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. STATE OF RHODE ISLAND/OFFICE OF THE RHODE ISLAND TREASURER ON BEHALF OF THE EMPLOYEES' RETIREMENT SYSTEM OF RHODE ISLAND, Individually and on Behalf of All Others Similarly Situated, Plaintiff, vs. ALPHABET, INC., LAWRENCE E. PAGE, SUNDAR PICHAI, GOOGLE LLC, KEITH P. ENRIGHT, and JOHN KENT WALKER, JR. Defendants.	Master File No. 4:18-cv-06245-JSW CLASS ACTION CONSOLIDATED AMENDED COMPLAINT FOR VIOLATION OF THE FEDERAL SECURITIES LAWS DEMAND FOR JURY TRIAL

Lead Plaintiff State of Rhode Island, Office of the Rhode Island Treasurer on behalf of the Employees' Retirement System of Rhode Island ("Plaintiff"), on behalf of itself and the Class (as defined below) it seeks to represent, alleges the following upon knowledge as to its own acts and upon the investigation conducted by its counsel, which included, among other things, a review of: U.S. Securities and Exchange Commission ("SEC") filings by Alphabet; securities analysts' reports about Alphabet; press releases and other public statements issued by the Companies (as defined herein) and media reports about the Companies.

INTRODUCTION

1. This securities class action is brought on behalf of those who purchased or otherwise acquired securities of Alphabet, Inc. ("Alphabet") between April 23, 2018 and October 7, 2018, inclusive (the "Class Period"), seeking to pursue remedies under §§10(b) and 20(a) of the Securities Exchange Act of 1934 ("Exchange Act") and Rule 10b-5 promulgated thereunder.

2. This case arises out of defendants' misleading statements relating to data security and management integrity. Specifically, defendants learned of a three-year-long software glitch in the Google+ social media network that potentially exposed the private personal data of millions of Google+ users to third-parties, and led to the discovery of other systemic vulnerabilities that further compromised the data security of Google+ users. Defendants knew of these data-security issues in March of 2018, but for months, they continued to stress to investors the importance of data security and simply warned investors about ***risks*** related to data-security issues and concerns, while concealing that these risks had already been realized and that defendants had such poor security controls and record keeping that they could not determine the scope of the data breach, identify all of the affected users, detect other data-security bugs, or protect the private personal data of the tens of millions of Google+ users. The *Wall Street Journal* ("*WSJ*") led the exposure of defendants' scheme, triggering governmental investigations, Congressional hearings, the shutdown of the Google+ social media network, undermined confidence in the integrity of defendants' data security and management, and damaged investors.

JURISDICTION AND VENUE

3. The claims asserted herein arise under and pursuant to §§10(b) and 20(a) of the Exchange Act, 15 U.S.C. §§78j(b) and 78t(a), and Rule 10b-5 promulgated thereunder by the U.S. Securities and Exchange Commission ("SEC"), 17 C.F.R. §240.10b-5.

4. This Court has jurisdiction over the action pursuant to 28 U.S.C. §1331 and §27 of the Exchange Act.

5. Venue is proper in this Judicial District pursuant to §27 of the Exchange Act, 15 U.S.C. §78aa, and 28 U.S.C. §1391(b) as Alphabet and Google LLC are headquartered in this Judicial District.

6. In connection with the acts and conduct alleged in this Complaint, defendants, directly or indirectly, used the means and instrumentalities of interstate commerce, including, but not limited to, the United States mail, interstate wire and telephone communications, and the facilities of a national securities exchange.

THE PARTIES

7. Plaintiff, as set forth in the certification previously submitted and incorporated herein by reference, acquired Alphabet securities at an artificially inflated price during the Class Period and was damaged as a result of defendants' alleged misconduct. *See* ECF No. 19-3.

8. Defendant Alphabet is a multinational conglomerate headquartered in Mountain View, California. Its ordinary shares trade on the NASDAQ Global Select Market ("NASDAQ") under the ticker symbol "GOOG." As of January 31, 2019, there were 349,291,348 ordinary shares of Alphabet stock outstanding.

9. Defendant Google LLC is a technology company that specializes in Internet-related services and products, which include online advertising technologies, search engine, cloud computing, software, and hardware. Alphabet was created after a corporate restructuring of Google, Inc. on October 2, 2015, where Alphabet became the parent company of Google, Inc. and several other Google, Inc. subsidiaries. As part of the Alphabet reorganization, Google, Inc. was converted

into a limited liability company in September 2017.[1] Google is a wholly owned subsidiary of Alphabet.

10. Defendant Keith P. Enright ("Enright") was Google's Legal Director of Privacy from 2016 until September 2018, when he became Google's Chief Privacy Officer. In addition, since May 2018, Enright has been Google's "data protection officer" ("DPO") for the purpose of compliance with the European Union's General Data Protection Regulation ("GDPR").

11. Defendant Lawrence E. Page ("Page") is the co-founder of Google. In 2001, Page stepped aside as Google's CEO, only to resume the role in 2011. Just four years later, Page became the CEO of Alphabet. Throughout the Class Period, Page sat on Alphabet's Board of Directors, and was a member of the Board's three-person Executive Committee.

12. Defendant Sundar Pichai ("Pichai") has served as Chief Executive Officer ("CEO") of Google since 2015. Pichai's involvement with Google began in 2004, when he joined as the head of product management and development. In 2008, after working on Google's own browser, Chrome, Pichai was named Vice President of Product Development, and in 2012, he was named Senior Vice President. Thereafter, in 2014, Pichai was made product chief over both Google and the Android smartphone operating system. Throughout the Class Period, Pichai sat on Alphabet's Board of Directors, and beginning in April 2018 became a member of the Board's three-person Executive Committee.

13. Defendant John Kent Walker, Jr. ("Walker") was Google's Vice President and General Counsel from 2006 until August 2018, when he became Google's Senior Vice President for Global Affairs. As General Counsel, Walker was responsible for managing Google's global legal team and advising the company's Board of Directors and management on legal issues and corporate governance matters.

14. The defendants referenced above in ¶¶10-13 are also referred to herein as the "Individual Defendants."

[1] Google, Inc. and Google LLC are collectively referred to herein as "Google." Google and Alphabet are collectively referred to as "the Companies."

15. During the Class Period, the Individual Defendants, as senior executive officers and/or directors of Alphabet and/or Google, were privy to confidential and proprietary, non-public information concerning the Companies' operations and possessed the power and authority to control the contents of the Companies' public statements, including quarterly and annual reports, press releases, Congressional testimony, and presentations to securities analysts, money and portfolio managers, and institutional investors. They either made or received the Companies' statements alleged herein to be misleading prior to or shortly after their issuance and had the ability and opportunity to prevent their issuance or cause them to be corrected. Because of their positions with the Companies, personal participation in the fraud as detailed herein, communications with other corporate officers and employees, including their attendance at management and Board of Directors meetings, and their access to material non-public information available to them but not to the public, the Individual Defendants knew or disregarded with severe recklessness that the adverse facts specified herein had not been disclosed to, and were being concealed from, the investing public.

16. The Individual Defendants are liable as direct participants in the wrongs complained of herein. In addition, Page and Pichai, by reason of their status as senior executive officers and/or directors, were "controlling persons" within the meaning of §20(a) of the Exchange Act, and had the power and influence to cause the Companies to engage in the unlawful conduct complained of herein. Because of their positions of control, Page and Pichai were able to, and did, directly or indirectly control the conduct of the Companies' business.

17. As senior executive officers and/or directors of a publicly traded company whose stock was, and is, registered with the NASDAQ and governed by the federal securities laws, the Individual Defendants had a duty to promptly disseminate accurate and truthful information with respect to the Companies' security measures, data protections, operations, business, products, management, and earnings, and to correct any previously issued statements that had been materially misleading or untrue, so that the market price of Alphabet securities would be based upon truthful and accurate information. The Individual Defendants' omissions during the Class Period violated these requirements and obligations.

SUBSTANTIVE ALLEGATIONS

The Companies' Professed Commitment to "Do[ing] the Right Thing"

18. Alphabet is essentially a holding company. Its lifeblood is Google, and Google's lifeblood is technology and trust. In just two decades, Google has grown to one of the world's most valuable companies based on technology that: (1) allows it to track and collect an unprecedented amount of personal information about people; and (2) enables it to use that information to help companies sell stuff to those people. No matter what anyone does anywhere, Google is watching, or trying to watch. Without tremendous trust in Google's technology and management, consumers and investors would condemn what Google does as not just an invasion of privacy, but the destruction of privacy.

19. Google's founders, Sergey Brin and defendant Page, were acutely aware of the fine line between innovative assistance and insidious invasiveness. Google's technology is inextricably intertwined with its trustworthiness because without extensive consumer buy-in and participation, Google would be worthless because it would not have a critical mass of personal data to mine and exploit. This is why Google has always gone to great lengths to portray itself as uncommonly trustworthy. The prospectus for its initial public offering memorialized this portrayal:

> DON'T BE EVIL
>
> ***Don't be evil. We believe strongly that in the long term, we will be better served – as shareholders and in all other ways – by a company that does good things for the world even if we forgo some short term gains. This is an important aspect of our culture and is broadly shared within the company***. (Emphasis in original.)
>
> * * *
>
> MAKING THE WORLD A BETTER PLACE
>
> We aspire to make Google an institution that makes the world a better place. . . . We know that some people have raised privacy concerns, primarily over Gmail's targeted ads, which could lead to negative perceptions about Google. However, we believe Gmail protects a user's privacy. By releasing services, such as Gmail, for free, we hope to help bridge the digital divide. AdWords connects users and advertisers efficiently, helping both. . . .
>
> SUMMARY AND CONCLUSION

> Google is not a conventional company. Eric, Sergey and I intend to operate Google differently, applying the values it has developed as a private company to its future as a public company. Our mission and business description are available in the rest of this prospectus; we encourage you to carefully read this information. We will optimize for the long term rather than trying to produce smooth earnings for each quarter. . . . We are conscious of our duty as fiduciaries for our shareholders, and we will fulfill those responsibilities. . . . We will live up to our "don't be evil" principle by keeping user trust and not accepting payment for search results.
>
> * * *
>
> We have a strong commitment to our users worldwide, their communities, the web sites in our network, our advertisers, our investors, and of course our employees. Sergey and I, and the team will do our best to make Google a long term success and the world a better place.

20. In October 2013, Google's then-Executive Chairman, Eric Schmidt ("Schmidt"), made clear that if Google were to have a significant data breach "it would be devastating." Schmidt emphasized that regardless of the succession plan at Google, when it comes to data breaches, "[w]e're always one mistake away. It's inconceivable you could materially change that." Schmidt reassured conference attendees that Google's focus on data privacy would remain constant because then-CEO Page "is so precisely wired on these issues, it is inconceivable that there would ever be a change" and Google's culture was so strongly fixed on data security that it would remain the focus of the company for the foreseeable future.

21. Years later, when Google created its own parent, Alphabet, "don't be evil" became "do the right thing," but the message remained the same: you can trust us.

22. Following the creation of Alphabet, the Companies continued to tout their leadership in data-use transparency and security, not only as a central pillar of the Companies' culture, but also as a competitive advantage for Google and Alphabet to succeed in new products and new markets.

23. For example, at the November 17, 2016 Phocuswright Conference for travel industry leaders, Oliver Heckmann ("Heckmann"), Google's Vice President of Travel, assured investors that Google was uniquely well-positioned in the travel sector precisely because of its ability to leverage its strategy of data movement across its various services while keeping the trust of its customers by "giving the user full control and ownership of [her or his] data." Heckmann stated that maintaining users' trust is essential to making users "more willing to have that data . . . used" across platforms, for example when allowing Google to analyze an air travel receipt from its user's Google Mail

(Gmail) account inbox and automatically importing those flight details into the user's Google Calendar account:

> **Elizabeth Harz –Adara – President, Media & CMO**
>
> So, as a consumer, I certainly see how my United flight data goes from Google Mail to my calendar and I would just love to get Google's perspective on data strategy – the collection, ownership, privacy. Many of those questions come up when you experience that kind of data movement.
>
> **Oliver Heckmann – Google Inc – VP, Travel**
>
> Yes, privacy is actually a topic that's important for us and as you know or might not know, there is something that's called the Google Dashboard that is creating transparency over the data that we have and the different services that Google has to the user, and it's using pretty clear language and it's giving the user full control and ownership of the data. ***And we feel that that's an important thing to do and as the user is in control and ownership of the data, he is more willing to have that data be used for us to create some delightful experiences***. If the user is not opting out of those services, what we can do is we can, from the email receipt in his inbox, for example, that's a new version of Gmail, we can show you your travel information more structured so you don't have to – you are landing in Paris; you are on roaming; you need to find your hotel and then the faster we can actually get you to that information, the more delightful and the less stressful your travel experience is going to be.

24. At the February 14, 2017 Goldman Sachs Technology Conference, Diane Greene ("Greene"), Board Member of Alphabet and Senior Vice President of Google Cloud, touted Google's superior data security as enhancing its prospects in the cloud computing and financial-technology ("FinTech") industries:

> ***Security, Google's had security pretty much from day one because of the necessity to keep people's data private. I think we arguably have the most secure cloud on the planet, but we've also really hunkered down over the last 16 months to get all the compliance and regulatory so our large customers can prove to their customers and to their regulators that they are indeed secure. I mean security matters from the board on down to the individual user, IT worker at a company***, it's so important and if you look at things like G Suite, our productivity suite built in the cloud completely in the secure cloud and you map that to the diskless Chromebook, you actually can run a workforce with an amazing level of security.
>
> Google, when I say it's a privilege to be at Google, Google organizing the world's information, we've been inventing how to manage data for 16 years now, how to really quickly go through massive amounts of data.
>
> * * *
>
> **Unidentified Audience Member**
>
> Could you talk a little more in detail about why FinTech has you so excited?

Diane Greene - Alphabet Inc - SVP, Google Cloud

> Oh, why does FinTech have me so excited? Well, it's a huge segment of the IT market, and we are like, there is a lot of data in FinTech, there's a lot of things just ripe for machine learning. ***And security is paramount there, it just seems so suited to our strengths and that's what we are seeing***. And also we're working with all the banks on projects and we can see how much there is to do. FinTech is, I mean, since my days at Sybase I've been working with FinTech, it's a big industry and there's a lot to do there.

25. At the September 7, 2017 Citi Global Technology Conference, Greene continued to highlight Google's focus on security and on being a "pioneer" in keeping "customers' data private." Greene began her speech with a nod to security, stating that it "is the most pervasive problem" facing any company because a "data breach is so expensive":

> We've got – we run approximately 1/3 of the world's Internet traffic. And in over the last 3 years, we spent $29 billion in CapEx, continuing to build out, keeping up with the enormous growth we're seeing.
>
> ***So I want to start with security because I strongly believe that is the most pervasive problem every company has. The data breach is so expensive, I think, our health record is $400 a health record if you get breached. And so Google, with all the information we have and the need to keep our customers' data private, has had to be a pioneer, and we feel pretty good about where we are in security, not that we aren't vigilant with our 800-plus dedicated security engineers every day. But I would say, all of Google's some-30,000-plus engineers are kind of security engineers, and we've built security into every layer of the system***. From proprietary purpose-built chips like Titan that say that the hardware hasn't been tampered with and you're running a binary you think you are to every layer of the stack on up to the software that detects a phishing attack and then in your mail and then says if someone tries – if you gave the password and someone tries to use it, it says, "Are you sure this person should have your password or do you want to change your password?"
>
> And we've also developed perimeter-less security, because if you just have a firewall protecting everything, if someone gets inside, you're kind of in trouble. And so we can look at what you're doing, where you're coming from and what call you're making, so that many, many of our services, Google services are just out there on the open Internet, because we can protect them much better than we could with a firewall.
>
> And you take something like a Chromebook with its – the Chrome OS tiny attack surface updated in the Cloud constantly. You don't get a Ransomware attack then or something like Heartbleed a few years ago. Google had that patched before it was publicly announced.

26. Although he was not one of Google's founders, Google's CEO, Pichai, embraced and perpetuated this mantra, as he demonstrated in this January 24, 2018 statement:

> 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. So we work hard to earn the trust every day. You know one of the biggest concerns of data as you saw through last year is security of data. So for example, when you use G-mail we work hard to make sure we keep your e-mail safe from all kinds of attacks that's possible. And I think that's the framework by which we operate. But I think that I always think data belongs to the user and as companies we are only stewards of it.

27. Consistent with Pichai's statement, for years, the Companies acknowledged the risks of their intertwined dependence on technology and trust, including in the "Risk Factors" section of Alphabet's 2017 Annual Report on Form 10-K ("2017 10-K"), which assured investors that "we expect to continue to expend significant resources to maintain state-of-the-art security protections that shield against theft and security breaches," but warned of the following risks, among others:

(a) "***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.)

(b) "***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***." (Emphasis in original.)

(c) "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."

(d) "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."

(e) "Our security measures may also be breached due to employee error, malfeasance, system errors or vulnerabilities, including vulnerabilities or our vendors, suppliers, their products, or otherwise."

(f) "Such breach or unauthorized access, increased government surveillance, or attempts by outside parties to fraudulently induce employees, users, or customers to disclose sensitive information in order to gain access to our data or our users' or customers' data could result in significant legal and financial exposure, damage to our reputation, and a loss of confidence in the security of our products and services that could potentially have an adverse effect on our business."

28. Beyond these risk warnings, Alphabet informed investors of the following realized risk: "We experience cyber attacks of varying degrees on a regular basis."

29. Echoing the importance of data security to the Companies at the February 13, 2018 Goldman Sachs Technology & Internet Conference, Greene stated that "security, first and foremost"

was Google's competitive advantage versus other cloud providers because of Google's sophistication at security matters and its history of discovering major vulnerabilities:

> **Heather Anne Bellini - Goldman Sachs Group Inc., Research Division - MD & Analyst**
>
> Right. So if you were sitting down with a CIO and they asked you, "What are your top 3 competitive advantages versus the other cloud providers?" What would be those 3 things?
>
> **Diane B. Greene - Alphabet Inc. – Director**
>
> Yes. Well, I'd say it's security, first and foremost, simply because I don't think anyone can afford not to be as secure as possible. And we've – not only do we discover these major problems, like the [Speck Hammer] or the Heartbleed and what have you, but we also – like with 1.4 billion Gmail accounts, we see everything. We can tell you, "Hey, someone – you just gave away your password. Are you sure you wanted to do it because we're not going to let them log in if you want to change your password?" And so we're even that sophisticated now. And so – and then what we're doing increasingly with GCP. So I say security and just because it's just so important. And then it's data analytics and machine learning and AI and . . . .

30. Alphabet's Chief Financial Officer ("CFO"), Ruth Porat ("Porat"), told analysts at the February 26, 2018 Morgan Stanley Technology, Media & Telecom Conference that because of "all that's going on with security" and the fact that security is "clearly what we've built Google on," the continued monetization of Google's advertised focus on privacy and security would remain a key strategic priority of the Companies:

> And then in terms of the key strategic priorities, they are the ones that we've been talking about for quite some time, and they really play to our strengths. One of the most important is all that's going on with security. We believe we're a leader in security. It's clearly what we've built Google on. And we're continuing to raise the bar there, just the extraordinary engineers we have. We're now taking this to the next level. And one of the things that we talked about is through 2017, with the development of a proprietary security chip that really enables us to take identification and authentication into hardware. So it's not just about software, it's also about hardware.

The Google+ Social Media Platform –
A "Social Layer" Across All Google Services

31. Google launched the Google+ platform in June 2011 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. As explained in March 2012 by then-Senior Vice President of Social, Vic Gundotra, "'[a]t its simplest level, Google+ is a social layer

across all of Google's services.'" Pichai similarly admitted to *Forbes* in February 2015 that "'Google+ has always meant two things'" for the company:

> "There's the stream in the product that you see." But Google+ also provided a way for the company to ensure users were signed in to its services with "a common identity across our products," he said. "The second part was in many ways even more important than the first part. That part has worked really well for us."

32. Because the company initially viewed Google+ as "'the next version of Google,'" defendants integrated Google+ into every other Google service, with former CEO Page even tying employee bonuses to the success of the Google+ platform. For instance, in late 2011. Google changed the sign up process for Gmail, whereby creating a Google or Gmail account would automatically create a Google+ profile. Google also released the Hangouts messaging app in 2011, which required a Google+ account to use. In 2013, Google similarly announced that users would be required to log in to a Google+ account in order to leave comments on YouTube. Even Google Search – the cornerstone of Google's business and one of the most frequented destinations on the Internet – was integrated into the Google+ platform with the "Search plus Your World" feature in 2012.

In Early 2018, Google Faced Unprecedented Public and Regulatory Scrutiny for Its Data Collection and Privacy Practices

33. By the spring of 2018, the trustworthiness of technology and those who control it were under unprecedented scrutiny. A pivotal moment was on March 17, 2018, when *The Observer* and the *New York Times* published reports alleging that research firm Cambridge Analytica improperly harvested data from Facebook users' profiles. The immediate effects of these allegations were devastating to Facebook and its investors. For example, in the week following the publication of these reports, Facebook's common stock suffered its third worst week in the company's history, declining more than 13% and losing approximately $75 billion of market capitalization. Almost immediately, 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:

(a) On March 26, 2018, the *Washington Post* published an article titled "Congress wants to drag Google and Twitter into Facebook's privacy crisis," which reported that:

> The Senate Judiciary Committee's chairman, Republican Sen. Chuck Grassley (Iowa), on Monday scheduled an April 10 hearing on the "future of data privacy and social media" – and the panel said it would explore potential new "rules of the road" for those companies.
>
> * * *
>
> [T]he Senate Judiciary Committee's hearing spells the first time that congressional lawmakers have expanded their scrutiny to include Zuckerberg's peers, Google CEO Sundar Pichai and Twitter CEO Jack Dorsey. The result could be a hearing that exposes both of those tech giants – whose data is not known to have been taken by Cambridge Analytica – to uncomfortable questions about the extent to which they profit from their users' most personal data, too.

(b) As later explained by Senator Charles Grassley, Google and Pichai "declined to come before Congress and the American people" for the April 2018 hearings, "asserting that the problems surrounding Facebook and Cambridge Analytica did not involve Google."

(c) On April 10, 2018, Senator Grassley sent a letter to Pichai 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," along with 14 questions to fully "understand how Google manages and monitors user privacy for the significant amounts of data which it collects."

(d) An April 13, 2018 article in *The New York Times* titled "Facebook Takes the Punches While Rest of Silicon Valley Ducks" detailed the heightened concern at Google of increased regulatory scrutiny following the Facebook/Cambridge Analytica hearings:

> Mr. Zuckerberg was prepared to say that his company accounts for just a slice of the $650 billion advertising market and that it has plenty of competitors. Google, for example, has an online advertising business more than twice the size of Facebook's. And Google also collects vast amounts of information about the people who use its online services.
>
> * * *
>
> "Outside of Facebook, there is probably no company paying more attention" than Google, said Jason Kint, a frequent critic of Google and Facebook and chief executive of Digital Content Next, a trade group that represents entertainment and news organizations, including The New York Times. "They're absolutely ducking for cover while the heat is on Facebook. They don't want to try to trip any alarms."
>
> * * *

> Over two days of hearings, Google was referenced 11 times by lawmakers. Twitter was mentioned 10 times and Amazon once. Apple was mentioned three times, mostly in passing.
>
> Google employees said they had not received explicit orders from management to keep a low profile because most already understood the risk. One employee, who spoke on the condition of anonymity because workers were not allowed to speak publicly on the issue, said there was an understanding inside Google that the company was the obvious next target.
>
> In a statement, Aaron Stein, a Google spokesman, said the company was "completely focused on protecting our users' data" and "will take action" if it found evidence of "deceptive behavior or misuse of personal data."

34. In addition to the heightened regulatory scrutiny on data collection and privacy issues in the United States, the spring of 2018 also saw the public's attention focused on the implementation of the GDPR, which went into effect in May 2018. The GDPR is a new European Union framework that reformed data privacy protections in all member-states and has implications for businesses and individuals across Europe and beyond. Under the terms of the GDPR, disclosure of data breaches is obligatory: "In the case of a personal data breach, the controller shall ***without undue delay*** and, where feasible, ***not later than 72 hours*** after having become aware of it, ***notify*** the personal data breach to the supervisory authority . . . ." Failure to follow the GDPR's guidelines can result in fines "[u]p to €10 million, or 2% of the worldwide annual revenue of the prior financial year, whichever is higher."

35. The public focus on the GDPR was not lost on Google. Starting in May of 2017, Google began issuing several blogs on its official website, The Keyword, detailing the steps it was taking to fully comply with the GDPR. In an August 8, 2017 blog post, William Malcolm ("Malcolm"), the Director of Privacy Legal EMEA, stressed that Google "is committed to complying with the GDPR across all of [its] services" and that its "aim is always to keep data private and safe." Less than a year later, Malcom again reaffirmed Google's dedication to data privacy protections emphasizing that it had been working on GDPR compliance efforts for over 18 months, that "Google has built a strong global privacy compliance program," and that its "ambition is to have the highest possible standards [for] data security and privacy."

36. Google was even more focused on data security issues because, in addition to the many universal issues, Google was operating under a Consent Order with the Federal Trade

Commission ("FTC"). The order resulted from a complaint filed in 2011 against Google's social network Google Buzz, the predecessor to Google+. The FTC concluded that Google violated its privacy promises and misrepresented to users of its email services how their information could be used, in some instances private information was shared publicly by default. In the end, the Consent Order, the first decision of its kind, required Google to do the following (among other obligations):

(a) establish and implement a comprehensive privacy program;

(b) maintain privacy controls that are appropriate to its size and complexity, the nature and scope of its activities, and the sensitivity of covered information;

(c) maintain privacy controls that meet or exceed the protections required by the Consent Order; and

(d) demonstrate that its privacy controls are operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and have so operated throughout each two-year reporting period through year 2031.

As Public Pressure Mounted, Defendants Learned of Major Data-Security Problems

37. In March 2018, Google learned that it had realized the risks it had been warning about for years. Its data privacy protections were not as trustworthy as it had previously believed. Specifically, it learned of a software glitch in its Google+ social networking site that gave hundreds of third-party developers potential access to the private user profile data for Google+ users (the "Three-Year Bug"). This private information included birth dates, photos, occupations, relationship status, email addresses, and home addresses. Worse, 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. Without sufficient record keeping, Google could only estimate that it exposed to third-parties the personal private data of hundreds of thousands of users, but this estimate was based on projections from less than 2% of the Three-Year Bug's lifespan, and Google had no way of determining how many third-parties had misused its users' personal private data. Google did not call or otherwise contact a single third-party developer to investigate the fallout from the bug.

38. A group of over 100 of Google's best and brightest engineers, product managers, and lawyers were responsible for uncovering the Three-Year Bug and fixing it, but they could not

confirm the damage from it or determine the number of other bugs. In or about early 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 (the Three-Year Bug and these additional vulnerabilities are collectively referred to as the "Privacy Bug" and the memo discussing them, the "Privacy Bug Memo"). The Privacy Bug Memo warned that disclosure of the Privacy Bug 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 Privacy Bug Memo also warned that disclosure "'almost guarantees Sundar [Pichai] will testify before Congress.'"

39. Defendant Pichai and other senior Google executives received and read the Privacy Bug Memo in or about early April 2018.

Not Doing the Right Thing – Defendants Hid the Truth

40. Despite being fully briefed on the Privacy Bug, Pichai approved a plan to hide the Privacy Bug from all users and everyone else outside of the Companies. One of the reasons Pichai approved this concealment plan was because he wanted to avoid any additional regulatory scrutiny, including having to testify before Congress.

41. This 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. At that time (spring 2018), Google+ had 395 million monthly active users. Putting this decision into context, at that same time, Twitter and Snapchat had 330 and 301 million monthly active users, respectively, and corresponding market capitalizations of over $20 billion each.

42. Worse, defendants chose to continue making statements concerning data security, related risks, and their trustworthiness, but these coordinated statements maintained the same assurances and warnings as before the Privacy Bug's discovery, while concealing the Privacy Bug itself. In other words, they decided to do the wrong thing by warning investors of risks that had

already been realized, and concealing the new risks they had discovered and created by concealing these risks.

43. On April 23, 2018, consistent with his understanding with Pichai, Page signed Alphabet's SEC Quarterly Report on Form 10-Q for the period ending March 31, 2018 (the "1Q 2018 10-Q"), which merely incorporated the identical risk disclosures from its 2017 10-K, without any mention of the Privacy Bug that defendants discovered after Alphabet had filed the 2017 10-K:

> 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.

44. On April 23, 2018, Alphabet held an earnings call to discuss its 1Q 2018 results. The call began with Ellen West ("West"), Alphabet's Head of Investor Relations, referring investors to the 2017 10-K risk disclosures:

> Thank you. Good afternoon, everyone, and welcome to Alphabet's First Quarter 2018 earnings conference call. With us today are Ruth Porat and Sundar Pichai. Now I'll quickly cover the safe harbor.
>
> Some of the statements that we make today may be considered forward looking, including statements regarding our future investments, our long-term growth and innovation, the expected performance of our businesses and our expected level of capital expenditures. These statements involve a number of risks and uncertainties that could cause actual results to differ materially. For more information, please refer to the risk factors discussed in our Form 10-K for 2017 filed with the SEC.

45. Without mentioning a word about the Privacy Bug, Pichai assured the public and investors that Google was prepared for the forthcoming GDPR, stressing that the company had "started working on GDPR compliance over 18 months ago and have been very, very engaged on it." Beyond mere GDPR compliance, Pichai emphasized that Google has a "very robust and strong privacy program."

46. On April 25, 2018, Google's Vice President of Public Policy and Government Affairs, Susan Molinari ("Molinari"), responded to Senator Grassley's April 10, 2018 letter on behalf of Pichai. Making no mention of the recently-discovered Privacy Bug, Molinari stated that "Google has a longstanding commitment to ensuring both that our users share their data only with

developers they can trust, and that they understand how developers will use that data," and that the company was "committed to protecting our users' data and prohibit developers from requesting access to information they do not need."

47. On April 27, 2018, Alphabet filed a Proxy Statement with the SEC pursuant to §14(a) of the Exchange Act. The voting matters for the June 6, 2018 Annual Meeting included management's proposed election of 11 directors, including Page and Pichai. Among the stockholder proposals was a proposal regarding a report on content governance, which requested that Alphabet "issue a report to shareholders at reasonable cost, omitting proprietary or legally privileged information, reviewing the efficacy of its enforcement of Google's terms of service related to content policies and assessing the risks posed by content management controversies, including election interference, to the company's finances, operations, and reputation." Alphabet opposed that stating in relevant part that: "***We believe that we have a responsibility to combat the misuse of our platforms and enforce our content policies. And we understand our continuing responsibility to update our users and stockholders on those efforts. We will continue to remain vigilant in this regard and plan to make regular public disclosures about our efforts, our results, and our future plans***." Alphabet also opposed a proposal requesting that it detail its policies and procedures concerning its lobbying efforts. Alphabet's statement in opposition stated, in relevant part: "***We are committed to transparency in all areas of our business***, including our public policy activities and lobbying expenditures. ***Google has long been a champion of disclosure and transparency***."

48. On June 6, 2018, during Alphabet's Annual Shareholders Meeting, defendant Walker, reassured shareholders that it had "long been one of the leading companies when it comes to privacy and security of user data" and that "we are in great pains to make sure that people have great control and notice over their data." Walker made this statement while he and all others at the Companies continued to conceal the Privacy Bug throughout June 2018.

49. On July 23, 2018, consistent with his agreement with Pichai, Page signed Alphabet's SEC Quarterly Report on Form 10-Q for the period ending June 30, 2018 (the "2Q 2018 10-Q"), which merely incorporated the identical risk disclosures from its 2017 10-K, without any mention of the Privacy Bug that defendants discovered after Alphabet had filed the 2017 10-K:

> 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.

50. That same day, at the outset of Alphabet's 2Q 2018 earnings call, West again referred investors to the 2017 10-K risk factors with a statement substantively identical to ¶44, and Pichai again highlighted that Google was "always . . . focused on user privacy" and security. West and Pichai made these statements while Pichai and all others at the Companies continued to conceal the Privacy Bug throughout July 2018.

51. The custom and practice of a newspaper of the size and sophistication of the *WSJ* would have meant that, by September, the *WSJ* would have directly or indirectly informed the Companies that it was investigating the Privacy Bug and their concealment of it. Realizing that the *WSJ* could soon expose the Privacy Bug and their concealment of it, Page and Pichai decided that neither they nor any other representative from the Companies would accept an invitation to testify before a Senate Intelligence Committee in September 2018. Representatives from the other two invitees, Facebook and Twitter, appeared and testified – beside an empty chair for Google.

52. On September 26, 2018, defendant Enright, Google's Chief Privacy Officer, provided written testimony to the Senate Committee on Commerce, Science, and Transportation, which included the following statements:

- "The foundation of our business is the trust of people that use our services."
- "With advertising, as with all our products, users trust us to keep their personal information confidential and under their control."
- "[A] healthy data ecosystem requires people feel comfortable that all entities who use personal information will be held accountable for protecting it."

53. Enright echoed these statements in an official Google blog published just two days earlier. In the blog, Enright highlighted that "users have long entrusted us to be responsible with their data and we take that trust and responsibility very seriously." In addition, Enright reaffirmed that "[p]eople deserve to feel comfortable that all entities that use personal information will be held

accountable for protecting it" and that their business model relies on personal data and their "work to comply with evolving data protection laws around the world."

54. Enright made these statements while he and the other defendants continued to conceal the Privacy Bug throughout September 2018.

55. The statements referenced in ¶¶43-53 above omitted to state material facts necessary in order to make them not misleading. Specifically, these statements omitted that in March 2018, Google learned that it had realized the risks it had been warning about for years; its data privacy protections were not as trustworthy as it had previously represented and believed; a bug in its Google+ social networking site had given hundreds of third-party developers potential access to the private user profile data for millions of Google+ users (this private information included birth dates, photos, occupations, relationship status, email addresses, and home addresses); its security controls were so inadequate that it failed to detect this bug for approximately 150 weeks, yet it could only identify two weeks' worth of users whose private profile information had been exposed; due to insufficient record keeping, Google could only estimate that it exposed to third-parties the personal private data of hundreds of thousands of users, and it had no way of determining how many third-parties had misused its users' personal private data; that it had identified systemic security deficiencies in its Google+ service that rendered additional bugs and data exposures virtually inevitable; and that key officers and directors, including Alphabet's CEO, Google's CEO, Google's General Counsel, and Google's Chief Privacy Officer, had decided to conceal all of this information from everyone outside the Companies. In short, these statements omitted facts that revealed that neither the Companies' technology nor its management was as trustworthy as they had led the public, including investors, to believe. Defendants also concealed the inevitability of all the foregoing risks materializing.

56. The SEC requires that a registrant's Form 10-Q set forth any material changes from risk factors as previously disclosed in the registrant's last Form 10-K. The 1Q 2018 10-Q and 2Q 2018 10-Q incorporated by reference the 2017 10-K risk disclosures and did not disclose any new risks. Accordingly, the 1Q 2018 10-Q and 2Q 2018 10-Q were materially misleading because they failed to disclose another category of risk: the risk that the concealment itself would be exposed,

which would trigger a host of immediate negative consequences, including reputational harm, diminished trust, intense regulatory scrutiny, higher expenses (including increased legal, PR, lobbying, and investigative expenses), just to name a few. Indeed, defendants knew that they could not keep the Privacy Bug concealed forever – too many people were aware of it, it was incendiary, and it was the final straw for shutting down Google+ – so they knew that it and their concealment of it would eventually be exposed, but they made the decision to buy time. Defendants calculated that the detrimental effects would be even worse if, at the time Facebook was getting pummeled in Congress, in the public, and in the financial markets, Google announced that it simply had no confidence in its data protections for hundreds of millions of users.

57. On October 8, 2018, the *WSJ* revealed the Three-Year Bug and the Companies' concealment of it.

58. In a blog posted contemporaneously to the publication of the *WSJ* article, Google admitted to the exposure of hundreds of thousands of users' private data and 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]." Google's statements on the Three-Year Bug did not dispute Pichai's reported receipt of the Privacy Bug Memo in or around early April 2018 or his involvement in the decision to conceal the Privacy Bug from users, regulators, and everyone else outside of the Companies. In the months following the *WSJ* article's publication, and in multiple statements relating to the Privacy Bug, none of defendants disputed a single fact from the article.

59. On October 10, 2018, three Democratic Senators wrote to the FTC Chairman, demanding an investigation into the Three-Year Bug, including Google's concealment of it. The letter highlighted the deceptiveness of Google's response to the *WSJ*'s article, including the following:

> 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.

60. Google "'found no evidence'" because it barely looked – reviewing data from less than 2% of the Three-Year Bug's lifespan, and there is "no evidence" that Google so much as called or contacted a single third-party developer. The Democratic Senators went on to explain how the revelation of Google's concealment of the Three-Year Bug revealed a corporate culture that bore no resemblance to one that "do[esn't] be evil" and "do[es] the right thing": "The awareness and approval by Google management to not disclose represents a culture of concealment and opacity set from the top of the company."

61. Google's scheme did manage to unite the country's two political parties. On October 11, 2018, three Republican Senators wrote a letter to Pichai that read, in part, "[a]t the same time that Facebook was learning the important lesson that tech firms must be forthright with the public about privacy issues, Google apparently elected to withhold information about a relevant vulnerability for fear of public scrutiny." The Republican Senators also confirmed the misleading nature of Enright's September 26, 2018 statements (*see* above): "We are especially disappointed given that Google's chief privacy officer testified before the Senate Commerce Committee on the issue of privacy on September 26, 2018 – just two weeks ago – and did not take the opportunity to provide information regarding this very relevant issue to the Committee."

62. On October 11, 2018, Senator Grassley wrote to Pichai regarding the "troubling reports" detailed in the *WSJ* article, and condemned Google's evasive responses to congressional inquiry earlier that year:

> Given your and Google's unwillingness to participate [in the April 10, 2018 Facebook/Cambridge Analytica hearing], I sent you a letter seeking information on Google's current data privacy policies, specifically as they relate to Google's third party developer APIs. Your responses to my questions highlighted Google's application verification process, the continuous monitoring of applications through machine learning, and the use of manual audits, all to ensure robust protection of user data.
>
> Despite your 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.

63. The *WSJ* article, Google's blog post, and the letters described in the preceding paragraphs contained enough information for investors to piece together that the Three-Year Bug was a symptom of the disease comprising the Privacy Bug.

64. As defendants had anticipated, just weeks after the *WSJ* revelations, defendants disclosed another Google+ bug had exposed user data from 52.5 million accounts. Defendants admitted that "users were impacted." Unlike the Three-Year Bug, which defendants deliberately concealed from users and the investing public, defendants disclosed this new bug in a December 10, 2018 blog post and began notifying the impacted users. Defendants also announced they were accelerating the shuttering of the consumer Google+ platform to April 2019 rather than August 2019, a further confirmation of Google's inability to protect users' personal and private information. Defendants' disclosure came just hours before Pichai was set to testify before the House Judiciary Committee.

65. Throughout the years, as discussed above, defendants repeatedly acknowledged that 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. 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 of its users in order to sell targeted ads." Fully aware of consumers' expectations that their private information will remain private, defendants repeatedly promised they would not only keep the information private but that they would notify users if their information was impacted.

66. The revelation that millions of users' data had been potentially exposed and that rather than notify users of the exposure, defendants chose to cover it up was a massive breach of consumers' trust, as well as a realization that Google had failed to develop adequate systems and controls to maintain the integrity of its users' private data. As one commentator put it: "Google's business model is based on trust, and hiding a potentially dangerous breach for six months is not the way to keep it." Another observed that through its "'digital coverup . . . Google has demonstrated that it cannot be relied on to protect privacy.'" Thus, the disclosure of the Privacy Bug and its

impact on users damaged Google's reputation and, thus, value. Indeed, the *WSJ*'s investigation, based on internal documents, revealed that in choosing to cover up the Privacy Bug, defendants sought to avoid regulatory scrutiny and reputational damage. Defendants were right to be concerned. Upon disclosure of the Privacy Bug and subsequent cover up, industry commentators noted increased regulatory scrutiny and that regulatory investigations were sure to come.

67. A *CNBC* article titled "Google learned the hard way it's better to be transparent about privacy bugs than cover them up" noted "[c]onsumers and regulators have shown they will judge companies far more harshly for covering up data security issues than for openly discussing them." That same article drew similarities between Google's cover-up of the Three-Year Bug and Uber's revelation of a data breach it had tried to cover up, noting the incident "was relatively minor except for the cover-up." As of October 2018, Uber has paid nearly $150 million in settlements related to the revelation and is subject to increased monitoring by the FTC for 20 years.

68. As predicted by *CNBC*, the very regulatory, legal, and reputational risks that the Companies warned about while defendants covered up the Privacy Bug materialized. For one thing, German regulators in Hamburg, where Google has its German office, have initiated an investigation into Google's handling of the Privacy Bug. In addition, regulators in Ireland indicated they "'will be seeking information on these issues from Google,'" referring to the Privacy Bug and Google's response to it. U.S. Senator Richard Blumenthal called for a full FTC investigation into the Privacy Bug. Several private lawsuits on behalf of consumers and shareholders have been filed against Google as a result of the Privacy Bug.

69. On November 2, 2018, Google announced that Molinari, the head of Google's Americas policy who drafted Pichai's response to Senator Grassley's April 10, 2018 letter, was stepping down from her role.

70. With the Companies' scheme exposed, Pichai testified before Congress on December 11, 2018. The ranking member's opening remarks specifically highlighted the Privacy Bug, including Google's concealment of it. As featured below, in neither his prepared opening remarks nor during any portion of his testimony did Pichai deny his awareness of the Privacy Bug for months

before disclosure, nor his involvement in the decision to conceal the Privacy Bug until the *WSJ* exposed it:

(a) "We take privacy seriously. The bugs you mentioned are bugs we found them by either doing an audit . . . .";

(b) "Building software inevitably has bugs associated as part of the process. We actually undertake a lot of efforts to find bugs, so we find it, [root it] out, and fix it, and that is how we constantly make our systems better."

(c) "The biggest area we see for our users is around security, that their account gets hacked or something. That is why we work hard."

71. Pichai battled questions about the data breach from the House Committee while also repeatedly emphasizing the Companies' aged mantra of trustworthiness through data protection:

(a) "Protecting the privacy and security of our users has long been an essential part of our mission."

(b) "We have invested an enormous amount of work over the years to bring choice, transparency, and control to our users. These values are built into every product we make."

(c) "Today, for any service we provide our users, we go to great lengths to protect their privacy and we give them transparency, choice, and control."

(d) "I am of the opinion we are better off with more of an overarching data production framework."

72. On February 5, 2019, Alphabet filed with the SEC its Form 10-K Annual Report for 2018, its first annual report since the revelation of the Privacy Bug, including the Companies' concealment of it. Unlike the 2017 "Risk Factors" that Alphabet had incorporated into its 1Q 2018 10-Q and its 2Q 2018 10-Q, the 2018 "Risk Factors" finally acknowledged that "***[b]ugs or defects in our products and services have occurred and may occur in the future***." (Emphasis in original.)

ADDITIONAL SCIENTER ALLEGATIONS

73. The facts detailed in ¶¶38-40, establish that Pichai and senior Google executives had actual knowledge of the Privacy Bug by early April 2018. Specifically, in or about early April 2018, senior Google executives, including Pichai, were personally notified that a bug in its Google+ social

networking site gave hundreds of third-party developers potential access to the private user profile data for Google+ users (this private information included birth dates, photos, occupations, relationship status, email addresses, and home addresses) who never intended to publicly share this private data. Pichai and senior Google executives received this information in the Privacy Bug Memo, which was prepared by Google's legal and policy staff. Given that Google failed to detect the bug for approximately 150 weeks but only kept two-weeks' worth of activity logs necessary to determine which users were affected and what types of data may potentially have been improperly collected, the Privacy Bug Memo stated that Google had no way of determining how many third-parties had misused the personal private data of a likewise unknown number of users. Likewise, the Privacy Bug Memo revealed systemic security deficiencies in Google's Google+ service that rendered additional bugs and data exposures virtually inevitable. Google admitted in its October 8, 2018 blog post that it discovered and remediated the lone Three-Year Bug in March 2018, but that was just the tip of the iceberg.

74. The facts detailed above, when viewed collectively and holistically with the other allegations in this Complaint, establish a strong inference that each of the defendants knew or recklessly disregarded that each of the statements set forth in ¶¶43-53 would be, and were, misleading to investors at the time they were made. This inference is far stronger than the alternative: that 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, as well as Google's Chief Privacy Officer and General Counsel – who both had primary responsibility for data-security issues at Google.

75. Defendants' scienter can also be inferred from the ***cover-up*** of the Privacy Bug. Specifically, the Companies' employees would not uniformly conceal the Privacy Bug without a directive to do so from the Individual Defendants, who were the individuals most responsible for responding to data-security issues. The Individual Defendants would have to have been informed and exercised their decision-making authority to conceal the Privacy Bug while persisting with the same pre-discovery assurances and risk warnings when that decision was largely driven by the desire to avoid regulatory scrutiny, Pichai's Congressional testimony, and reputational damage. Indeed, the

Privacy Bug Memo expressly warned that disclosure of the Privacy Bug would likely trigger "'immediate regulatory interest'" and "'almost guarantees Sundar [Pichai] will testify before Congress.'" Accordingly, defendants covered up the Privacy Bug until the publication of the *WSJ* article.

76. Defendants' scienter can likewise be inferred from their immediate announcement of significant and extensive ***remedial measures*** on the day that the *WSJ* article was released, including the shuddering of Google+ – the world's fifth largest social media network. Also on October 8, 2018, Google announced a sweeping set of data privacy measures as part of its response to the events described in the *WSJ* article, including: (1) launching more granular Google Account permissions to give consumers "more fine-grained control over what account data they choose to share with each app"; (2) limiting the applications that may seek permission to access users' Gmail data; and (3) limiting the ability of applications to ask for permission to access information in users' telephones. In addition, Google pledged that "[i]n the coming months, we'll roll out additional controls and update policies across more of our APIs." These are the types of decisions that the Companies consider and study for months, not minutes, before making them.

77. Defendants' scienter may be further inferred from other facts alleged herein, including that:

(a) defendants had been repeatedly warned of and were aware of the significant, and potentially existential, risks to the Companies arising from the public discovering a data breach;

(b) defendants knew that providing truthful, accurate, and complete disclosures would threaten their business model, as it would expose them to regulatory scrutiny, reputational damage, and Pichai's testimony being sought by Congress;

(c) Google was subject to an FTC consent decree at the time the statements were made, providing defendants with heightened awareness of the risks of and their responsibilities with respect to violating user privacy rights;

(d) Pichai and Page's reluctance to testify before Congress at a time when Facebook was being pilloried for a data leak was a powerful incentive for defendants to approve Google's decision to cover up the Privacy Bug, as evidenced by their widely publicized refusal to

accept the United States Senate Select Committee on Intelligence's invitation to testify about election interference in September 2018, and the Privacy Bug Memo's explicit warning that disclosure "'almost guarantees Sundar [Pichai] will testify before Congress'"; and

(e) the omissions at issue concerned one of the most significant issues and severe risks that Alphabet faced.

78. The below-listed defendants held high-level positions and had access to material, adverse, non-public information concerning specific and imminent privacy risks facing Google, including the Privacy Bug and the repercussions of disclosing it:

(a) Page founded Google, was the chief operating decision maker of Alphabet and was responsible for making, and did make, key operating decisions at Google. Pichai directly reported to, and was directly accountable to, and maintained regular contact with, Page.[2] Page received weekly reports of Google's operating results.

(b) Enright was Google's Chief Privacy Officer since September 2018. Prior to that, he was the "Legal Director of Privacy" at Google since 2016. In May of 2018, Enright was named Google's DPO for the purpose of the GDPR, which requires Google to "ensure that the data protection officer is involved, properly and ***in a timely manner, in all issues which relate to the protection of personal data***." Enright's DPO responsibilities began on May 24, 2018.

(c) Walker has been Google's General Counsel since 2006. In providing written testimony to the Senate in November 2017, Walker stated that he leads Google's "legal, policy, trust and safety, and corporate philanthropy teams." In August 2018, Walker became Google's Senior Vice President for Global Affairs.

79. Because of their positions, Enright and Walker: (1) comprise or oversee Google's Privacy and Data Protection Office, the "council of top product executives who oversee key decisions relating to privacy," which deliberated on whether to notify users of the Privacy Bug at or shortly after the time it was discovered; and (2) comprise or oversee the "legal and policy staff" that prepared the Privacy Bug Memo.

[2] As Google's CEO, Pichai was responsible for making, and did make, key operating decisions at Google. As set forth above, Pichai was a direct recipient of the Privacy Bug Memo.

80. In connection with Alphabet's 1Q 2018 10-Q and 2Q 2018 10-Q, Page signed certifications pursuant to Exchange Act Rules 13a-14(a) and 15(d)-14(a), as adopted pursuant to §302 of the Sarbanes-Oxley Act of 2002. In these certifications, Page declared that he and Porat were responsible for establishing and maintaining disclosure controls (as defined in Exchange Act Rule 13a-15(e)), and that they "[d]esigned such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under [their] supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to [them] by others within those entities, particularly during the period in which this report is being prepared." Page further certified that he and Porat "[e]valuated the effectiveness of the registrant's disclosure controls and procedures and presented in this report [their] conclusions about the effectiveness of the disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation." Pursuant to the SEC's February 21, 2018, "Statement and Guidance on Public Company Cybersecurity Disclosures," Release Nos. 33-10459, 34-82746, any such certifications made pursuant to Exchange Act Rules 13a-14(a) and 15(d)-14(a) "***should take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents and for assessing and analyzing their impact***." Therefore, prior to vouching for the accuracy of the statements made in Alphabet's 1Q 2018 10-Q and 2Q 2018 10-Q, Page was obligated to familiarize himself with the adequacy and controls for identifying cybersecurity risks and incidents and for assessing their impact. Any such review would necessarily involve an analysis of the Privacy Bug, the Privacy Bug Memo, and the conscious decision to continue concealing it in the backdrop of Facebook receiving unprecedented criticism for the Cambridge Analytica data scandal.

LOSS CAUSATION/ ECONOMIC LOSS

81. As a result of defendants' scheme, Alphabet was overvalued throughout the Class Period. Put simply, the Companies' data security and management were less trustworthy than defendants had led the world to believe. Accordingly, Alphabet's securities were riskier and thus were worth less than they appeared to be worth.

82. The revelation of the facts and circumstances that defendants had misleadingly omitted exposed both defendants' scheme and the overvaluation from the scheme. One measure of that inflated value was Alphabet's stock price, which fell $11.91 on October 8, 2018, $10.75 on October 9, 2018, and $53.01 on October 10, 2018. These price drops were caused, in part, by the market processing the implications of defendants' scheme. The revelation of defendants' scheme revealed that investors had paid more for Alphabet securities than they would have paid but for the scheme.

ALPHABET SECURITIES TRADED IN AN EFFICIENT MARKET

83. The Class Period inflation in the price of Alphabet securities was eliminated when the financial conditions, business risks, and other information concealed by defendants' fraud was revealed to the market.

84. At all relevant times, the market for Alphabet securities was an efficient market for the following reasons, among others:

(a) Alphabet securities met the requirements for listing, and were listed and actively traded on the NASDAQ, a highly efficient and automated market;

(b) during the Class Period, a high weekly volume of Alphabet securities traded on the NASDAQ;

(c) as a regulated issuer, Alphabet filed periodic public reports with the SEC and NASDAQ;

(d) throughout the Class Period, over a dozen different firms and dozens of analysts covered Alphabet securities;

(e) throughout the Class Period, Alphabet was eligible to file an SEC Registration Form S-3;

(f) Alphabet regularly communicated with investors via established market communication mechanisms, including through regular disseminations of press releases on national circuits of major newswire services, the Internet, and other wide-ranging public disclosures; and

(g) unexpected material news about Alphabet was rapidly reflected in and incorporated into its stock price.

85. As a result of the foregoing, the market for Alphabet securities promptly digested current information regarding Alphabet from all publicly available sources and reflected such information in the prices of Alphabet securities. Under these circumstances, all purchasers of Alphabet securities during the Class Period suffered similar injury when the revelation of defendants' scheme removed the artificial inflation that had been part of the price they paid when they purchased Alphabet securities.

86. A class-wide presumption of reliance is appropriate in this action under the Supreme Court's holding in *Affiliated Ute Citizens of Utah v. United States*, 406 U.S. 128 (1972), because the Class's claims are grounded on defendants' material omissions. Because defendants omitted to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading, positive proof of reliance is not required. All that is necessary is that the facts omitted be material in the sense that a reasonable investor might have considered them important in making investment decisions. Given the importance of the Class Period omissions set forth above, that requirement is satisfied here.

CLASS ACTION ALLEGATIONS

87. Plaintiff brings this action as a class action pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3) on behalf of a class consisting of all those who purchased or otherwise acquired Alphabet securities between April 23, 2018 and October 7, 2018, inclusive, and who were damaged thereby (the "Class"). Excluded from the Class are defendants, the officers and directors of the Companies, members of their immediate families and legal representatives, heirs, successors, or assigns, and any entity in which defendants have or had a controlling interest.

88. The members of the Class are so numerous that joinder of all members is impracticable. Throughout the Class Period, Alphabet securities were extensively traded on the NASDAQ. As of January 31, 2019, Alphabet had 299,360,029 shares of Class A common stock outstanding, 46,535,019 shares of Class B common stock outstanding, and 349,291,348 shares of Class C capital stock outstanding. The exact number of class members can be determined only by appropriate discovery, but Plaintiff believes that there are likely thousands of class members that are geographically dispersed, if not more. Record owners and other members of the Class may be

identified from books and records maintained by Alphabet or its transfer agent. Notice can be provided to such record owners by a combination of published notice and first-class mail, using techniques and a form of notice similar to those customarily used in class actions arising under the federal securities laws.

89. Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff has retained competent counsel experienced in class action litigation under the federal securities laws to further ensure such protection and intends to prosecute this action vigorously.

90. Plaintiff's claims are typical of the claims of the other members of the Class because Plaintiff's and all the class members' damages arise from and were caused by the misleading omissions made by or chargeable to defendants. Plaintiff does not have any interests antagonistic to, or in conflict with, the Class.

91. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Since the damages suffered by individual class members may be relatively small, the expense and burden of individual litigation make it virtually impossible for the class members to seek redress for the wrongful conduct alleged. Plaintiff knows of no difficulty that will be encountered in the management of this litigation that would preclude its maintenance as a class action.

92. Common questions of law and fact exist as to all members of the Class and predominate over any questions solely affecting individual members of the Class. Among the questions of law and fact common to the Class are:

(a) whether the federal securities laws were violated by defendants' acts as alleged herein;

(b) whether defendants' publicly disseminated statements to the investing public during the Class Period omitted material facts;

(c) whether defendants failed to convey material facts;

(d) whether defendants acted knowingly or with severe recklessness in omitting material facts;

(e) whether the price of Alphabet securities was artificially inflated during the Class Period; and

(f) whether members of the Class have sustained damages, and, if so, the appropriate measure of damages.

CLAIMS FOR RELIEF

COUNT I
For Violation of §10(b) of the Exchange Act and Rule 10b-5 (Against All Defendants)

93. Plaintiff incorporates ¶¶1-92 by reference.

94. During the Class Period, defendants disseminated or approved the statements as specified above in ¶¶43-53, which they knew or recklessly disregarded, and omitted material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading.

95. Defendants violated §10(b) of the Exchange Act and SEC Rule 10b-5 in that they:

(a) employed devices, schemes, and artifices to defraud;

(b) omitted to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; or

(c) engaged in acts, practices, and a course of business that operated as a fraud or deceit upon Plaintiff and others similarly situated in connection with their purchase of Alphabet securities during the Class Period.

96. Defendants, individually and together, directly and indirectly, by the use of the means and instrumentalities of interstate commerce and/or the mails, engaged and participated in a continuous course of conduct to conceal the truth and/or adverse material information about Alphabet's business and operations as specified herein.

97. Defendants had actual knowledge of the omitted material facts set forth herein, or recklessly disregarded the omitted material facts that were available to them.

98. As a result of the dissemination of the misleading information and failure to disclose material facts, as set forth above, the market price of Alphabet securities was artificially inflated during the Class Period. In ignorance of the fact that the market price of Alphabet securities was

artificially inflated, Plaintiff and other members of the Class purchased or otherwise acquired Alphabet securities during the Class Period at artificially high prices and were damaged thereby.

99. Plaintiff and the Class paid artificially inflated prices for Alphabet securities, and suffered losses when the relevant facts were revealed. Plaintiff and the Class would not have purchased or otherwise acquired Alphabet securities at the prices they paid, or at all, if they had been aware that the market prices had been artificially and falsely inflated by these defendants' misleading statements.

100. As a direct and proximate result of these defendants' wrongful conduct, Plaintiff and other members of the Class suffered damages in connection with their Class Period transactions in Alphabet securities.

101. By reason of the foregoing, defendants named in this Count have violated §10(b) of the Exchange Act and SEC Rule 10b-5.

COUNT II
For Violation of §20(a) of the Exchange Act
(Against Defendants Alphabet, Google, Pichai, and Page)

102. Plaintiff incorporates ¶¶1-101 by reference.

103. Defendants Pichai and Page were controlling persons of Alphabet and Google within the meaning of §20(a) of the Exchange Act. By virtue of their high-level positions as officers and/or directors of the Companies, their ownership and contractual rights, participation in and awareness of the Companies' operations, and intimate knowledge of the statements filed by Alphabet with the SEC and/or disseminated to the investing public, these defendants had the power to influence and control and did influence and control, directly or indirectly, the decision-making of the Companies, including the content and dissemination of the allegedly false and misleading statements.

104. In particular, each of these defendants had direct or supervisory responsibility over the day-to-day operations of the Companies and, therefore, are presumed to have had the power to control or influence the particular transactions and business practices giving rise to the securities violations as alleged in Count I, and exercised that power.

105. Alphabet controlled Google and the Individual Defendants, and is a controlling person of those defendants within the meaning of §20(a) of the Exchange Act.

106. Google controlled all of its employees, including Pichai, Enright, and Walker, and is a controlling person of those defendants within the meaning of §20(a) of the Exchange Act.

107. As a direct and proximate result of these defendants' wrongful conduct, Plaintiff and other members of the Class suffered damages in connection with their purchases and acquisitions of Alphabet securities during the Class Period when the relevant truth was revealed.

108. By reason of the foregoing, the defendants named in this Count violated §20(a) of the Exchange Act.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for the judgment as follows:

A. Determining that this action is a proper class action, certifying Plaintiff as Class Representative under Rule 23 of the Federal Rules of Civil Procedure and designating Lead Counsel as Class Counsel;

B. Awarding compensatory damages in favor of Plaintiff and other members of the Class against all defendants, jointly and severally, for all damages sustained as a result of defendants' wrongdoing, in an amount to be proven at trial, including interest thereon;

C. Awarding Plaintiff's reasonable costs and expenses, including attorneys' fees and expert fees; and

D. Awarding such other relief as the Court may deem just and proper.

JURY DEMAND

Plaintiff demands a trial by jury.

DATED: April 26, 2019

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

CERTIFICATE OF SERVICE

I hereby certify under penalty of perjury that on April 26, 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
- **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
- **Danielle Suzanne Myers**
  dmyers@rgrdlaw.com,3045517420@filings.docketbird.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
- **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)