ROBBINS GELLER RUDMAN
& DOWD LLP
JASON A. FORGE (181542)
MICHAEL ALBERT (301120)
J. MARCO JANOSKI GRAY (306547)
TING H. LIU (307747)
655 West Broadway, Suite 1900
San Diego, CA 92101
Telephone: 619/231-1058
619/231-7423 (fax)
jforge@rgrdlaw.com
malbert@rgrdlaw.com
mjanoski@rgrdlaw.com
tliu@rgrdlaw.com

Lead Counsel for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

In re ALPHABET, INC. SECURITIES LITIGATION This Document Relates To: ALL ACTIONS.	Master File No. 4:18-cv-06245-JSW CLASS ACTION PLAINTIFF'S OPPOSITION TO DEFENDANTS' MOTION TO DISMISS DATE: August 23, 2019 TIME: 9:00 a.m. COURTROOM: 5 JUDGE: Hon. Jeffrey S. White

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

CASES

Page

Page

Page

STATUTES, RULES AND REGULATIONS

Page

SECONDARY AUTHORITY

Lead Plaintiff State of Rhode Island, Office of the Rhode Island Treasurer on behalf of the Employees' Retirement System of Rhode Island ("Plaintiff"), respectfully submits this opposition to Defendants' Motion to Dismiss Consolidated Amended Complaint for Violation of the Federal Securities Laws (ECF No. 71) ("MTD").[1]

I. Summary of Argument

By March 2018, data security at Google, whose entire existence depends on consumers trusting it with their private information, was a sinking ship. Defendants stumbled upon a "bug" they had overlooked for years, which potentially exposed hundreds of millions of users' private information; they had no way to determine the extent of harm from it; they learned more bugs were likely coming, but were so helpless to stop them, they had to prepare to shut down the world's fifth-largest social-media network; and all of this was happening at a time when Congressional hearings into consumer data leaks were underway and the markets were pummeling Facebook for its data-security failings. So Defendants decided to deceive investors by portraying Google's data-security situation as completely unchanged and themselves as completely trustworthy.

Defendants' uncandid approach continues with their MTD, which refuses to accept the facts as alleged in the Complaint and baselessly alleges new facts to contest them. Disregarding allegations of a threat to Defendants' "lifeblood" that would be "devastating" and could render Google "worthless," Defendants proclaim that Plaintiff fails to allege materiality. A data exposure they had failed to detect for years and whose harm they could not determine is declared to have been "quickly remediated." Just like the Titanic's course was "quickly remediated" – after Captain Smith had failed to avoid a collision whose harm he could not determine.

Defendants' MTD lacks substance because it is just a procedural gambit to exploit the Private Securities Litigation Reform Act of 1995's ("PSLRA") automatic discovery stay, as demonstrated by

[1] "Defendants" are Alphabet, Inc. ("Alphabet"), Google LLC, Keith P. Enright ("Enright"), Lawrence E. Page ("Page"), Sundar Pichai ("Pichai") and John Kent Walker, Jr. ("Walker"). Alphabet and Google LLC are collectively referred to as "Google" or the "Company." Enright, Page, Pichai and Walker are collectively referred to as the "Individual Defendants." All "¶_" or "¶¶_" references are to the Consolidated Amended Complaint for Violation of the Federal Securities Laws (ECF No. 62) (the "Complaint"). All emphasis is added and citations are omitted unless otherwise stated.

their resort to defying facts alleged in the Complaint and alleging new ones outside it, violating the rules of engagement at the pleading stage. But now that the discovery-stay box has been checked, it is time to turn to the merits because the inadequacy of Defendants' MTD confirms that this case should proceed.

II. Factual Background[2]

A. Defendants Stumble upon the Tip of a Data-Security Iceberg

The Google+ social media platform launched in 2011 to compete with Facebook and Twitter, and to create a "common identity" or "social layer" of user information across all Google products (*e.g.*, Search, Gmail, Maps, YouTube). ¶¶31-32. The mass collection and aggregation of personal user data is ultimately what fuels Google, which mines the treasure trove of personal information it collects to sell targeted ads. ¶¶18, 65. As such, Google depends on extensive consumer buy-in, and consequently, on the trust that Google users place in the privacy and security of the personal data they allow the Company to collect. ¶¶18-20, 23-26. For years, the Company acknowledged the existential risks that data-privacy concerns posed in the "Risk Factors" section of its U.S. Securities and Exchange Commission ("SEC") filings. ¶27. For instance, the Company's 2017 Annual Report on Form 10-K ("2017 10-K"), filed in February 2018, warned of the following risks, among others:

- "***Privacy concerns relating to our technology could damage our reputation and deter current and potential users or customers from our products and services***." ¶28 (emphasis in original).
- "***If our security measures are breached resulting in the improper use and disclosure of user data, or if our services are subject to attacks that degrade or deny the ability of users to access our products and services, our 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***." *Id*. (emphasis in original).
- "***Concerns*** 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***." *Id*.
- "Any systems failure or compromise of our security that results in the release of our users' data, or in our or our users' ability to access such data, could seriously harm our reputation and brand and, therefore, our business, and impair our ability to attract and retain users." *Id*.

[2] Plaintiff summarizes its factual allegations in this section for purposes of brevity, but Defendants' MTD should be judged against the "complaint in its entirety." *See Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007).

In March 2018, however, a month after filing the 2017 10-K, Google learned that its data security was in disarray and the data-privacy risks it had warned investors about for years were materializing and poised to get worse. ¶37. The tip of this iceberg was a software bug that allowed hundreds of third-party developers access to private user-profile data in its Google+ social-networking platform. *Id.* The exposed user data included full names, email addresses, birth dates, gender, profile photos, places lived, occupations and relationship status. *Id.* Google had failed to detect this bug for over three years and it only maintained two weeks of activity logs, which meant it could not identify affected users and had no way to determine the extent of third-party exploitation. ¶¶37, 73. The Complaint refers to this lone bug as the "Three-Year Bug," and its belated discovery led to Google's realization of other vulnerabilities, including the inevitability of more bugs, that it simply could not contain – the Complaint refers to this overarching iceberg of data-security issues as the "Privacy Bug." ¶38.

In or around April 2018, Google's legal and policy staff prepared a memo on the Privacy Bug that outlined the Company's internal debate as to whether it should disclose the Three-Year Bug to the public ("Privacy Bug Memo"). ¶¶38-39. Pichai and other senior Google executives received and read the Privacy Bug Memo, which explicitly warned that disclosure of the Three-Year Bug would likely trigger "'immediate regulatory interest'"; result in Defendants "'coming into the spotlight alongside or even instead of Facebook despite having stayed under the radar throughout the Cambridge Analytica scandal'"[3]; and would "'almost guarantee[] Sundar [Pichai] will testify before Congress.'" ¶38. In other words, revealing the tip would make the rest of the iceberg much harder to hide. So, Pichai and other senior Google executives, including the other Individual Defendants, decided to prepare to shutdown Google+, the world's fifth largest social media network, and approved a plan to conceal everything. ¶¶39-41.

[3] In April 2018, Congressional hearings were underway into the "future of data privacy and social media" following the revelation of Facebook's leak of user information to third-party research firm Cambridge Analytica. ¶33. While Defendants evaded the hearings to distance themselves from the scandal, Cambridge Analytica was able to harvest private user information from Facebook using the exact same type of faulty mechanism that plagued Google+: an API that allowed third-party developers access to private information from both users and those users' connections. ¶¶33, 62.

B. Defendants Chose to Discuss Data-Security and Trust Issues, but Did so in a Misleadingly Incomplete Manner

On April 23, 2018, the first day of the Class Period (April 23, 2018 to October 7, 2018), Defendants filed their Quarterly Report on Form 10-Q for the period ending March 31, 2018 (the "1Q 2018 10-Q"). In it, Defendants intentionally chose to include a "Risk Factors" section; intentionally incorporated the Risk Factors disclosures from the Company's 2017 10-K; intentionally represented that "[t]here have been no material changes to our risk factors since our [2017 10-K]"; and intentionally omitted any reference to the Three-Year Bug and the overarching Privacy Bug, which, as alleged, created a whole new (and undisclosed) risk: that consumers, legislators and regulators would find out that Defendants had abandoned their self-proclaimed role as "champion[s] of disclosure and transparency" for a policy of concealment and opacity (the "Policy Pivot"). ¶¶43-44, 47, 55-56. Instead, Defendants continued touting their supposed "robust and strong privacy program" while concealing the Three-Year Bug and the Privacy Bug on the 1Q 2018 earnings call (¶45), as well as throughout the remainder of the Class Period (¶¶46-50, 52-53) and many additional statements they chose to make regarding data-security and their trustworthiness, including statements: (a) in an April 27, 2018 Proxy Statement (¶47); (b) at a June 6, 2018 Annual Shareholders Meeting (¶48); (c) in a July 23, 2018 Quarterly Report on Form 10-Q for the period ending June 30, 2018 (the "2Q 2018 10-Q") and on an earnings call that same day (¶¶49-50); (d) in a September 24, 2018 blog post (¶53); and (e) in September 26, 2018 written testimony to the Senate Committee on Commerce, Science and Transportation (¶52). Even in response to a request from the Senate Judiciary Committee for "information on Google's current data privacy policies, ***specifically as they relate to Google's third party developer APIs***," Defendants concealed the fact that the Three-Year Bug had exposed user data to third-party developers since 2015 and that more bugs were on the horizon. ¶¶38, 46, 62, 64.

C. Defendants Lose Containment of the Privacy Bug

On October 8, 2018, the *Wall Street Journal* ("*WSJ*") published an article entitled "Google Exposed User Data, Feared Repercussions of Disclosing to Public," exposing Defendants' discovery of, and decision to conceal, the Three-Year Bug. ¶57. That same day, Google published a response

that did not dispute Pichai's reported receipt of the Privacy Bug Memo and involvement with the decision to conceal the Three-Year Bug. ¶58. Google also alluded to the overarching Privacy Bug by admitting that it could not adequately secure its Google+ platform. *Id*.

The response to this revelation and others to follow was significant. Both Republican and Democratic Senators condemned Defendants' concealment and called for further investigations into the Company, stating that "[t]he awareness and approval by Google management to not disclose represents a culture of concealment and opacity set from the top of the company." ¶¶59-62. Media reports similarly slammed the Company, noting that "Google's business model is based on trust, and hiding a potentially dangerous breach for six months is not the way to keep it." ¶¶66-67. Following these reactions and other revelations and manifestations, Alphabet's stock price fell both immediately and belatedly, damaging investors. ¶82.

D. Straightening Defendants' Spin

Page constraints prevent Plaintiff from correcting all of Defendants' fact-twisting. Nevertheless, the following examples demonstrate their MTD's unreliability:

DEFENDANTS' SPIN	REALITY
"Nor was it happenstance that Google itself found and fixed the problem. The Google+ bug was discovered as part of Google's own proactive attempt to review its policies and third[-]party developer access." MTD at 4.	"Google's security controls were so inadequate that it failed to detect this Three-Year Bug for approximately 150 weeks, yet it could only identify two weeks' worth of users whose private profile information had been exposed." ¶37. Unless Defendants reviewed Google's data security only once every three years (which would be another problem altogether), their belated discovery of the Three-Year Bug was very much a coincidence.
"Google found no evidence of data misuse." MTD at 4.	Democratic Senators: "Google has claimed that it 'found no evidence that any developer was aware of this bug, or abusing the API . . . .' These denials clash with the fact that Google has insufficient records to determine whether a breach occurred. According to its statement, the company only kept logs for two weeks. Google can only account for whether the vulnerability had been exploited in the weeks preceding its discovery. As such, we may never know the full extent of the damage caused by the failure to provide adequate controls and protection to users." ¶59.
"Plaintiff again fails to plead facts showing that the bug was material." MTD at 8.	Pichai: "I think today we always think we operate under the framework that users use Google because they trust us and it is something easy to lose if you are not good stewards of it." ¶26.

DEFENDANTS' SPIN	REALITY
	2017 10-K: "***Concerns*** 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***." ¶27.
"At the time the statements were made, ***there was no bug or vulnerability to disclose***." MTD at 8 (emphasis in original).	Republican Senators: "Google apparently elected to withhold information ***about a relevant vulnerability*** for fear of public scrutiny." ¶61. "[The Privacy Bug Memo concerned] the many shortcomings in Google's security system and record keeping, which revealed previously unknown, or unappreciated, ***security vulnerabilities that made additional data exposures virtually inevitable***." ¶38. Google also confirmed the existence of previously undisclosed vulnerabilities when it announced that it was "shutting down its Google+ social networking site and service for consumers because Google had failed to develop a product consumers wanted to use, including one with adequate controls over Google+ users' private data, which the blog described as 'significant challenges' that the authors of the Privacy Bug Memo had 'highlight[ed].'" ¶58 Weeks after the *WSJ* exposed the Three-Year Bug, Google confirmed the inevitability of the additional exposures from the vulnerabilities that remained ***after*** Google plugged (and concealed) the Three-Year Bug by revealing that "another Google+ bug had exposed user data from 52.5 million accounts." ¶64.

III. Legal Standard

The federal securities laws were enacted "to substitute a philosophy of ***full disclosure*** for the philosophy of *caveat emptor* and thus to achieve a high standard of business ethics in the securities industry." *SEC v. Capital Gains Research Bureau, Inc.*, 375 U.S. 180, 186 (1963). In order to establish a claim of securities fraud under §10(b) of the Securities Exchange Act of 1934 ("Exchange Act") and SEC Rule 10b-5, a plaintiff must allege: (1) a material misrepresentation or omission; (2) made with scienter; (3) in connection with the purchase or sale of a security; (4) relied upon by plaintiff; (5) a loss causally connected to the alleged fraud; and (6) economic loss or damages.[4] *Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 1008 (9th Cir. 2018); *see also Dura Pharm.,*

[4] Defendants' MTD challenges only the elements of falsity and scienter, conceding that Plaintiff has adequately pled the remaining four elements of its §10(b) claim (*i.e.*, purchase of a security, reliance, loss causation and damages).

Inc. v. Broudo, 544 U.S. 336, 341-42 (2005). Under Rule 10b-5, it is unlawful "to omit to state a material fact necessary in order to make the statements made . . . not misleading." 17 C.F.R. §240.10b-5(b).

In assessing a motion to dismiss under Fed. R. Civ. P. 12(b)(6), a court must "consider the complaint in its entirety," "accept all factual allegations . . . as true" and construe those allegations in the light most favorable to the plaintiff. *Tellabs*, 551 U.S. at 322-23. A complaint "does not need detailed factual allegations," but need only allege "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555, 570 (2007). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

In addition to Rule 12(b)(6)'s requirements, under Fed. R. Civ. P. 9(b), Plaintiff's omissions and scienter allegations must include "the 'time, place, and specific content of the [misleading statement] as well as the identities of the parties to the [statement].'" *Swartz v. KPMG LLP*, 476 F.3d 756, 764 (9th Cir. 2007).

IV. The MTD Is Limited to Only One Aspect of Plaintiff's Allegations

The MTD neither acknowledges nor seeks to dismiss the Complaint's allegations regarding the overarching Privacy Bug or their Policy Pivot. ¶¶38, 55-56. Nor do Defendants acknowledge or address any allegations concerning the Privacy Bug Memo. ¶¶38-39. Of course, Defendants may not use their reply brief to belatedly challenge these allegations. *See, e.g.*, *United States v. Cox*, 7 F.3d 1458, 1463 (9th Cir. 1993) ("a party may not make new arguments in the reply brief"). Accordingly, Defendants' MTD is one for partial dismissal, and it is not well taken even as to this limited scope.[5]

[5] If the Court grants Defendants' MTD in whole or in part, Plaintiff respectfully requests leave to amend. *See Eminence Capital, LLC v. Aspeon, Inc.*, 316 F.3d 1048, 1051-52 (9th Cir. 2003) (leave to amend should be granted "'with extreme liberality,'" especially in securities fraud cases).

V. The Complaint Properly Alleges How and Why Defendants' Omissions Rendered Its Public Statements Materially Misleading

A sound complaint for securities fraud is one that "'specifi[es] each statement alleged to have been misleading, [and] the reason or reasons why the statement is misleading.'" *In re VeriFone Holdings, Inc. Sec. Litig.*, 704 F.3d 694, 701 (9th Cir. 2012) (quoting 15 U.S.C. §78u-4(b)(1)(B)); *see also In re Daou Sys., Inc.*, 411 F.3d 1006, 1014 (9th Cir. 2005). Even an objectively true statement "may be misleading if it ***omits*** material information." *Khoja*, 899 F.3d at 1008-09; *Brody v. Transitional Hosps. Corp.*, 280 F.3d 997, 1006 (9th Cir. 2002) (holding that an omission is actionably misleading when it "create[s] an impression of a state of affairs that differs in a material way from the one that actually exists"). In other words, "'once defendants [choose] to tout positive information to the market, they [are] bound to do so in a manner that wouldn't mislead investors, including disclosing adverse information that cuts against the positive information.'" *Khoja*, 899 F.3d at 1009 (quoting *Schueneman v. Arena Pharm., Inc.*, 840 F.3d 698, 705-06 (9th Cir. 2016)); *see also In re Vivendi, S.A. Sec. Litig.*, 838 F.3d 223, 258 (2d Cir. 2016) ("'[O]nce a company speaks on an issue or topic, there is a duty to tell the whole truth,' '[e]ven when there is no existing independent duty to disclose information' on the issue or topic."). "[W]hether a public statement is misleading, or whether adverse facts were adequately disclosed is a mixed question to be decided by the trier of fact." *Fecht v. Price Co.*, 70 F.3d 1078, 1080-81 (9th Cir. 1995). Thus, "only if the adequacy of the disclosure or the materiality of the statement is 'so obvious that reasonable minds [could] not differ' are these issues 'appropriately resolved as a matter of law.'" *Id.*; *see also SEC v. Todd*, 642 F.3d 1207, 1220 (9th Cir. 2011) ("[R]esolving an issue as a matter of law is only appropriate when the adequacy of the disclosure is 'so obvious that reasonable minds [could] not differ.'").

Defendants do not dispute that the Complaint identifies the precise statements about Google's data privacy practices alleged to be misleading, who made those statements and where and when the statements were made. *See* ¶¶43-53. Nor can Defendants dispute that Plaintiff has alleged, with specificity, how those statements "omitted to state material facts necessary in order to make them not misleading." *See* ¶¶55-56. Faced with these facts, Defendants resort to arguing that

plugging one leak (the Three-Year Bug) somehow righted their sinking data-security ship and: (1) absolved them of any responsibility for concealing the Three-Year Bug (MTD at 8-9) (again, Defendants ignore altogether their responsibility for concealing the Privacy Bug and the new risks of their Policy Pivot); and (2) rendered immaterial the concealed information that reached to the core of Google's business model (*id*. at 10-13). Defendants' arguments would ring hollow at any stage of this litigation (including trial), but they are particularly inapt, and contrary to well-established Ninth Circuit law, at the pleading stage.

A. Defendants' SEC Filings and Public Statements Misleadingly Omitted the Three-Year Bug, the Privacy Bug, and the Policy Pivot

Defendants did not disclose the Three-Year Bug, the Privacy Bug, or their Policy Pivot in: (a) the Forms 10-Q that the Company filed with the SEC on April 23, 2018 and July 23, 2018 (¶¶43, 49); or (b) any of their public statements discussing data privacy and security, as well as their trustworthiness, over the course of the Class Period (¶¶44-48, 50, 52-53). Both the 1Q and 2Q 2018 10-Qs directly incorporated the "Risk Factors" from the Company's 2017 10-K, and stated that there were no material changes to those risk factors concerning data privacy and security issues (*see* ¶¶27, 43, 49) – portraying Google's data-security situation as completely unchanged. But a statement that "speaks entirely of as-yet-unrealized risks and contingencies" is misleading where it does not "alert[] the reader that some of these risks may already have come to fruition." *See Berson v. Applied Signal Tech., Inc*., 527 F.3d 982, 986 (9th Cir. 2008). Courts in the Ninth Circuit have consistently found risk disclosures to be actionably misleading by omission where defendants knew that the factors they warned of as mere possibilities had already come to pass. *See id*; *Khoja*, 899 F.3d at 1016 (holding complaint sufficiently pled falsity by omission where statements in Form 10-Q warned that new data "'***may*** be inconsistent'" with prior results, when defendants "already [knew] that the 'new data' revealed exactly that"); *Siracusano v. Matrixx Initiatives, Inc.*, 585 F.3d 1167, 1181 (9th Cir. 2009) (Form 10-Q statements were misleading for giving "no indication that the risk 'may already have come to fruition'" were "sufficiently strong to survive a motion to dismiss" where complaint alleged that defendants had knowledge that the risks had materialized), *aff'd*, 563 U.S. 27 (2011); *In re Snap Inc. Sec. Litig.*, No. 2:17-cv-03679-SVW-AGR, 2018 WL 2972528, at *6 (C.D. Cal. June 7, 2018)

(finding that "hypothetical risk disclosures – *e.g.*, Instagram Stories '***may*** be directly competitive,' – do not absolve Defendants of their duty to disclose known material adverse trends currently affecting Snap's user growth") (emphasis in original); *Flynn v. Sientra, Inc.*, No. CV 15-07548 SJO (RAOx), 2016 WL 3360676, at *10-*11 (C.D. Cal. June 9, 2016) (holding that plaintiff adequately pled falsity where risk factor statements spoke "'about the risks of [product contamination and failure to comply with GMP] in the abstract, with no indication that the risk[s] "may already have come to fruition"'").

Ignoring this wealth of in-Circuit case law, Defendants reach for an unpublished Sixth Circuit opinion, *Bondali v. Yum! Brands, Inc.*, 620 F. App'x 483 (6th Cir. 2015), in purported support of their extraordinary claim that where "a company warns that a problem may occur ***in the future***, but does not disclose that the problem had actually occurred and was remediated ***in the past***, the nondisclosure does not render the warning misleading." *See* MTD at 8-9 (emphasis in original). As discussed above, Defendants' proposition flies in direct contravention of the Ninth Circuit's holdings in *Berson*, 527 F.3d at 986, *Khoja*, 899 F.3d at 1016, and *Siracusano*, 585 F.3d at 1181, regarding the misleading nature of risk disclosures that omit to mention that those very risks have "come to fruition."[6] Even courts within the Sixth Circuit have refused to read *Bondali* as somehow rewriting the Exchange Act. *See, e.g.*, *Weiner v. Tivity Health, Inc.*, 365 F. Supp. 3d 900, 905, 909-10 (M.D. Tenn. 2019) (recognizing that "*Bondali* is unpublished and therefore not 'binding precedent' or 'binding authority,'" and denying motion to dismiss where risk disclosures failed to disclose that a competitive "potentiality had become a reality").

In fact, Defendants' argument contradicts their own warnings, which consistently recognized that the greatest threat Google faces is the ***perception*** of inadequate security. *See, e.g.*, ¶27

[6] Defendants' citation to *Kim v. Advanced Micro Devices, Inc.*, No. 5:18-cv-00321-EJD, 2019 WL 2232545, at *7 (N.D. Cal. May 23, 2019), is inapposite, as the Court there found that "the potential risks disclosed in the SEC filings had ***not*** come to fruition when Defendants filed the challenged risk disclosures." That is because in *Kim*, "the danger warned of by Defendants were cyber-attacks, data breaches, and resulting litigation – not the discovery of vulnerabilities in AMD's processors." *Id.* at *8. Here, even Defendants' myopic MTD concedes that "Plaintiff's substantive allegations allege a bug," and that the Company's risk disclosures "warned of" bugs and data vulnerabilities as unrealized potentialities. MTD at 9 n.9. Unlike *Kim*, the risks that had come to fruition here were the same kind of risks Google had described as mere potentialities.

("***Privacy concerns relating to our technology could damage our reputation and deter current and potential users or customers from our products and services***.") (emphasis in original); *id.* ("***Concerns*** 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***.").[7] Clearly, Google had never prepared investors for a world in which its business model depended on securing users' private data ***and*** concealing any privacy exposures and vulnerabilities. If "remediation" = "plug and conceal," why would Google's reputation be at risk? How could Google's reputation suffer from failings it successfully conceals? Plugging and concealing the Three-Year Bug did not fully remediate anything, let alone everything.[8]

Aside from the risk factor statements in the Forms 10-Q, Defendants argue that the remaining Class Period statements (*see* ¶¶45-48, 50, 52-53) "are too vague and generalized to be actionable." MTD at 13-15. But Defendants' argument is based on their misconstruction of the Complaint, which does not allege false statements, as in the cases regarding statements of corporate optimism and puffery on which Defendants rely. Instead, the Complaint plainly and clearly alleges that Defendants' voluntary public statements highlighting Google's purported trustworthiness and commitment to data privacy and security were misleading by way of omission (*see* ¶¶55-56), as they created "an impression of a state of affairs that differ[ed] in a material way from the one that actually exist[ed]." *See Brody*, 280 F.3d at 1006. That is, after learning of the Three-Year Bug, the

---

[7] Defendants argue that, "[i]t is hard to see how the above-quoted warnings [from the 2017 10-K] did not adequately warn investors, even without disclosure of the past bug." MTD at 9-10. But Defendants conceded the inadequacy (*i.e.*, the incompleteness) of their prior disclosures when they filed the Company's 2018 Form 10-K, which ***added*** previously omitted information. ¶72. Defendants' Class Period statements would have conveyed a vastly different impression if they included the information Defendants omitted. For example, adding the emphasized omitted information to the following actual statement gives it a much different meaning: "Concerns 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. [***Accordingly, the best way to protect our reputation is to patch and conceal data-security vulnerabilities without determining the extent of harm or notifying users, while professing our commitment to disclosure and transparency, because what users don't know can't hurt us***]."

[8] Defendants' citation to a series of inapposite cases where the warned-of risks never materialized (*see* MTD at 9 n.8) does not support the claim that their "remediation" efforts absolved themselves of their duty to disclose the Privacy Bug.

overarching Privacy Bug, and responding with the Policy Pivot, Defendants misleadingly spent the next six months painting a rosy picture of stability and an unflinching commitment to data-security and "transparency in all areas of [its] business." ¶47. "[O]nce defendants chose to tout" the security of its products and their policy of disclosure and transparency, "they were bound to do so in a manner that wouldn't mislead investors," which is the opposite of what they did. *See Berson*, 527 F.3d at 987; *In re Questcor Sec. Litig.*, No. SA CV 12-01623 DMG (FMOx), 2013 WL 5486762, at *11 (C.D. Cal. Oct. 1, 2013) ("Rule 10b-5 forbids omissions of 'material fact[s] necessary in order to make the statements made . . . not misleading.'"); *KB Partners I, L.P. v. Pain Therapeutics, Inc.*, No. A-11-CA-1034-SS, 2015 WL 7760201, at *8 (W.D. Tex. Dec. 1, 2015) ("'under Rule 10b-5, a duty to speak the full truth arises when a defendant undertakes a duty to say anything'"); *Meyer v. JinkoSolar Holdings Co., Ltd.*, 761 F.3d 245, 250 (2d Cir. 2014) ("[O]nce a company speaks on an issue or topic, there is a duty to tell the whole truth.").

B. Data Security and Trustworthiness Matter Most When Your Only Product Is Consumers' Private Data

The Complaint also plainly alleges why the Three-Year Bug, the overarching Privacy Bug, and the Policy Pivot were material, *i.e.*, that "'"'disclosure of the[m] would have been viewed by the reasonable investor as having significantly altered the "total mix" of information made available."'" *Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. 27, 38 (2011); *see also Omnicare, Inc. v. Laborers Dist. Council Constr. Indus. Pension Fund*, __ U.S. __, 135 S. Ct. 1318, 1333 (2015) (omitted fact is material if "'there is a substantial likelihood that a reasonable [investor] would consider it important'"). Defendants' challenge to materiality (MTD at 10-13) simply ignores the Complaint's overwhelming allegations:

- The omission of the facts set forth in ¶55 from Alphabet's Forms 10-Q jeopardized the central element of what "the Companies' success is largely dependent on" – "maintaining consumers' trust such that users will continue to entrust Google with their private data, which Google can then monetize." ¶65; *see also* ¶¶18, 23-30, 65 (discussing importance of confidence in Google's data-security of private information).[9] This was particularly true because the facts were withheld

[9] *See also Litwin v. Blackstone Grp., L.P.*, 634 F.3d 706, 720 (2d Cir. 2011) (a misstatement or omission's "significance to a particularly important segment of a registrant's business tends to show its materiality"); *In re Equifax Inc. Sec. Litig.*, 357 F. Supp. 3d 1189, 1224 (N.D. Ga. 2019) ("Furthermore, the fact that these statements relate to a core aspect of Equifax's business makes it even more likely that a reasonable investor would assign weight to them. Since data security plays an

at a time when Google faced "unprecedented public and regulatory scrutiny for its data collection and privacy practices," due to, *inter alia*, Facebook's data security scandal which quickly shifted Congress's focus to Google (¶33), worldwide implementation of the European Union's General Data Protection Regulation ("GDPR") (¶¶34-35) and Google's Consent Order with the Federal Trade Commission ("FTC") (¶36).

- The Privacy Bug revealed that Google's technology to protect users' private data was not as good as investors were led to believe. It exposed systemic securities deficiencies in the Company's Google+ service that "rendered additional bugs and data exposures virtually inevitable," an area of materiality that Defendants gloss over. ¶¶38, 55, 73.

- Defendants adopted a "plan to hide the Privacy Bug from all users and everyone else outside of the Companies," which Pichai personally approved because, *inter alia*, he thought it would subject Google and him to regulatory scrutiny. ¶¶40-42; *see also* ¶¶61, 68. Defendants' decision to conceal the Privacy Bug and their motivation for doing so also provides an altogether independent basis for the materiality of the Forms 10-Q: it revealed that "management was [not] at trustworthy as they had led the public, including investors, to believe," an area of obvious importance to reasonable investors. ¶55.[10]

- The harms suffered by the Company (many of which the Privacy Bug Memo anticipated) when the truth was disclosed included: governmental investigations, Congressional hearings, consumer and shareholder lawsuits, and a stock-price drop. ¶¶38, 61, 64, 68, 70, 81-82.[11] Moreover, as alleged, "[t]his was such a significant breach and Google's faith in its security was so shaken, the Privacy Bug led Pichai and Page to approve a plan to shutdown Google's Google+ social networking site and service. Put simply, Google no longer trusted itself." ¶41; *see also* ¶76.

In addition to ignoring these clear materiality allegations, Defendants disregard the law of materiality, which is an inherently fact-based inquiry that is rarely appropriate for pre-trial determination, let alone at the pleading stage. *See Litwin*, 634 F.3d at 717 (""[A] complaint may

---

important part of a business such as Equifax, investors would be even more likely to find these types of representations important in making their investment decisions.").

[10] *See In re Sipex Corp. Sec. Litig.*, No. C 05-00392 WHA, 2005 WL 3096178, at *2 (N.D. Cal. Nov. 17, 2005) ("Moreover, the sham transaction was material in a wholly different sense: Investors would be interested in knowing that the company CEO, president and director was personally orchestrating the phony sale alleged. This would have raised a red flag for investors that top management was potentially corrupt. This was not disclosed. This alone made the sham transaction material.").

[11] *See Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, Release Nos. 33-10459, 34-82746 (Feb. 21, 2018) ("The materiality of cybersecurity risks and incidents also depends on the range of harm that such incidents could cause. This includes 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.").

not properly be dismissed . . . on the ground that the alleged misstatements or omissions are not material unless they are so obviously unimportant to a reasonable investor that reasonable minds could not differ on the question of their importance.""""); *see also TSC Indus., Inc. v. Northway, Inc.*, 426 U.S. 438, 450 (1976) (noting that even at the summary judgment stage, the "determination [of materiality] 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, and these assessments are peculiarly ones for the trier of fact").

Defendants are certainly free to try to convince a jury that the Three-Year Bug was immaterial because "the data at issue here were [not] of an inherently sensitive nature, such as social security numbers, medical records, or bank account information." MTD at 11. Plaintiff welcomes such an argument because it ignores: (1) that the exposed data – which included birth dates, photos, occupations, relationship status, email addresses and places lived – was information ***that users had designated as private***; (2) that Google failed to discover or patch this leak for over three years and could not determine the extent of exposure or exploitation; (3) the overarching Privacy Bug; and (4) the Policy Pivot – all of which would undermine consumer confidence in Google's data security and integrity, which would imperil Google's business model, as Google had repeatedly warned.[12] In light of these facts and circumstances, if either side were entitled to a pleading-stage materiality determination, it would be Plaintiff, not Defendants. *See, e.g.*, *Equifax*, 357 F. Supp. 3d at 1224 ("[T]he Court cannot say, as a matter of law, that Equifax's representations that its cybersecurity efforts were extensive or that it was 'committed' to data security were so 'obviously unimportant' to its shareholders that they should be considered immaterial."). Likewise, it is of no moment that the

[12] Similarly misguided is Defendants' assertion that "***Plaintiff . . . fails to identify a single user whose Google+ information or data were* (sic) *actually misused***." MTD at 12 (emphasis in original). Again, what is important is that ***Google cannot identify a single user whose information or data was not misused*** because Defendants simply do not know due to their lax security measures. Such uncertainty is exactly what leads to "***[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***, [that] ***could damage our reputation and adversely affect our operating results***." ¶27.

Privacy Bug is not alleged to have "materially affected earnings." MTD at 11; *see Matrixx*, 563 U.S. at 44 (rejecting bright-line rule for materiality, which requires a "contextual inquiry").[13]

The Complaint clearly establishes that a reasonable investor would want to know the omitted information described in ¶¶55-56. Defendants' disregard of Plaintiff's allegations and the well-established legal principle that materiality is a question of fact means their materiality argument should be disregarded.

VI. The Complaint Alleges Both Direct Knowledge and Particularized Facts that Raise a Strong Inference of Scienter

A complaint successfully pleads the element of scienter where it "state[s] with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind" – *i.e.*, that the defendants' conduct was "'***knowing***' or '***intentional***'" or otherwise rose to the level of "'deliberate recklessness.'" *S. Ferry LP, No. 2 v. Killinger*, 542 F.3d 776, 782 (9th Cir. 2008) (emphasis in original); 15 U.S.C. §78u-4(b)(2)(A); *see also Provenz v. Miller*, 102 F.3d 1478, 1490 (9th Cir. 1996) (same). A "strong inference" is one that a reasonable person would deem "cogent and at least as compelling as any opposing inference one could draw from the facts alleged." *Tellabs*, 551 U.S. at 324. The key question in evaluating scienter is "whether ***all*** of the facts alleged, taken collectively, give rise to a strong inference of scienter, not whether any individual allegation, scrutinized in isolation, meets that standard." *Id.* at 322-23 (emphasis in original). No "smoking-gun" is necessary, nor does the inference need to be the "'most plausible of competing inferences.'" *Id.* at 324.

Here, the Complaint alleges that Defendants had actual knowledge of the Three-Year Bug, the overarching Privacy Bug, and that they decided on the Policy Pivot – all to avoid public and

---

[13] *See also Nathanson v. Polycom, Inc.*, 87 F. Supp. 3d 966, 974 (N.D. Cal. 2015) ("Even assuming, as Defendants argue, that these misstatements or omissions were 'minor or technical in nature,' and thus quantitatively immaterial, Plaintiff has adequately pleaded materiality because '[i]nvestors have a right to know – and would consider it important . . . .'"); *Smilovits v. First Solar Inc.*, 119 F. Supp. 3d 978, 1002-03 (D. Ariz. 2015) ("But the test for materiality is factual – whether a misrepresented or omitted fact would have been viewed by a reasonable investor as having significantly altered the total mix of information made available – and Defendants fail to provide undisputed evidence that a reasonable investor would consider a product defect irrelevant if it constitutes, say, only 1.5% of net income."); *aff'd sub nom. Mineworkers' Pension Scheme v. First Solar Inc.*, 881 F.3d 750 (9th Cir. 2018).

regulatory scrutiny at a time of legislative hearings and maximum sensitivity to privacy issues. ¶¶37-39, 55-56. These facts alone establish scienter, and the competing inferences that Defendants wish the Court to draw simply confirm that this is a question of fact.

A. Defendants' Direct Knowledge of the Privacy Bug and Direct Involvement in the Policy Pivot Establish Scienter

The "'fact that the defendants published statements when they ***knew*** facts suggesting the statements were inaccurate or misleadingly incomplete is classic evidence of scienter.'" *In re Immune Response Sec. Litig.*, 375 F. Supp. 2d 983, 1022 (S.D. Cal. 2005) (quoting *Aldridge v. A.T. Cross Corp.*, 284 F.3d 72, 83 (1st Cir. 2002)); *see also N.M. State Inv. Council v. Ernst & Young LLP*, 641 F.3d 1089, 1095 (9th Cir. 2011) ("A complaint can plead scienter by raising a strong inference that the defendant possessed ***actual knowledge*** or acted with deliberate recklessness.").[14] As alleged, Google discovered the Three-Year Bug in March 2018. ¶37. In April 2018, "Google's legal and policy staff prepared a memo concerning this security breach, including the many shortcomings in Google's security system and record keeping, which revealed previously unknown, or unappreciated, security vulnerabilities that made additional data exposures virtually inevitable" – *i.e.*, the Privacy Bug Memo about the overarching Privacy Bug. ¶38. Pichai and other senior Google executives received and read the Privacy Bug Memo in or around early April 2018. ¶39. By way of their positions as Legal Director of Privacy/Chief Privacy Officer and General Counsel, respectively, defendants Enright and Walker comprised or oversaw the staff that prepared the Privacy Bug Memo, and they were part of the select group of top product executives who decided on the Policy Pivot, so the allegations establish their direct knowledge and scienter. ¶¶55, 74, 79. Defendant Page is the only defendant for whom an inference of knowledge is necessary, and he was "the chief operating decision maker of Alphabet [who] was responsible for making . . . key operating decisions at Google," as well as Pichai's lone superior. ¶78(a). It is implausible to the point of

[14] Detailed allegations demonstrating that "defendants had ***actual access*** to the disputed information" are also sufficient to raise a strong inference of scienter. *S. Ferry*, 542 F.3d at 785-86. "To raise an inference of scienter as to a corporate defendant . . . a complaint generally must plead scienter as to the individual executives or directors of the entity." *Brown v. China Integrated Energy, Inc.*, 875 F. Supp. 2d 1096, 1120 (C.D. Cal. 2012); *see also In re Cendant Corp. Litig.*, 264 F.3d 201, 238 (3d Cir. 2001) ("a corporate officer's fraud is imputed to the corporation").

absurdity that Page would not have been aware of the Three-Year Bug, the overarching Privacy Bug or involved in the Policy Pivot and the related decision to shut down the world's fifth-largest social media network, as that would mean "the 100-person task force, which discovered the largest data-security vulnerability in the history of two Companies whose existence depends on data security, concealed it from the Companies' CEOs." ¶74.[15]

When considered with the allegations of the Individual Defendants' direct knowledge, the Complaint's additional allegations concerning the: (a) critical nature of these issues; (b) importance of the decisions that had to be made regarding them; (c) reasons for those decisions (which directly impacted Pichai and Page); and (d) statements from a variety of speakers throughout the Class Period that faithfully omitted any reference to the Three-Year Bug, the overarching Privacy Bug, and the Policy Pivot, establish an inference of Defendants' scienter that is so strong, it is the lone logical inference under these circumstances.[16] ¶¶73-80.

B. Defendants' Motive Buttresses the Strong Inference of Scienter

While "motive is not required to adequately plead scienter" (*Gammel v. Hewlett-Packard Co.*, No. SACV 11-1404 AG (RNBx), 2013 WL 1947525, at *21 (C.D. Cal. May 8, 2013)), the Complaint details Defendants' motive to conceal the Three-Year Bug, the overarching Privacy Bug, and the Policy Pivot.[17] *See Reese v. Malone*, 747 F.3d 557, 569 (9th Cir. 2014) (facts showing a motive to commit fraud can "provide some reasonable inference of intent"); *Tellabs*, 551 U.S. at 325

[15] The Complaint also alleges that Page would have become aware of the Privacy Bug through his certification and adoption of Alphabet's 1Q 2018 10-Q and 2Q 2018 10-Q. ¶80. Page's certifications included an obligation to familiarize himself with the adequacy and controls for identifying cybersecurity risks. *Id*. Any such review would have necessarily involved an analysis of the Privacy Bug Memo. *Id*. Thus, Page's personal supervision and participation in this function also supports an inference of scienter that is, "as plausible as an inference of nonculpability." *See Commc'ns Workers of Am. Plan for Emps.' Pensions & Death Benefits v. CSK Auto Corp.*, 525 F. Supp. 2d 1116, 1124 (D. Ariz. 2007).

[16] Google was also subject to an FTC consent decree at the time Defendants learned of the Google+ bug, providing Defendants with heightened awareness of the risks and their responsibilities with respect to violating user-privacy rights. ¶36.

[17] Tellingly, one page of the MTD contends that "Plaintiff fails to articulate a coherent theory of, or any motive for, fraud" (MTD at 15), while the very next quotes an actual motive allegation from the Complaint (*id*. at 16 ("Plaintiff alleges that scienter may be inferred because Defendants purportedly 'approved a plan to hide the privacy Bug . . . to avoid additional regulatory scrutiny, including having to testify before Congress.'")).

("motive can be a relevant consideration"). Defendants expressly acknowledged their motive to conceal in their Privacy Bug Memo, which warned that disclosure would: (1) likely trigger "'immediate regulatory interest'"; (2) result in Defendants "'coming into the spotlight alongside or even instead of Facebook despite having stayed under the radar throughout the Cambridge Analytica scandal'"; and (3) "'almost guarantee[] Sundar [Pichai] will testify before Congress.'" ¶38.

Consistent with their history of omitting material information, Defendants' MTD refuses to acknowledge the Privacy Bug Memo. Instead, Defendants disingenuously claim that their handling of the Three-Year Bug had absolutely no relation to the Facebook Cambridge Analytica scandal. MTD at 16-17. Beyond the unambiguous language in the Privacy Bug Memo, Defendants' argument improperly contradicts Plaintiff's allegations, including that:

- At the time Defendants learned of the Three-Year Bug, "Congressional hearings into Facebook's leak of user information to third-party Cambridge Analytica were underway and threatened to turn to Google's data collection and privacy practices." ¶33.
- On April 10, 2018, after Google declined to participate in the Cambridge Analytica hearings, Senator Charles Grassley sent Pichai a letter outlining the Senate Judiciary Committee's "significant concerns regarding the data security practices of large social media platforms and their interactions with third party developers and other commercials users of such data" (*id.*) and "seeking information on Google's current data privacy policies, ***specifically as they relate to Google's third party developer APIs***." ¶62.
- On October 11, 2018, Senator Grassley sent Pichai a letter regarding the "troubling reports" detailed in the *WSJ* article, and noting that "[d]espite [Google's] contention that Google did not have the same data protection failures as Facebook, it appears from recent reports that ***Google+ had an almost identical feature to Facebook, which allowed third party developers to access information from users as well as private information of those users' connections***. Moreover, it appears that you were aware of this issue at the time I invited you to participate in the hearing and sent you the letter regarding Google's policies." ¶62.

These allegations, coupled with the Privacy Bug Memo, demonstrate that Defendants made a calculated decision to adopt the Policy Pivot to conceal the Three-Year Bug and the overarching Privacy Bug at a time when the "trustworthiness of technology and those who control it were under unprecedented scrutiny." ¶33.

C. Defendants' Other Factors and "Competing Inferences" Fail to Undermine the Strong Inference of Scienter

Having no answer for the fact that the Complaint alleges: (a) Defendants' direct knowledge; (b) facts establishing an overwhelming inference of scienter; and (c) a clear motive to conceal, Defendants are left with only rote arguments that ring hollow. MTD at 15-16.

First, the lack of Class Period stock sales does not negate a finding of scienter, and courts have repeatedly rejected Defendants' contrary argument. *See, e.g.*, *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."); *Sharenow v. Impac Mortg. Holdings, Inc.*, 385 F. App'x 714, 717 n.2 (9th Cir. 2010) ("we do not draw a negative inference from the absence of stock sales"); *In re LDK Solar Sec. Litig.*, 584 F. Supp. 2d 1230, 1255 (N.D. Cal. 2008) ("[P]laintiffs did not rely on allegations of insider trading to establish scienter, so the lack of stock sales by defendants did not negate the inference of scienter.").

Second, Defendants have no support for their remarkable contention that the lack of confidential witness allegations undermines scienter. MTD at 15-16. Indeed, courts have consistently found scienter sufficiently pled without the use of any confidential witnesses. *See, e.g.*, *Nursing Home Pension Fund, Local 144 v. Oracle Corp.*, 380 F.3d 1226, 1230 (9th Cir. 2004); *Ernst & Young*, 641 F.3d at 1095-103; *SEC v. Bardman*, 216 F. Supp. 3d 1041, 1052-54 (N.D. Cal. 2016).[18]

Finally, Defendants assert that when viewed holistically, the competing inferences in this case undermine a strong inference of scienter. MTD at 17. But Defendants' "competing" inferences are simply generic arguments that do not "compete" with Plaintiff's actual scienter allegations, and

[18] The cases Defendants do cite do not support their argument. *City of Roseville Emps.' Ret. Sys. v. Sterling Fin. Corp.*, 963 F. Supp. 2d 1092, 1132 (E.D. Wash. 2013), *aff'd*, 691 F. App'x 393 (9th Cir. 2017), only supports the proposition that confidential witnesses can be but one potential piece in a holistic analysis, as the court there placed equal weight on the fact that there were "no documents or internal communication to show that Defendants were apprised of adverse financial information which they then failed to communicate to the public." Similarly, Defendants cherry-pick a statement from *Applestein v. Medivation, Inc.*, 561 F. App'x 598, 600-01 (9th Cir. 2014), to manufacture their argument that a lack of confidential witness statements undermines scienter. MTD at 16. *Applestein*, however, is inapposite, as the allegations of securities fraud there were mainly based on the statements from three confidential witnesses who did not provide statements regarding defendants' knowledge of the fraud. 561 F. App'x at 601.

no court has ever granted a motion to dismiss based on generic arguments that do not address, let alone undermine, specific overwhelming evidence of scienter. Instead, Defendants cite a series of cases in which "the allegations d[id] not suggest that [] management was aware of the [allegedly concealed] problems,"[19] whereas here, Plaintiffs' allegations confirm management's awareness. *Compare* ¶¶37-39, 55-56, 70, 75-79, *with* MTD at 17-18 (citing cases with no factual allegations even suggesting management's knowledge).

VII. Section 20(a) Control Person Liability Is Properly Pled

Defendants do not dispute that the Complaint sufficiently alleges each Defendants' control and participation. *See* MTD at 18 n.21. Because Plaintiff has sufficiently alleged a primary violation of §10(b) and Rule 10b-5, the Complaint properly pleads control person liability under §20(a) as well.

VIII. Conclusion

For the reasons set forth above, Plaintiff has satisfied all applicable pleading standards and Defendants' MTD should be denied in its entirety.

DATED: July 8, 2019

Respectfully submitted,

ROBBINS GELLER RUDMAN
& DOWD LLP
JASON A. FORGE
MICHAEL ALBERT
J. MARCO JANOSKI GRAY
TING H. LIU

s/ JASON A. FORGE
JASON A. FORGE

655 West Broadway, Suite 1900
San Diego, CA 92101
Telephone: 619/231-1058
619/231-7423 (fax)

Lead Counsel for Plaintiff

[19] *In re Siebel Sys., Inc. Sec. Litig.*, No. C 04-0983 CRB, 2005 WL 3555718, at *5 (N.D. Cal. Dec. 28, 2005).

CERTIFICATE OF SERVICE

I hereby certify under penalty of perjury that on July 8, 2019 I authorized the electronic filing of the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the e-mail addresses on the attached Electronic Mail Notice List, and I hereby certify that I caused the mailing of the foregoing via the United States Postal Service to the non-CM/ECF participants indicated on the attached Manual Notice List.

s/ JASON A. FORGE
JASON A. FORGE

ROBBINS GELLER RUDMAN
& DOWD LLP
655 West Broadway, Suite 1900
San Diego, CA 92101-8498
Telephone: 619/231-1058
619/231-7423 (fax)

E-mail: jforge@rgrdlaw.com

Mailing Information for a Case 4:18-cv-06245-JSW In re ALPHABET, INC. SECURITIES LITIGATION

Electronic Mail Notice List

The following are those who are currently on the list to receive e-mail notices for this case.

- **Michael Albert**
  malbert@rgrdlaw.com,7223240420@filings.docketbird.com
- **Adam Marc Apton**
  aapton@zlk.com
- **Austin P. Brane**
  abrane@rgrdlaw.com
- **Benjamin Matthew Crosson**
  bcrosson@wsgr.com,bgavin@wsgr.com,fgarcia@wsgr.com
- **Boris Feldman**
  boris.feldman@wsgr.com,ncarvalho@wsgr.com
- **Jason A. Forge**
  jforge@rgrdlaw.com,kmccormack@rgrdlaw.com,e_file_sd@rgrdlaw.com
- **Cheryl Weisbard Foung**
  cfoung@wsgr.com,lcardenas@wsgr.com
- **J Alexander Hood , II**
  ahood@pomlaw.com,abarbosa@pomlaw.com
- **Joseph Marco Janoski Gray**
  mjanoski@rgrdlaw.com,tdevries@rgrdlaw.com
- **Phillip Kim**
  pkim@rosenlegal.com
- **Jeremy A Lieberman**
  jalieberman@pomlaw.com,disaacson@pomlaw.com,abarbosa@pomlaw.com,lpvega@pomlaw.com
- **Ting Hsiang Liu**
  TLiu@rgrdlaw.com
- **Danielle Suzanne Myers**
  dmyers@rgrdlaw.com,dmyers@ecf.courtdrive.com,e_file_sd@rgrdlaw.com
- **Jennifer Pafiti**
  jpafiti@pomlaw.com,disaacson@pomlaw.com,cgarcia@pomlaw.com,abarbosa@pomlaw.com
- **Samuel James Reed Dippo**
  sreeddippo@wsgr.com,srhodes@wsgr.com
- **Laurence Matthew Rosen**
  lrosen@rosenlegal.com,larry.rosen@earthlink.net

- **Shane Palmesano Sanders**
  ssanders@robbinsarroyo.com,notice@robbinsarroyo.com

- **Stephen Bruce Strain**
  sstrain@wsgr.com,pmarquez@wsgr.com

- **Shawn A. Williams**
  shawnw@rgrdlaw.com,e_file_sd@rgrdlaw.com,1101510420@filings.docketbird.com

Manual Notice List

The following is the list of attorneys who are **not** on the list to receive e-mail notices for this case (who therefore require manual noticing). You may wish to use your mouse to select and copy this list into your word processing program in order to create notices or labels for these recipients.

- (No manual recipients)