir. 2015).

Privacy Bug Memo was not limited to discussing the discovery of the software glitch that had been remediated because it highlighted additional security vulnerabilities that were so significant that they allegedly led to Google's decision to shut down the Google+ consumer platform.

Second, Alphabet contends that the 10-Q omissions were not material because the software bug did not lead to the release of sensitive information like financial or medical information or cause harm to any user and because Alphabet's revenue increased from $12 billion to $30 billion between 2017 and 2018. These arguments fail because a cybersecurity incident may be material even if it does not compromise sensitive financial or medical information or have an immediate financial impact on the company. The standard is whether there is a "substantial likelihood" that the information at issue "would have been viewed by the reasonable investor as having significantly altered the total mix of information made available for the purpose of decisionmaking by stockholders concerning their investments." *Hewlett-Packard*, 845 F.3d at 1274 (cleaned up). Because cybersecurity incidents may cause a range of substantial costs and harms,[7] reasonable investors would likely find omissions regarding significant cybersecurity incidents material to their decisionmaking. The likelihood is particularly substantial here, given the nature of Alphabet's business. As the SEC has explained, the materiality of

[7] *See Cybersecurity Disclosures*, 83 Fed. Reg. at 8167–69 & n.32 (noting that a cybersecurity incident can cause a company to incur remediation costs, increased cybersecurity protection costs, lost revenues, harm to customer retention or attraction, litigation and legal risks, increased insurance premiums, reputational damage, and damage to stock price and shareholder value).

compromised information may "depend on the nature of the company's business" and "the scope of the compromised information." *Id.* at 8169 n.33. Here, for instance, the complaint alleges that the *Wall Street Journal* article resulted in a swift stock price decline, legislative scrutiny, and public reaction, all of which support the allegation that the Privacy Bug was material even absent a release of sensitive information or revenue decline.

Applying our objective materiality standard to the 10-Qs here, Rhode Island's complaint plausibly alleges the materiality of the costs and consequences associated with the Privacy Bug, and its public disclosure, and how Alphabet's decision to omit information about the Privacy Bug in its 10-Qs significantly altered the total mix of information available for decisionmaking by a reasonable investor.

B

We now consider whether the complaint adequately alleges scienter for the materially misleading omissions from the 10-Q statements. Because Rule 10b-5 makes it unlawful "[t]o *make* any untrue statement" or to omit material facts necessary to make "the statements *made*" not misleading, 17 C.F.R. § 240.10b-5(b) (emphasis added), we must first determine who was the maker of the statement for purposes of Section 10(b) and Rule 10b-5(b) and whether the complaint adequately alleged that the maker omitted material information knowingly, intentionally, or with deliberate recklessness. In other words, the complaint must plausibly allege, with the particularity required by the PSLRA, that the maker of the statements knew about the security vulnerabilities and intentionally or recklessly did not disclose them.

Alphabet is at least one alleged maker of the 10-Q statements here, because Alphabet has "ultimate authority over the statement, including its content and whether and how to communicate it," *Janus*, 564 U.S. at 142.[8]

Because Alphabet is a corporation, it "'can only act through its employees and agents' and can likewise only have scienter through them." *In re ChinaCast Educ. Corp. Sec. Litig.*, 809 F.3d 471, 475 (9th Cir. 2015) (quoting *Suez Equity Invs., L.P. v. Toronto-Dominion Bank*, 250 F.3d 87, 101 (2d Cir. 2001)). We have explained that the "scienter of the senior controlling officers of a corporation may be attributed to the corporation itself to establish liability as a primary violator of § 10(b) and Rule 10b-5 when those senior officials were acting within the scope of their apparent authority." *Id.* at 476 (quoting *Adams v. Kinder-Morgan, Inc.*, 340 F.3d 1083, 1106–07 (10th Cir. 2003)).

The complaint's specific allegations, taken as a whole, raise a strong inference that Page, and therefore Alphabet, knew about the Three-Year Bug, the Privacy Bug, and the Privacy Bug Memo, and that Alphabet intentionally did not disclose this information in its 10-Q statements.

The complaint's allegations, read as a whole, raise a strong inference that Alphabet was aware of the information in the Privacy Bug Memo. In this case, the complaint alleges that Pichai and other Google senior executives read the Privacy Bug Memo, and so necessarily knew of the Three-Year Bug and other security vulnerabilities, before Alphabet

[8] The complaint does not allege, and Rhode Island does not argue, that Page is a maker of the 10-Q statements for purposes of Section 10(b) and Rule 10b-5. We therefore do not address this issue.

made its April 2018 10-Q statement. The complaint alleges with particularity that the memo informed senior executive leadership at Google of the scope of the problem, warned of the consequences of disclosure, and presented Google leadership with a clear decision on whether to disclose those problems. *See South Ferry*, 542 F.3d at 785–86 (describing "actual access to the disputed information" as supporting a strong inference of scienter).

The complaint also raises a strong inference that Pichai communicated this information to Page, and therefore Page was also aware of the Three-Year Bug and other security vulnerabilities before he signed the April 2018 10-Q statement. Although the complaint does not directly allege that Page read the Privacy Bug Memo, we may consider a senior executive's role in a company to determine whether there is a cogent and compelling inference that the senior executive knew of the information at issue. *Id.* at 785. This includes consideration of the executive's access to the information, and, whether, given the importance of the information, "it would be 'absurd' to suggest that management was without knowledge of the matter." *Id.* at 786 (quoting *Berson*, 527 F.3d at 988).

Here, numerous allegations in the complaint raise the strong inference that Page was vitally concerned with Google's operations. *See id.* at 785–86. Specifically, the complaint alleges that Alphabet is essentially a holding company for Google (i.e., Google was the "lifeblood" of Alphabet). Page, the former CEO of Google, received weekly reports of Google's operating results and made "key operating decisions" at Google. Pichai, as the replacement CEO of Google, reported directly to Page. Moreover, the complaint alleges that Pichai and Page together approved a

plan in spring 2018 to shut down Google+ because of the security concerns revealed by the Privacy Bug Memo. Taken together, these specific allegations raise the strong inference that Pichai informed Page of any information regarding Google's operations that was material and that there was shared decision-making on key issues. *See id.* (identifying a combination of allegations regarding corporate structure, importance of information, and exposure to factual information that "may be relevant and help to satisfy the PSLRA scienter requirement"). The complaint also cogently alleges that the Three-Year Bug and other security vulnerabilities that were disclosed in the Privacy Bug Memo were highly material to Google's operations, for the reasons explained above.

Therefore, considering these allegations together, there is a strong inference that Page knew of these problems and the consequences of disclosure when Alphabet made its 10-Q statements in April and July 2018. The competing inference—that Pichai concealed "the largest data-security vulnerability in the history of two Companies whose existence depends on data security" from the CEO of Alphabet at a time when social media networks were under immense regulatory and governmental scrutiny—is not plausible. Accordingly, we conclude there is a strong inference that Page had the requisite knowledge, which can be imputed to Alphabet. *ChinaCast*, 809 F.3d at 475.

For the same reasons, there is an equally strong inference that, armed with this knowledge, Alphabet intentionally did not disclose the cybersecurity information to the public in order to avoid or delay the impacts disclosure could have on regulatory scrutiny, public criticism, and loss of consumer confidence. The complaint also alleges that Pichai approved

a cover-up to avoid regulatory scrutiny and testimony before Congress. The complaint alleges that "key officers and directors," including Page and Pichai, "had decided to conceal all of this information from everyone outside the Companies." This decision to conceal was calculated to "buy time" by avoiding putting Google in the spotlight alongside the Facebook-Cambridge Analytica scandal and at the time of heightened public and regulatory scrutiny. As it turned out, Alphabet successfully bought itself about six months of time between the April 2018 decision not to disclose and the October 2018 publication of the *Wall Street Journal* article. Again, the competing inference that Alphabet knew of this information but was merely negligent in not disclosing it is not plausible.

Finally, Alphabet argues that the complaint does not raise a strong inference that Alphabet intentionally omitted material information from its 10-Q statement because the complaint does not allege that company officials made suspicious stock sales or include allegations from confidential witnesses. This argument fails. Although such allegations may support an inference of scienter, they are not a sine qua non for raising such an inference. *See, e.g.*, *Siracusano*, 585 F.3d at 1180–83 (rejecting need for stock sales and identifying sufficient scienter allegations without witnesses); *No. 84 Employer-Teamster Joint Council Pension Tr. Fund v. Am. W. Holding Corp.*, 320 F.3d 920, 944 (9th Cir. 2003) ("[T]he lack of stock sales by a defendant is not dispositive as to scienter."). Allegations of suspicious stock sales or information from confidential witnesses are not needed where, as here, other allegations in the complaint raise a strong inference of scienter. Alphabet also argues that because Google fixed the Three-Year Bug and no users were harmed, Alphabet's failure to disclose does not support a

strong inference of scienter. This argument is little more than a restatement of Alphabet's contention, which we have already rejected, that the Three-Year Bug and the Privacy Bug were not material because they had been remediated. *See supra* Part III.A.

Rhode Island adequately alleged falsity, materiality, and scienter for the April 2018 and July 2018 10-Q statements. We therefore reverse the district court's holdings to the contrary. The defendants' motion to dismiss did not challenge the remaining elements of the Section 10(b) and Rule 10b-5(b) statement liability claims for these or other statements, so we do not address the elements of connection to the sale of a security, reliance, economic loss, or loss causation.

Because we reverse the district court's dismissal of Rhode Island's claims related to Alphabet's 10-Q statements, we also reverse its dismissal of the complaint's Section 20(a) claims based on those statements, which allege that Pichai and Page were controlling persons of Alphabet under Section 20(a). The district court dismissed these claims solely on the ground that Rhode Island failed to state a claim for a primary violation of Section 10(b) and Rule 10b-5. We remand to the district court to reconsider Pichai and Page's liability under Section 20(a) in light of our holding today.

C

We now consider the ten remaining statements identified in the complaint.

First, the complaint identifies statements made in two earnings calls in April and July 2018 by Ellen West,

Alphabet's Head of Investor Relations. According to the complaint, after noting that "[s]ome of the statements that we make today may be considered forward looking" and that "[t]hese statements involve a number of risks and uncertainties that could cause actual results to differ materially," West stated: "For more information, please refer to the risk factors discussed in our Form 10-K for 2017 filed with the SEC."[9] These statements alone did not plausibly give a reasonable investor the "impression of a state of affairs that differs in a material way from the one that actually exists," *Hewlett-Packard*, 845 F.3d at 1275 (quoting *Berson*, 527 F.3d at 985), because, unlike the 2018 10-Q statements, West's statement did not include the express assurance that there had been "no material changes" to Alphabet's risk factors since the 2017 10-K filing.

Second, the complaint identifies statements made by Pichai, three senior Google executives, and an Alphabet proxy statement. These statements emphasize Google's and Alphabet's commitment to user privacy, data security, and regulatory compliance and discuss Google and Alphabet's ongoing efforts to secure user data and work on GDPR compliance. For instance, the complaint alleges that, on the April 2018 earnings call for Alphabet, Pichai assured the public and investors that Google "started working on GDPR compliance over 18 months ago and ha[d] been very, very engaged on it" and that Google has a "very robust and strong privacy program." Similarly, in an April 2018 letter to Senator Grassley, a senior Google executive stated that "Google has a longstanding commitment to ensuring both that our users share their data only with developers they can trust,

[9] The complaint alleges that West's statements on the April 2018 and July 2018 earnings calls were substantively identical.

and that they understand how developers will use that data" and that Google was "committed to protecting our users' data and prohibit[s] developers from requesting access to information they do not need." Google executives elsewhere touted Alphabet as "one of the leading companies when it comes to privacy and security of user data," explained that Alphabet was taking "great pains to make sure that people have great control and notice over their data," and affirmed that the "foundation of [Google's] business is the trust of people that use our services."

While these statements are relevant and were made while Google and Alphabet allegedly chose a strategy of concealment over disclosure, these statements do not rise to the level of "concrete description of the past and present" that affirmatively create a misleading impression of a "state of affairs that differed in a material way from the one that actually existed." *Quality Systems*, 865 F.3d at 1144 (cleaned up). They instead amount to vague and generalized corporate commitments, aspirations, or puffery that cannot support statement liability under Section 10(b) and Rule 10b-5(b). *See Hewlett-Packard*, 845 F.3d at 1278; *Intuitive Surgical*, 759 F.3d at 1060.

Finally, the complaint alleges that Page and Pichai decided not to testify before the United States Senate Intelligence Committee in September 2018 alongside Facebook and Twitter, which left "an empty chair for Google." An empty chair is neither a statement of material fact nor the misleading omission of a material fact. *See* 17 C.F.R. § 240.10b-5(b); *see also Hewlett-Packard*, 845 F.3d at 1278.

Because the complaint does not plausibly allege that these remaining statements are misleading material misrepresentations or omissions, we affirm the district court's dismissal of the Section 10(b) and Rule 10b-5(b) statement liability claims based on these statements. We also affirm the district court's dismissal of the Section 20(a) controlling-person claims for these statements.

## IV

Finally, Rhode Island argues on appeal that the district court erred in dismissing its claims under Rule 10b-5(a) and (c) (referred to in the complaint as a "scheme liability claim") when it dismissed the complaint in its entirety without addressing those claims. In its complaint, Rhode Island alleged that the defendants "disseminated or approved the statements" alleged to be materially misleading and "engaged and participated in a continuous course of conduct to conceal the truth and/or adverse material information about Alphabet's business and operations."

Alphabet argues that Rhode Island waived these claims because it failed to raise them to the district court in opposition to Alphabet's motion to dismiss. Alphabet also contends that the complaint's claims under Rule 10b-5(a) and (c) are duplicative of the claims under Rule 10b-5(b) seeking to hold the defendants liable for misleading statements. Both arguments fail.

First, because Alphabet's motion to dismiss did not target Rhode Island's Rule 10b-5(a) and (c) claims, Rhode Island did not waive those claims by failing to address them in opposition to the motion to dismiss. A party's failure to oppose an argument that was not made does not constitute a

waiver. Second, Alphabet's argument that Rule 10b-5(a) and (c) claims cannot overlap with Rule 10b-5(b) statement liability claims is foreclosed by *Lorenzo*, which rejected the petitioner's argument that Rule 10b-5(a) and (c) "concern 'scheme liability claims' and are violated only when conduct other than misstatements is involved." 139 S. Ct. at 1101–02.[10] Rather, *Lorenzo* explained that "considerable overlap" exists among the subsections of Rule 10b-5 and held that disseminating false statements "ran afoul of subsections (a) and (c)." *Id.* at 1102.

Because the district court erred in sua sponte dismissing Rhode Island's claims under Rule 10b-5(a) and (c) when Alphabet had not targeted those claims in its motion to dismiss, we reverse dismissal of the claims under Section 10(b) and Rule 10b-5(a) and (c) against all defendants and remand to the district court. *See Golden Gate Hotel Ass'n v. City & County of San Francisco*, 18 F.3d 1482, 1487 (9th Cir. 1994); *see also Reed v. Lieurance*, 863 F.3d 1196, 1207–08 (9th Cir. 2017) (reversing sua sponte dismissal). We also reverse the dismissal of Rhode Island's claims under Section 20(a) to the extent those claims depend on claims alleging violations of Rule 10b-5(a) and (c).

**REVERSED IN PART, AFFIRMED IN PART, JUDGMENT VACATED, REMANDED FOR FURTHER PROCEEDINGS.**[11]

---

[10] In reaching this holding, *Lorenzo* abrogated our contrary holding in *WPP Luxembourg Gamma Three Sarl v. Spot Runner, Inc.*, 655 F.3d 1039, 1057–58 (9th Cir. 2011). *See Lorenzo*, 139 S. Ct. at 1100.

[11] Each party will bear its own costs on appeal.