

1 JOHN A. YANCHUNIS (*pro hac vice*)  
2 [jyanchunis@forthepeople.com](mailto:jyanchunis@forthepeople.com)  
3 JONATHAN B. COHEN (*pro hac vice*)  
4 [jcohen@forthepeople.com](mailto:jcohen@forthepeople.com)  
5 RYAN J. MCGEE (*pro hac vice*)  
6 [rmcgee@forthepeople.com](mailto:rmcgee@forthepeople.com)  
7 **MORGAN & MORGAN**  
8 **COMPLEX LITIGATION GROUP**  
9 201 N. Franklin Street, 7th Floor  
10 Tampa, Florida 33602  
11 Telephone: (813) 223-5505  
12 Facsimile: (813) 223-5402

13 *Counsel for Plaintiffs Matt Matic and*  
14 *Zak Harris*

15 IVY T. NGO, SBN 249860  
16 [ngo@fdazar.com](mailto:ngo@fdazar.com)  
17 **FRANKLIN D. AZAR & ASSOCIATES, P.C.**  
18 14426 East Evans Avenue  
19 Aurora, Colorado 80014  
20 Telephone: (303) 757-3300  
21 Facsimile: (720) 213-5131

22 *Counsel for Plaintiffs Charles Olson and*  
23 *Eileen M. Pinkowski*

24 Clayeo C. Arnold, SBN 65070  
25 [carnold@justice4you.com](mailto:carnold@justice4you.com)  
26 Joshua H. Watson, SBN 238058  
27 [jwatson@justice4you.com](mailto:jwatson@justice4you.com)  
28 **CLAYEO C. ARNOLD**  
**A PROFESSIONAL LAW**  
**CORPORATION**  
865 Howe Avenue  
Sacramento, California 95825  
Telephone: (916) 777-7777  
Facsimile: (916) 924-1829

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

IN RE GOOGLE PLUS PROFILE  
LITIGATION

Case No. 5:18-cv-06164-EJD (VKD)  
**CONSOLIDATED CLASS ACTION  
COMPLAINT**

Judge: Hon. Edward J. Davila  
Date Filed: October 8, 2018  
Lead Counsel Hearing: March 23, 2019  
Trial Date: None set



1 Fifth Claim for Relief..... 30  
2       Invasion of Privacy ..... 30  
3 Sixth Claim for Relief..... 31  
4       Breach of Confidence ..... 31  
5 Seventh Claim for Relief ..... 32  
6       Deceit by Concealment or Omission(Cal. Civil Code §§ 1709, 1710) ..... 32  
7 Eighth Claim for Relief..... 34  
8       Breach of Contract ..... 34  
9 Ninth Claim for Relief ..... 36  
10       Breach of Implied Covenant of Good Faith and Fair Dealing(In the Alternative) ..... 36  
11 PRAYER FOR RELIEF ..... 37  
12 JURY TRIAL DEMANDED..... 38

13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

1 For their Consolidated Class Action Complaint, Plaintiffs Matt Matic, Zak Harris, Charles  
2 Olson, and Eileen M. Pinkowski (collectively “Plaintiffs”) on behalf of themselves and all others  
3 similarly situated, allege the following against Defendant Google LLC (“Google”) and Alphabet  
4 Inc. (“Alphabet”) (collectively, “Defendants”), based on personal knowledge as to Plaintiffs and  
5 Plaintiffs’ own acts and on information and belief as to all other matters based upon, *inter alia*,  
6 the investigation conducted by and through Plaintiffs’ undersigned counsel:

7 **SUMMARY OF THE CASE**

8 This case involves two related data leaks affecting millions of people who have used  
9 Defendants’ Google+ social network. The first data leak, which Defendants knew about for  
10 months before announcing it on October 8, 2018, involves the improper exposure of the personal  
11 information of up to 500,000 Google+ users (“Google+ Users” or “Users”) due to a software  
12 glitch that gave third-party application developers access to private Google+ profile data between  
13 2015 and March 2018 (the “First Data Leak”). The second data leak, as Defendants disclosed just  
14 over two months later on December 10, 2018, similarly involves the improper exposure of the  
15 personal information of Users to third-party application developers, except this time, *up to 52.5*  
16 *million Users* were affected (the “Second Data Leak”). These data leaks are collectively referred  
17 to herein as the “Google+ Data Leaks.”

18 Launched in June 2011, Google+ (or Google Plus) is a social network owned and operated  
19 by Google for consumers with Google accounts. Google+ facilitates the sharing of information,  
20 photographs, weblinks, conversations, and other shared content similar in many respects to the  
21 Facebook news feed or Twitter stream. Google+ replaced Google’s previous social network  
22 effort, Google Buzz, after the platform faced lawsuits and an action by the Federal Trade  
23 Commission (“FTC”) concerning users’ numerous privacy concerns with the platform, including  
24 alleged misrepresentations regarding Google’s privacy assurances to users.

25 As part of the sign-up process and as a consequence of interacting with the network,  
26 Google+ Users create, maintain, and update profiles containing significant amounts of Personal  
27 Information, including their names, birthdates, hometowns, addresses, locations, interests,  
28

1 relationships, email addresses, photos, and videos, amongst other information (“Personal  
2 Information”).

3 Google maintains a privacy policy that makes specific representations to its users  
4 regarding its affirmative duty to protect users’ Personal Information, specifically providing that  
5 users are in control of who has access to their Personal Information (“Privacy Policy”).

6 When a User adds a contact to his or her Google+ account, the User assigns that person  
7 to one or more “circles” in order to categorize or organize the contact. Google+ Users determine  
8 privacy settings for content they share on Google+, allowing content to be shared with the public  
9 or with only those people in their designated circles.

10 While Users’ Personal Information was supposed to be protected and shared only with  
11 their expressed permissions and limitations, Defendants allowed third-party application  
12 developers to improperly collect the Personal Information of up to 500,000 Google+ Users in the  
13 First Data Leak.

14 Instead of choosing to be transparent about the First Data Leak, Defendants explicitly  
15 chose to conceal it from the public until after the public outcry following Facebook’s widely  
16 publicized Cambridge Analytica scandal had exhausted – hoping to avoid both public and  
17 Congressional scrutiny.

18 Then, just over two months after Defendants’ announcement of the First Data Leak,  
19 Defendants announced the Second Data Leak, whereby the Personal Information of Users was,  
20 **again**, improperly exposed to third-party applications developers. But this time, **up to 52.5**  
21 **million Users** were impacted.

22 This Consolidated Class Action Complaint is filed on behalf of all persons in the United  
23 States, described more fully *infra*, whose Personal Information was compromised in the Google+  
24 Data Leaks.

25 **JURISDICTION AND VENUE**

26 This Court has jurisdiction over this action pursuant to the Class Action Fairness Act  
27 (“CAFA”), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds  
28 \$5,000,000, exclusive of interests and costs, there are more than 100 class members, and at least

1 one class member is a citizen of a state different from Defendants. The Court also has  
2 supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

3 Venue is proper under 28 U.S.C. § 1391(c) because Defendants are corporations that do  
4 business in and are subject to personal jurisdiction in this District. Venue is also proper because  
5 a substantial part of the events or omissions giving rise to the claims in this action occurred in or  
6 emanated from this District, including the decisions made by Defendants' governance and  
7 management personnel that led to the Google+ Data Leaks and the decision not to disclose the  
8 First Data Leak earlier.

9 Further, the venue provision in Google's Terms of Service governing users in the United  
10 States provides an additional reason that venue is proper in this District. That provision provides  
11 for venue in the Northern District of California for all claims arising out of Plaintiffs' relationship  
12 with Google.

13 The Terms of Service also provide that all claims that might arise between Users and  
14 Defendants would be governed by the laws of California, without regard to conflict-of-law  
15 provisions. Accordingly, the choice-of-law provision establishes that California law applies to  
16 Plaintiffs' and the other Class members' claims.

17 **PARTIES**

18 **A. Plaintiffs**

19 Plaintiff Matt Matic is a resident and citizen of California. Plaintiff Matic opened a  
20 Google+ account and has used it for many years. Plaintiff Matic also uses a Gmail account for his  
21 primary email. Through the opening and use of these accounts, Plaintiff Matic has entrusted  
22 Google with his Personal Information for all relevant time periods.

23 Plaintiff Zak Harris is a resident and citizen of Florida. Plaintiff Harris opened a Google+  
24 account and has used it since the inception of the platform. Plaintiff Harris also uses a Gmail  
25 account for email. Through the opening and use of these accounts, Plaintiff Harris has entrusted  
26 Google with his Personal Information for all relevant time periods.

27 Plaintiff Charles Olson is a resident and citizen of Colorado. Plaintiff Olson opened a  
28 Google+ account and has used it for at least four years. Plaintiff Olson also uses a Gmail account

1 for his primary email. Through the opening and use of these accounts, Plaintiff Olson has  
2 entrusted Google with his Personal Information for all relevant time periods.

3 Plaintiff Eileen M. Pinkowski is a resident and citizen of Colorado. Plaintiff Pinkowski  
4 opened a Google+ account and has used it since the inception of the platform. Plaintiff also uses  
5 a Gmail account for her primary email. Through the opening and use of these accounts, Plaintiff  
6 Pinkowski has entrusted Google with her Personal Information for all relevant time periods.

7 **B. Defendants**

8 Defendant Google LLC (“Google”), is a Delaware corporation with its principal  
9 headquarters in Mountain View, California.

10 Defendant Alphabet Inc. (“Alphabet”), is a Delaware corporation with its principal  
11 headquarters in Mountain View, California. Alphabet is a public holding company formed in a  
12 corporate reorganization by Google. Through the corporate restructuring, Defendant Google is  
13 now a direct, wholly owned subsidiary of Defendant Alphabet.<sup>1</sup>

14 At all relevant times, Defendants were and are engaged in business in San Mateo County  
15 and throughout the United States of America.

16 **FACTUAL BACKGROUND**

17 **A. Defendants Made Specific Representations to Users Regarding Defendants’  
18 Protection of Users’ Personal Information**

19 Google’s Terms of Service make it clear that Google collects information from its users.<sup>2</sup>  
20 However, at all relevant times, Google has maintained a Privacy Policy that makes specific  
21 representations to Users regarding its protection and exposure of their Personal Information.<sup>3</sup>  
22  
23  
24

---

25 <sup>1</sup> Google, *Form 8-K* filed with the U.S. Securities and Exchange Commission (“SEC”) on August 10, 2015,  
26 <https://www.sec.gov/Archives/edgar/data/1288776/000128877615000039/a20150810form8-k.htm> (last visited  
December 11, 2018).

27 <sup>2</sup> Google, *Terms of Service* (October 25, 2017), <https://policies.google.com/terms?hl=en&gl=ZZ> (last visited  
December 11, 2018).

28 <sup>3</sup> Google, *Privacy Policy* (May 25, 2018), <https://policies.google.com/privacy>  
(last visited December 11, 2018).

1 The Google Privacy Policy specifically advises Users that: “When you use our services,  
2 you’re *trusting us* with your information.<sup>4</sup> We understand this is a *big responsibility* and work  
3 hard to protect your information and put *you* in control.” Further, Google represents that “We’ll  
4 share Personal Information outside Google *when we have your consent*.”<sup>5</sup>

5 Other specific representations to Users in the Google Privacy Policy include:

- 6 1. “You have choices regarding the information we collect and how it’s used.”<sup>6</sup>
- 7 2. “We’ll ask for your consent before using your information for a purpose that  
8 isn’t covered in this Privacy Policy.”<sup>7</sup>
- 9 3. “We’ll ask for your *explicit* consent to share any sensitive personal  
10 information.”<sup>8</sup>

9 And importantly for the Google+ Data Leaks, Google represents to its users they can  
10 “[c]ontrol whom you share information with through your account on Google+.”<sup>9</sup>

11 Despite these representations, Google’s lax approach to data security resulted in the  
12 Google+ Data Leaks affecting up to 53 million Google+ users over a period of at least 3 years.<sup>10</sup>

13 Likewise, Google has specifically disclosed that it owes a duty to Users to timely inform  
14 them of breaches involving private personal data, like the Personal Information exposed in the  
15 Google+ Data Leaks. On December 11, 2018, Google CEO Sundar Pichai was called to testify  
16 before the House Judiciary Committee on the various privacy and antitrust issues plaguing  
17 Google, including the Google+ Data Leaks.<sup>11</sup> During an exchange with Congressman Jerrold  
18 Nadler (D-NY), in a direct reference to the Google+ Data Leaks, Pichai admitted that Google  
19

---

21 <sup>4</sup> *Id.* (emphasis added).

22 <sup>5</sup> *Id.* (emphasis added).

23 <sup>6</sup> *Id.*

24 <sup>7</sup> *Id.*

25 <sup>8</sup> *Id.* (emphasis added).

26 <sup>9</sup> *Id.*

27 <sup>10</sup> The Wall Street Journal, *Google Exposed User Data, Feared Repercussions of Disclosing to Public*  
28 (October 8, 2018), available at <https://www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194> (last visited December 11, 2018); The Wall Street Journal, *Google to Accelerate Closure of Google+ Social Network After Finding New Software Bug* (December 10, 2018), available at <https://www.wsj.com/articles/google-to-accelerate-closure-of-google-social-network-1544465975> (last visited December 11, 2018).

<sup>11</sup> C-SPAN, *Google Data Collection* (December 11, 2018) available at <https://www.c-span.org/video/?455607-1/google-ceo-sundar-pichai-testifies-data-privacy-bias-concerns> (last visited December 18, 2018).



1 understood that it needed to notify impacted Users within **72 hours** of ascertaining who the Users  
2 are:

3 **Jerrold Nadler (D-NY):** According to media reports Google found evidence that – well,  
4 let me go to the other one first. Google found a bug in its Google Plus social media  
5 platform that could have potentially exposed the private data of up to half a million users  
6 without the consent to third-party developers. Google however did not disclose this bug  
7 until months later after it was revealed by a report in the Wall Street Journal. Yesterday,  
8 as I mentioned before, they found – you announced another bug. *What legal obligations  
is the company under to disclose data exposures that do not involve sensitive financial  
information, but still involve private personal data, like users’ name, age, email address  
or phone number. . . .*

9 **Sundar Pichai (CEO – Google):** Today, right now, if you’ve found a bug – you know,  
10 and you’ve ascertained – once you’ve done the investigation and you’ve ascertained the  
11 users who are eligible for notification, my understanding is **you have 72 hours**, and we  
12 both notify users as well as regulators in that timeframe.<sup>12</sup>

13 Despite Pichai’s representations of Defendants’ duty of timely disclosure, Defendants hid  
14 the First Data Leak from Users, the general public, and regulators for over **7 months**.

15 **B. Google’s Inadequate Data Security Allowed for the First Data Leak Which  
16 Was Intentionally Concealed from the Public for Over Seven Months**

17 On October 8, 2018, Defendants announced that they would be permanently shutting  
18 down the consumer functionality of Google+.<sup>13</sup> Within this announcement, Defendants disclosed  
19 that a “software glitch” had allowed outside application (i.e. “app”) vendors access to private  
20 Google+ User profile data between 2015 and March 2018.<sup>14</sup>

21 Google+ Users may allow third party applications to access their private profile data. But  
22 a “glitch” or “bug” in the Application Program Interfaces (“API”) allowed third-party applications  
23 to access the personal profile data of other Google+ Users within the authorizing User’s circles  
24

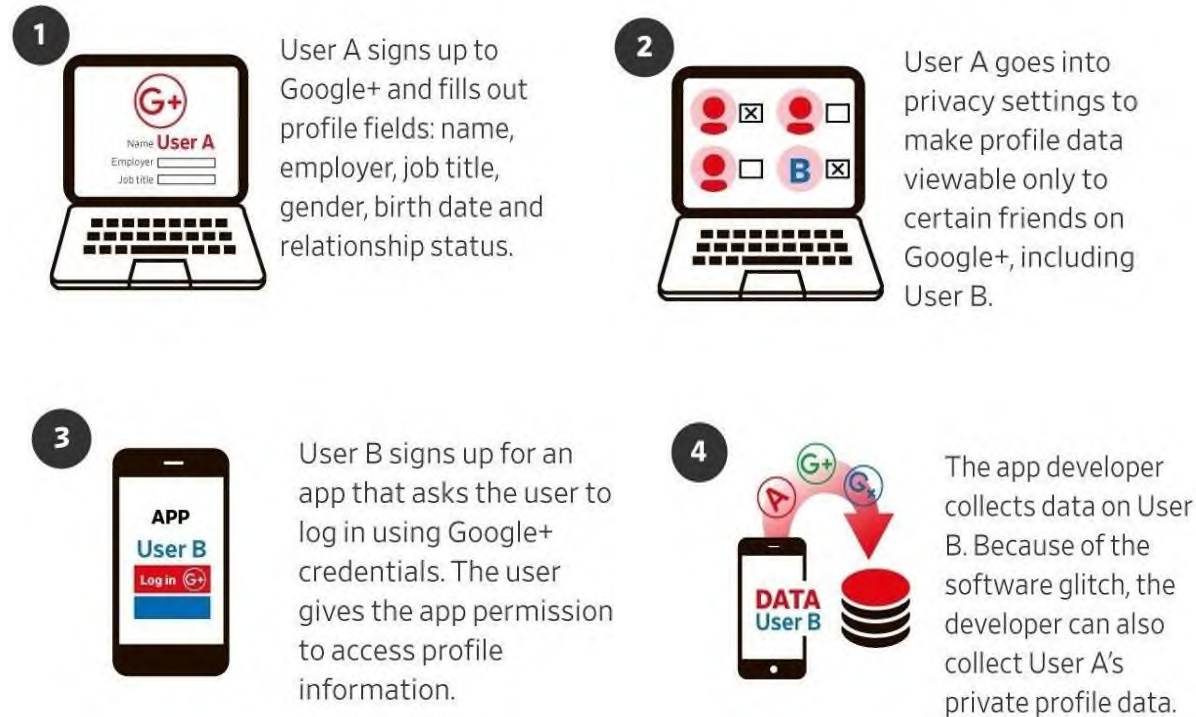
25 <sup>12</sup> *Id.* at 41:00.

26 <sup>13</sup> Google, *Project Strobe: Protecting your data, improving our third-party APIs, and sunseting consumer*  
27 *Google+*, (October 8, 2018), available at <https://www.blog.google/technology/safety-security/project-strobe/> (last  
28 visited December 11, 2018); see also The Wall Street Journal, *Google Exposed User Data, Feared Repercussions*  
*of Disclosing to Public*, *supra* fn. 10.

<sup>14</sup> Google, *Project Strobe: Protecting your data, improving our third-party APIs, and sunseting consumer*  
*Google+*, *supra* fn. 11.

1 without User consent. Google represented that this vulnerability could have potentially affected  
 2 up to half a million Google users from 2015 and May 2018.<sup>15</sup>

3 In sum, the First Data Leak made it possible for third parties to access private Personal  
 4 Information about Users who never had an opportunity to consent to such access. The access  
 5 allowed through this “glitch” is shown in the following illustration:



19 Defendants have advised that at least 438 third-party applications may have used the API  
 20 related to the First Data Leak and thereby had been allowed unauthorized access to certain  
 21 Google+ users’ Personal Information for nearly 3 years.<sup>16</sup>

22 When the First Data Leak was disclosed, it immediately drew comparisons to Facebook’s  
 23 leak of user information to Cambridge Analytica and other third-party application developers.<sup>17</sup>

25 <sup>15</sup> The Wall Street Journal, *Google Exposed User Data, Feared Repercussions of Disclosing to Public*, *supra*  
 26 fn. 10.

26 <sup>16</sup> Google, *Project Strobe: Protecting your data, improving our third-party APIs, and sunseting consumer*  
 27 *Google+*, *supra* fn. 11.

27 <sup>17</sup> The Wall Street Journal, *Google Exposed User Data, Feared Repercussions of Disclosing to Public*, *supra*  
 28 fn. 10. See also The Washington Post, *Facebook: ‘Malicious actors’ used its tools to discover identities and collect*  
*data on a massive global scale* (April 4, 2018), available at <https://www.washingtonpost.com/news/the->

1 Given that Google+ was launched to challenge Facebook, the data security incidents suffered by  
2 Facebook users should have made Defendants more sensitive to the necessary protection of  
3 Google+ Users’ data.

4 Instead, after discovering this vulnerability in the Google+ platform, Defendants kept  
5 silent for at least seven months, making a calculated decision to not inform Users that their  
6 Personal Information was compromised and allowing the unauthorized compromise of Users’  
7 Personal information and their exposure to risk of identity theft or worse to continue during that  
8 time.

9 Although Defendants claimed in the blog post announcing the First Data Leak that they  
10 “found no evidence that any developer was aware of this bug, or abusing the API” or “that any  
11 Profile data was misused,” Defendants also represented that they only kept logs for two weeks.<sup>18</sup>  
12 Thus, based on Defendants’ own admission that they can only account for whether the Google+  
13 vulnerability had been exploited in the two weeks preceding its discovery, they have insufficient  
14 records to confirm whether and what data breaches had occurred during the three-year exposure  
15 period. As such, the full extent of the damage caused by Defendants’ failure to provide adequate  
16 controls and protection for Users’ Personal Information may never be known. Accordingly, the  
17 number of impacted Users, as well as the third-party applications that may have been able to  
18 exploit the Google+ vulnerability to access Users’ Personal Information, was likely significantly  
19 more than what Google disclosed – 500,000 Users and 438 third-party applications.

20 Plaintiffs’ gravest concerns proved true when Defendants announced the Second Data  
21 Leak just over two months later, which concerned similar-if-not-identical API, exposing the  
22 Personal Information of approximately 52.5 million Google+ Users – bringing the total potential  
23 exposure to 53 million Google+ Users.<sup>19</sup>

24  
25  
26 

---

[switch/wp/2018/04/04/facebook-said-the-personal-data-of-most-its-2-billion-users-has-been-collected-and-shared-with-outsiders/?utm\\_term=.61ae2fe14b0b](https://www.switch/wp/2018/04/04/facebook-said-the-personal-data-of-most-its-2-billion-users-has-been-collected-and-shared-with-outsiders/?utm_term=.61ae2fe14b0b) (last visited December 11, 2018).

27 <sup>18</sup> Google, *Project Strobe: Protecting your data, improving our third-party APIs, and sunseting consumer*  
*Google+*, *supra* fn. 11.

28 <sup>19</sup> The Wall Street Journal, *Google to Accelerate Closure of Google+ Social Network After Finding New*  
*Software Bug*, *supra* fn. 10.

1 Although Defendants have represented that the Second Data Leak only existed from  
2 November 7, 2018 through November 13, 2018, Defendants have provided few details and still  
3 intend to operate the clearly bug-ridden and unsecure Google+ platform until April 2019.<sup>20</sup>

4 This case involves the absolute and intentional disregard with which Defendants have  
5 chosen to treat the Personal Information of Users who have utilized their Google+ social media  
6 platform. While this Personal Information was supposed to be protected and shared only with  
7 expressed permissions, Defendants – without authorization – exposed that information to third  
8 parties through lax and non-existent data safety and security policies and protocols.

9 **C. Defendants’ Business Decision to Not Immediately Disclose the First Data**  
10 **Leak Put Their Interests Above That of Google+ Users and Exacerbated the**  
11 **Harm Caused**

12 Equally troubling to the widespread and unknown impact of the First Data Leak is  
13 Defendants’ intentional effort, approved by their upper management, to conceal the leak from the  
14 public and their victims.

15 When Defendants announced the First Data Leak, they shocked the public by revealing  
16 that they had discovered and “fixed” the security vulnerability in March 2018 – an astonishing  
17 seven months before the announcement.<sup>21</sup>

18 According to the Wall Street Journal, a Google internal memorandum prepared by its legal  
19 and policy staff and shared with its senior executives revealed that Google had hidden the security  
20 vulnerability for six months to avoid public scrutiny about its privacy practices.<sup>22</sup> According to  
21 that internal memorandum, Defendants’ decision not to disclose the Google+ vulnerability was  
22 motivated by the fear that doing so would draw “immediate regulatory interest,” bring Google  
23 “into the spotlight alongside or even instead of Facebook despite having stayed under the radar  
24

---

25 <sup>20</sup> *Id.* See also Google, *Expediting changes to Google+* (December 10, 2018), available at  
26 <https://www.blog.google/technology/safety-security/expediting-changes-google-plus/> (last visited December 11,  
2018).

27 <sup>21</sup> Google, *Project Strobe: Protecting your data, improving our third-party APIs, and sunseting consumer*  
28 *Google+, supra* fn. 11.

<sup>22</sup> The Wall Street Journal, *Google Exposed User Data, Feared Repercussions of Disclosing to Public, supra*  
fn. 10.

1 throughout the Cambridge Analytica scandal,” and “almost [guarantee that] Sundar [Pichai, Chief  
2 Executive Officer of Google,] will testify before Congress.”<sup>23</sup>

3 Google’s failure to adequately disclose the Google+ vulnerability for months on end has  
4 made the regulatory and congressional interest in the data breach even greater than if Google had  
5 simply disclosed it when it was discovered. The First Data Leak has directly led to recent  
6 Congressional calls for investigation, including questions regarding Google’s compliance with  
7 the aforementioned FTC consent decree’s requirements with respect to privacy settings and the  
8 protection of private information.<sup>24</sup>

9 An October 11, 2018 letter to Pichai from Commerce Committee Chairman John Thune  
10 (R-S.D.) detailed Google’s culture of concealment and opacity, noting that:

11 At the same time that Facebook was learning the important lesson that tech firms  
12 must be forthright with the public about privacy issues, Google apparently elected  
13 to withhold information about a relevant vulnerability for fear of public scrutiny.  
14 We are especially disappointed given that Google’s chief privacy officer testified  
15 before the Senate Commerce Committee on the issue of privacy on September 26,  
16 2018—just two weeks ago—and did not take the opportunity to provide  
17 information regarding this very relevant issue to the Committee.<sup>25</sup>

18 In addition, an October 11, 2018 letter to Pichai from Senate Judiciary Committee  
19 Chairman Chuck Grassley not only detailed the obvious similarities between the First Data Leak  
20 and Facebook’s widely publicized Cambridge Analytica scandal, but also reprimanded Google  
21 for its refusal to participate in past hearings on data breaches when it had concealed knowledge  
22 of the First Data Leak:

23 In March of this year, data privacy and social media was in the spotlight thanks to  
24 events surrounding Facebook and Cambridge Analytica. I convened a hearing with  
25 the CEO of Facebook on April 10, 2018, and according to his testimony, a feature  
26 in Facebook’s application programming interface, or API, allowed third party

27 <sup>23</sup> *Id.*

28 <sup>24</sup> *Senator Blumenthal’s Letter to FTC Chairman* (October 10, 2018), available at  
<https://www.blumenthal.senate.gov/imo/media/doc/10.10.18%20-%20FTC%20-%20Google%20Plus%20Exposure.pdf> (last visited December 11, 2018); *Senator Thune’s Letter to Sundar Pichai*  
(October 11, 2018), available at [https://www.commerce.senate.gov/public/\\_cache/files/4852b311-0953-4ac8-ac43-a91dde229cc1/E300DA0C7659678AE0AE37AEB9746200.thune-wicker-moran-letter-to-google-10.11.18.pdf](https://www.commerce.senate.gov/public/_cache/files/4852b311-0953-4ac8-ac43-a91dde229cc1/E300DA0C7659678AE0AE37AEB9746200.thune-wicker-moran-letter-to-google-10.11.18.pdf) (last  
visited December 11, 2018); *Senator Grassley’s Letter to Sundar Pichai* (October 11, 2018), available at  
<https://www.judiciary.senate.gov/imo/media/doc/2018-04-10%20CEG%20to%20Google%20-%20Data%20Privacy.pdf> (last visited December 11, 2018).

<sup>25</sup> *Senator Thune’s Letter to Sundar Pichai*, *supra* fn. 22.

1 developers to pull information not just from users of an application, but also that  
2 user's friends, even if the friend had made their information private. . . .

3 At the time, I invited you and the CEO of Twitter to participate in the hearing to  
4 discuss the future of data privacy in the social media industry. . . . ***Your office,***  
5 ***however, declined to come before Congress and the American people, asserting***  
6 ***that the problems surrounding Facebook and Cambridge Analytica did not***  
7 ***involve Google.***

8 Given your and Google's unwillingness to participate. I sent you a letter seeking  
9 information on Google's current data privacy policies, specifically as they relate  
10 to Google's third-party developer APIs. Your responses to my questions  
11 highlighted Google's application verification process, the continuous, monitoring  
12 of applications through machine learning, and the use of manual audits, all to  
13 ensure robust protection of user data.

14 ***Despite your contention that Google did not have the same data protection***  
15 ***failures as Facebook, it appears from recent reports that Google+ had an almost***  
16 ***identical feature to Facebook, which allowed third party developers to access***  
17 ***information from users as well as private information of those users'***  
18 ***connections.*** Moreover, it appears that you were aware of this issue at the time I  
19 invited you to participate in the hearing and sent you the letter regarding Google's  
20 policies.<sup>26</sup>

21 Defendants thus chose to protect themselves from potential governmental inquiry rather  
22 than protect the Personal Information of Google+ users and advise them that their Personal  
23 Information had been exposed in the First Data Leak to unauthorized third parties.

24 Defendants withheld the information of the First Data Leak from Google+ users and the  
25 public until announcing it alongside their decision to shut down the Google+ service for  
26 consumers in August 2019 —approximately 10 months later.

27 At every turn, Defendants put their own business interests ahead of the privacy interests  
28 of Google+ users, causing harm to Plaintiffs and Class members.

The First Data Leak has caused significant harm to Plaintiffs and other Class members by  
allowing third-parties to access their Personal Information without their consent. This harm was  
exacerbated by Google's culture of concealment and opacity regarding its insufficient data  
protection policies and the resulting data breach.

---

<sup>26</sup> *Senator Grassley's Letter to Pichai, supra* fn. 22 (emphasis added).

1 Despite numerous lapses in and rebukes on its approach to data security, Google still lacks  
 2 sufficient safeguards and protections for Users' Personal Information and has shown a conscious  
 3 disregard for any transparency regarding the potential exposure of their personal information.  
 4 This danger has already manifested in the Second Data Leak revealed by Defendants just months  
 5 later. Thus, Plaintiffs and Class members' Personal Information remains at risk today and into the  
 6 future, until Google is compelled to secure their Personal Information.

7 **D. Defendants Failed to Properly Secure Google+ After the First Data Leak,**  
 8 **Resulting in the Exposure of Even More Users' Personal Information in the**  
 9 **Second Data Leak**

9 Despite the increased attention from the First Data Leak in October 2018, Defendants  
 10 continued to operate the Google+ service and collect Users' Personal Information, with no plans  
 11 to shut the Google+ service down until August 2019.

12 Then, just *nine weeks* after their announcement of the First Data Leak, Defendants had to  
 13 disclose that they had again improperly exposed Users' Personal Information to third-party  
 14 application developers.

15 Specifically, on December 10, 2018, Defendants announced that they would be expediting  
 16 their closure of Google+ due to the Second Data Leak, whereby the Personal Information of Users  
 17 was, again, improperly exposed to third-party application developers.<sup>27</sup> This time, up to 52.5  
 18 million Users were impacted.<sup>28</sup> Defendants had permitted the Second Data Leak to persist from  
 19 November 7, 2018 until November 13, 2018, when they allegedly identified and fixed  
 20 vulnerabilities that had again permitted unauthorized third parties to access and aggregate Users'  
 21 Personal Information.<sup>29</sup>

22 The Second Data Leak allowed third-party application developers to view profile  
 23 information from Users, including, *inter alia*, a User's name, email address, occupation, work  
 24

---

25 <sup>27</sup> Google, *Expediting changes to Google+* (December 10, 2018), available at  
 26 <https://www.blog.google/technology/safety-security/expediting-changes-google-plus/> (last visited December 11,  
 2018).

27 <sup>28</sup> *Id.*

28 <sup>29</sup> Statt and Brandom, *Google will shut down Google+ four months early after second data leak* (December  
 10, 2018), available at [https://www.theverge.com/platform/amp/2018/12/10/18134541/google-plus-privacy-api-  
 data-leak-developers](https://www.theverge.com/platform/amp/2018/12/10/18134541/google-plus-privacy-api-data-leak-developers) (last visited December 11, 2018).

1 history, age, relationship status, biography, gender, and birthday – even if the User’s account was  
 2 set to private.<sup>30</sup> Third-party developers were also able to improperly access Users’ profile data  
 3 that had been shared with a specific User, but was not shared publicly by the User.<sup>31</sup>

4 As a result of the Second Data Leak, Defendants announced their decision to accelerate  
 5 the shut-down of the consumer functionality of Google+ from August 2019 to April 2019.<sup>32</sup>

#### 6 **E. Users’ Personal Information Is an Increasingly Valuable Commodity**

7 Personal information from social media, like the Personal Information encompassed in  
 8 the Google+ Data Leaks, is incredibly valuable to companies like Google. In 2017 alone,  
 9 Google’s advertisement revenue – which is dependent on Google’s ability to collect personal  
 10 information about its users – amounted to nearly \$95.4 billion.<sup>33</sup>

11 One study found that the average consumer in the U.S. can make \$240 per year monetizing  
 12 his or her personal data for digital advertising.<sup>34</sup> Another study in 2018 found that social media  
 13 advertising revenue currently amounts to \$67.97 billion, and that the average revenue per Internet  
 14 user currently amounts to approximately \$22.84.<sup>35</sup> Similarly, a 2016 study found that Google  
 15 makes approximately \$7.00 per monthly active user each quarter, or approximately \$28.00 per  
 16 user each year.<sup>36</sup>

17 Defendants’ calculation of the average revenue each user generates is derived from an  
 18 analysis of, *inter alia*, the content and information each user shares.<sup>37</sup> Thus, when Users signed  
 19 up to join Google+, they were entering into a transaction – a value-for-value exchange – in which  
 20

---

21 <sup>30</sup> Google, *Expediting changes to Google*, *supra* fn. 25; Google, *Google+ API, List of Personal Information*,  
 22 available at <https://developers.google.com/+/web/api/rest/latest/people> (last visited December 11, 2018). *See also*  
 Statton and Brandom, *supra*, fn. 26.

23 <sup>31</sup> *Id.*

24 <sup>32</sup> Google, *Expediting changes to Google*, *supra* fn. 25.

25 <sup>33</sup> Alphabet, *Form 10-K* for the fiscal year ended December 31, 2017, filed with the SEC on February 6, 2018,  
 26 at 28.

27 <sup>34</sup> Medium, *How Much is Your Data Worth? At Least \$240 per Year. Likely Much More*, available at  
 28 <https://medium.com/wibson/how-much-is-your-data-worth-at-least-240-per-year-likely-much-more-984e250c2ffa>  
 (last visited December 11, 2018).

<sup>35</sup> Statista, *Social Media Advertising*, available at <https://www.statista.com/outlook/220/100/social-media-advertising/worldwide#market-revenuePerInternetUser> (last visited December 11, 2018).

<sup>36</sup> Ampere Analysis, *Facebook Closes the Gap on Google*, available at  
<https://www.ampereanalysis.com/blog/fd5b6dc9-d76e-40a8-b8f2-e5ed15bc32bb> (last visited December 11, 2018).

<sup>37</sup> See, *i.e.*, Google, *Google AdMob ARPU (metric)*, available at  
<https://support.google.com/admob/answer/7374260?hl=en> (discussing the metric of average revenue per user, or  
 ABPU, that third-party application developers have access to when using Google’s AdMob advertising platform).



1 they agreed to provide content and Personal Information that Defendants could use, subject to the  
2 Users' privacy restrictions. Because exclusive access to such content and information confers a  
3 competitive advantage, there is a "first user" value to the content and information. That value has  
4 now been lost due to the Google+ Data Leaks.

5 Additionally, the Personal Information compromised in the Google+ Data Leaks is highly  
6 valuable to identity thieves. The names, birthdates, hometowns, addresses, locations, interests,  
7 relationships, email addresses, photos, and videos, and other valuable personal information can  
8 all be used to gain access to a variety of existing accounts and websites.

9 Identity thieves can also use the Personal Information to harm Plaintiffs and the other  
10 Class members through embarrassment, blackmail, or harassment in person or online or to  
11 commit other types of fraud including obtaining ID cards or driver's licenses, fraudulently  
12 obtaining tax returns and refunds, and obtaining government benefits. A Presidential identity theft  
13 report from 2008 states that:

14 In addition to the losses that result when identity thieves fraudulently open  
15 accounts or misuse existing accounts, . . . individual victims often suffer indirect  
16 financial costs, including the costs incurred in both civil litigation initiated by  
17 creditors and in overcoming the many obstacles they face in obtaining or retaining  
18 credit. Victims of non-financial identity theft, for example, health-related or  
19 criminal record fraud, face other types of harm and frustration.

20 In addition to out-of-pocket expenses that can reach thousands of dollars for the  
21 victims of new account identity theft, and the emotional toll identity theft can take,  
22 some victims have to spend what can be a considerable amount of time to repair  
23 the damage caused by the identity thieves. Victims of new account identity theft,  
24 for example, must correct fraudulent information in their credit reports and  
25 monitor their reports for future inaccuracies, close existing bank accounts and  
26 open new ones, and dispute charges with individual creditors.<sup>38</sup>

27  
28 <sup>38</sup> U.S. FTC, *The President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan*, (April 2007), <https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf> (last visited December 11, 2018).

1 To put it into context, the 2013 Norton Report<sup>39</sup> – based on one of the largest consumer  
 2 cybercrime studies ever conducted – estimated that the global price tag of cybercrime was around  
 3 **\$113 billion** at that time, with the average cost per victim being \$298 dollars, as demonstrated in  
 4 the chart below:



16 The problems associated with identity theft are exacerbated by the fact that many identity  
 17 thieves will wait years before attempting to use the Personal Information they have obtained.  
 18 Indeed, in order to protect themselves, Plaintiffs and the other Class members will need to remain  
 19 vigilant against unauthorized data use for years and decades to come.

20 Once stolen, personal information can be used in a number of different ways. One of the  
 21 most common ways is that it is offered for sale on the dark web, a heavily encrypted part of the  
 22 Internet that makes it difficult for authorities to detect the location or owners of a website. Due to  
 23 its hidden nature and the use of special applications to maintain anonymity, the dark web is a  
 24 haven for all kinds of illicit activity, including the trafficking of stolen personal information

28 <sup>39</sup> Norton by Symantec, *2013 Norton Report*, available at [https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton\\_raportti.pdf](https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf) (last visited December 10, 2018).

1 captured via data breaches or hacks.<sup>40</sup> One 2018 study found that an individual’s online identity  
 2 is worth approximately \$1,170 on the dark web.<sup>41</sup>

3 Once someone buys personal information, it is then used to gain access to different areas  
 4 of the victim’s digital life, including bank accounts, social media, and credit card details. During  
 5 that process, other sensitive data may be harvested from the victim’s accounts, as well as from  
 6 those belonging to family, friends, and colleagues.

7 Personal information can also be used by scammers to target victims using phishing  
 8 scams.<sup>42</sup> Phishing is when scammers use personal information they have obtained about victims  
 9 to send fraudulent emails or texts, or copycat websites to get victims to share additional valuable  
 10 personal information – such as account numbers, Social Security numbers, or login IDs and  
 11 passwords.<sup>43</sup> Scammers use victims’ information, including Personal Information, to steal the  
 12 victims’ money, identity, or both.<sup>44</sup> Scammers also use phishing emails to get access to a victim’s  
 13 computer or network, then install programs like ransomware that can lock a victim out of  
 14 important files on their computer.<sup>45</sup> According to one Federal Bureau of Investigation study,  
 15 scammers collected more than \$676 million in 2017 alone through two types of phishing scams:  
 16 “Business Email Compromise” and “Email Account Compromise.”<sup>46</sup>

17 Due to Defendants’ conduct described herein, Plaintiffs and the other Class members have  
 18 a greater risk of identity theft, manipulation, fraud, scams, and/or targeted unwanted and  
 19 unnecessary advertising, including inappropriate communications. Additionally, Plaintiffs and  
 20 the other Class members now face additional security risks such as phishing attempts, efforts by  
 21

22 \_\_\_\_\_  
 23 <sup>40</sup> Experian, *What is the Dark Web?* (April 8, 2018), available at <https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/> (last visited December 10, 2018). See also Brian Hamrick, *The dark web: A trip into the underbelly of the internet*, WLWT News (Feb. 9, 2017), <http://www.wlwt.com/article/the-dark-web-a-trip-into-the-underbelly-of-the-internet/8698419> (last visited December 10, 2018).

24 <sup>41</sup> TOP10VPN, Dark Web Market Price Index (US Edition) (February 27, 2018), available at  
 25 <https://www.top10vpn.com/privacy-central/privacy/dark-web-market-price-index-feb-2018-us/> (last visited  
 December 10, 2018).

26 <sup>42</sup> U.S. FTC, *Phishing* (July 2017), available at <https://www.consumer.ftc.gov/articles/0003-phishing> (last  
 visited December 12, 2018).

27 <sup>43</sup> *Id.*

<sup>44</sup> *Id.*

<sup>45</sup> *Id.*

28 <sup>46</sup> U.S. Federal Bureau of Investigation, *2017 Internet Crime Report*, available at  
[https://pdf.ic3.gov/2017\\_IC3Report.pdf](https://pdf.ic3.gov/2017_IC3Report.pdf) (last visited December 12, 2018).

1 hackers trying to access or log in to their online accounts, friend requests from trolls or cloned or  
2 imposter accounts, and/or other interference with their online accounts. Plaintiffs and the other  
3 Class members are subjected to a heightened risk of such predatory conduct due to Defendants’  
4 failure to secure their Personal Information, including the sale of their content and Personal  
5 Information on the dark web and other illicit databases.

6 **F. Google Has A Long History of Improper Data Practices**

7 Google has been on notice of deficiencies regarding its policies involving the retention of  
8 User data since at least 2010. The FTC specifically found that Google used deceptive tactics and  
9 violated its own privacy promises to consumers when it launched its first social network product,  
10 Google Buzz, in 2010.

11 As a result of such deficiencies, Google agreed to a proposed settlement in March 2011,  
12 which contained a consent decree under which the FTC barred Google from misrepresenting the  
13 privacy of personal information or the extent to which consumers may exercise control over the  
14 collection, use, or exposure of their covered personal information.<sup>47</sup> The FTC also required  
15 Google to establish a “comprehensive privacy program that is reasonably designed to: (1) address  
16 privacy risks related to the development and management of new and existing products and  
17 services for consumers, and (2) protect the privacy and confidentiality of covered information.”  
18 Included in this privacy program was the “regular testing or monitoring of the effectiveness of  
19 those privacy controls and procedures,” which would be audited by an independent third-party  
20 professional.<sup>48</sup>

21 Less than a year after entering into the FTC consent decree, Google violated it – becoming  
22 one of the rare companies in the country that has violated an FTC consent decree – and paid a  
23 record fine for its circumvention of privacy protections in the web browser Safari.<sup>49</sup> In discussing  
24

25 \_\_\_\_\_  
26 <sup>47</sup> U.S. FTC, *In the Matter of GOOGLE INC., a corporation* (October 13, 2011), Docket No. C-4436,  
available at <https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf> (last visited  
December 11, 2018).

27 <sup>48</sup> *Id.*

28 <sup>49</sup> U.S. FTC, *Google Will Pay \$22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to  
Users of Apple’s Safari Internet Browser* (August 9, 2012), available at <https://www.ftc.gov/news-events/press->

1 the settlement, Jon Leibowitz, Chairman of the FTC, said, “The record setting penalty in this  
2 matter sends a clear message to all companies under an FTC privacy order. No matter how big or  
3 small, all companies must abide by FTC orders against them and keep their privacy promises to  
4 consumers, or they will end up paying many times what it would have cost to comply in the first  
5 place.”<sup>50</sup>

6 **CLASS ACTION ALLEGATIONS**

7 Pursuant to Federal Rules of Civil Procedure (“Rules” or “Rule”) 23(b)(2), (b)(3), and  
8 (c)(4), Plaintiffs, individually and on behalf of all others similarly situated, bring this lawsuit on  
9 behalf of themselves and as a class action on behalf of the following Class:

10 All persons in the United States who registered for Google+ accounts and whose Personal  
11 Information was accessed, compromised, or obtained from Google by third-party  
12 applications without authorization or in excess of authorization as a result of the 2018  
Data Leaks.

13 Excluded from the Class are Defendants and any entities in which Defendants or their  
14 subsidiaries or affiliates have a controlling interest, as well as Defendants’ officers, agents, and  
15 employees. Also excluded from the Class are the judge assigned to this action, members of the  
16 judge’s staff, and any member of the judge’s immediate family. Plaintiffs reserve the right to  
17 amend the Class definitions if discovery and further investigation reveal that any definitions  
18 should be expanded or otherwise modified.

19 **Numerosity:** The members of the Class are so numerous that joinder of all members of  
20 the Class would be impracticable. Defendants have indicated that at least 500,000 people had  
21 their Google+ accounts compromised as a result of the First Data Leak, and as many as  
22 52,500,000 people had their Google+ accounts compromised as a result of the Second Data Leak.  
23 The identity of these Google+ users can be determined through records and documents maintained  
24 by Defendants.

25  
26  
27 \_\_\_\_\_  
28 releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented (last visited December 11,  
2018).

<sup>50</sup> *Id.*

1           **Commonality and Predominance:** This action involves common questions of law or  
2 fact, which predominate over any questions affecting individual Class members, including:

- 3           i.       Whether Defendants represented to Plaintiffs and the Class that they would  
4           safeguard Class members' Personal Information;
- 5           ii.       Whether Defendants owed a legal duty to Plaintiffs and the Class to exercise due  
6           care in collecting, storing, and safeguarding their Personal Information;
- 7           iii.       Whether Defendants breached a legal duty to Plaintiffs and the Class to exercise  
8           due care in collecting, storing, and safeguarding their Personal Information;
- 9           iv.       Whether third parties improperly obtained Plaintiffs and Class members' Personal  
10           Information without authorization or in excess of any authorization;
- 11           v.       Whether Defendants were aware of other third parties' collection of Plaintiffs and  
12           Class members' Personal Information without authorization or in excess of any  
13           authorization;
- 14           vi.       Whether Defendants knew about the First Data Leak before it was announced to  
15           the public and whether Defendants failed to timely notify the public of the First  
16           Data Leak;
- 17           vii.       Whether Defendants knew about the Second Data Leak before it was announced  
18           to the public and whether Defendants failed to timely notify the public of the  
19           Second Data Leak;
- 20           viii.       Whether Defendants' conduct violated Cal. Civ. Code § 1750, *et seq.*;
- 21           ix.       Whether Defendants' conduct was an unlawful or unfair business practice under  
22           Cal. Bus. & Prof. Code § 17200, *et seq.*;
- 23           x.       Whether Defendants' conduct violated the Consumer Records Act, Cal. Civ. Code  
24           § 1798.80 *et seq.*;
- 25           xi.       Whether Defendants' conduct violated § 5 of the FTC Act, 15 U.S.C. § 45, *et seq.*;
- 26           xii.       Whether Plaintiffs and the Class are entitled to equitable relief, including, but not  
27           limited to, injunctive relief and restitution; and
- 28           xiii.       Whether Plaintiffs and the other Class members are entitled to actual, statutory, or  
                other forms of damages, and other monetary relief.

                Defendants engaged in a common course of conduct giving rise to the legal rights sought  
to be enforced by Plaintiffs individually and on behalf of the Class members. Similar or identical

1 statutory and common law violations, business practices, and injuries are involved. Individual  
2 questions, if any, pale by comparison, in both quantity and quality, to the numerous common  
3 questions that dominate this action.

4 Google's choice-of-law provision is further indication of the common questions of law.  
5 Google's Terms of Service provide, in relevant part, that "you agree that the laws of California,  
6 U.S.A., excluding California's choice of law rules, will apply to any disputes arising out of or  
7 relating to these terms or the Services."

8 **Typicality:** Plaintiffs' claims are typical of the claims of the other members of the class  
9 because, among other things, Plaintiffs and the other Class members were injured through the  
10 substantially uniform misconduct by Defendants. Plaintiffs are advancing the same claims and  
11 legal theories on behalf of themselves and all other Class members, and there are no defenses that  
12 are unique to Plaintiffs. The claims of Plaintiffs and those of other Class members arise from the  
13 same operative facts and are based on the same legal theories.

14 **Adequacy of Representation:** Plaintiffs are adequate representatives of the classes  
15 because their interests do not conflict with the interests of the other Class members they seek to  
16 represent, they have retained counsel competent and experienced in complex class action  
17 litigation, and they will prosecute this action vigorously. The Class members' interests will be  
18 fairly and adequately protected by Plaintiffs and their counsel.

19 **Superiority:** A class action is superior to any other available means for the fair and  
20 efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered  
21 in the management of this matter as a class action. The damages, harm, or other financial  
22 detriment suffered individually by Plaintiffs and the other members of their respective classes are  
23 relatively small compared to the burden and expense that would be required to litigate their claims  
24 on an individual basis against Defendants, making it impracticable for Class members to  
25 individually seek redress for Defendants' wrongful conduct. Even if Class members could afford  
26 individual litigation, the court system could not. Individualized litigation would create a potential  
27 for inconsistent or contradictory judgments, and increase the delay and expense to all parties and  
28 the court system. By contrast, the class action device presents far fewer management difficulties

1 and provides the benefits of single adjudication, economies of scale, and comprehensive  
2 supervision by a single court.

3 Further, Defendants has acted or refused to act on grounds generally applicable to the  
4 Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the  
5 members of the Class as a whole is appropriate under Rule 23(b)(2).

6 Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because  
7 such claims present only particular, common issues, the resolution of which would advance the  
8 disposition of this matter and the parties' interests therein. Such particular issues include, but are  
9 not limited to:

- 10 a. Whether Class members' Personal Information was improperly obtained by third  
11 parties;
- 12 b. Whether (and when) Defendants knew about any security vulnerabilities that led  
13 to the First Data Leak before they were announced to the public and whether  
14 Defendants failed to timely notify the public of those vulnerabilities and the First  
15 Data Leak;
- 16 c. Whether (and when) Defendants knew about any security vulnerabilities that led  
17 to the Second Data Leak before they were announced to the public and whether  
18 Defendants failed to timely notify the public of those vulnerabilities and the  
19 Second Data Leak;
- 20 d. Whether Defendants' conduct was an unlawful or unfair business practice under  
21 Cal. Bus. & Prof. Code § 17200, *et seq.*;
- 22 e. Whether Defendants' representations that they would secure and protect the  
23 Personal Information of Plaintiffs and the other members of the Class were facts  
24 that reasonable persons could be expected to rely upon when deciding whether to  
25 use Defendants' services;
- 26 f. Whether Defendants misrepresented the safety of their many systems and services,  
27 specifically the security thereof, and their ability to safely store Plaintiffs' and the  
28 other Class members' Personal Information;
- g. Whether Defendants concealed crucial information about their inadequate data  
security measures from Plaintiffs and the Class;
- h. Whether Defendants failed to comply with their own policies and applicable laws,  
regulations, and industry standards relating to data security;



- 1 i. Whether Defendants knew or should have known that they did not employ  
2 reasonable measures to keep Plaintiffs’ and the other Class members’ Personal  
3 Information secure and prevent the unauthorized disclosure of that information;
- 4 j. Whether Defendants failed to “implement and maintain reasonable security  
5 procedures and practices” for Plaintiffs’ and the other Class members’ Personal  
6 Information in violation of § 5 of the FTC Act;
- 7 k. Whether Defendants failed to provide timely notice of the First Data Leak in  
8 violation of California Civil Code § 1798.82;
- 9 l. Whether Defendants failed to provide timely notice of the Second Data Leak in  
10 violation of California Civil Code § 1798.82;
- 11 m. Whether Defendants’ conduct violated Cal. Bus. & Prof. Code § 22575, *et seq.*;
- 12 n. Whether Defendants owed a duty to Plaintiffs and the Class to safeguard their  
13 Personal Information and to implement adequate data security measures;
- 14 o. Whether Defendants breached that duty;
- 15 p. Whether Defendants failed to adhere to their posted privacy policy concerning the  
16 care they would take to safeguard Plaintiffs’ and the other Class members’  
17 Personal Information in violation of California Business and Professions Code §  
18 22576;
- 19 q. Whether Defendants negligently and materially failed to adhere to their posted  
20 privacy policy with respect to the extent of their disclosure of users’ data, in  
21 violation of California Business and Professions Code § 22576;
- 22 r. Whether such representations were false with regard to storing and safeguarding  
23 Class and Class members’ Personal Information; and
- 24 s. Whether such representations were material with regard to storing and  
25 safeguarding Class members’ Personal Information.

26 **First Claim for Relief**

27 **Violation of California’s Unfair Competition Law (“UCL”) – Unlawful Business  
28 Practice (Cal. Bus. & Prof. Code § 17200, et seq.)**

Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

Defendants’ choice-of-law provision establishes that California law applies to Plaintiffs’ and the other Class members’ claims.

1 By reason of the conduct alleged herein, Defendants engaged in unlawful practices within  
2 the meaning of the UCL. The conduct alleged herein is a “business practice” within the meaning  
3 of the UCL.

4 Google represented that it would not disclose Google+ users’ Personal Information  
5 without consent and/or notice. Google further represented that it would utilize sufficient data  
6 security protocols and mechanisms to protect Google+ users’ Personal Information.

7 Defendants failed to abide by these representations. Defendants did not prevent the  
8 improper disclosure of Plaintiffs’ and the Class’s Personal Information.

9 Defendants stored the Personal Information of Plaintiffs and the members of their  
10 respective Classes in Defendants’ electronic and consumer information databases. Defendants  
11 falsely represented to Plaintiffs and the other members of the Classes that the Personal  
12 Information databases were secure and that their Personal Information would remain private.  
13 Defendants knew or should have known they did not employ reasonable, industry standard, and  
14 appropriate security measures that complied “with federal regulations” and that would have kept  
15 Plaintiffs’ and the other Class members’ Personal Information secure and prevented the loss or  
16 misuse of such Personal Information.

17 Even without these misrepresentations, Plaintiffs and the other Class members were  
18 entitled to assume, and did assume, that Defendants would take appropriate measures to keep  
19 their Personal Information safe. Defendants did not disclose at any time that Plaintiffs’ Personal  
20 Information was accessible to third party application vendors because Defendants’ data security  
21 measures were inadequate, even though Defendants were the only ones in possession of that  
22 material information, which they had a duty to disclose. Defendants violated the UCL by  
23 misrepresenting, both by affirmative conduct and by omission, the strength of the security of their  
24 many systems and services, and their ability to honor the disclosure authorizations established by  
25 Plaintiffs and the other Class members for their Personal Information.

26 Defendants also violated the UCL by failing to implement reasonable and appropriate  
27 security measures or follow industry standards for data security, and failing to comply with their  
28

1 own posted privacy policies. If Defendants had complied with these legal requirements, Plaintiffs  
2 and the other Class members would not have suffered the damages described herein.

3 Defendants' acts, omissions, and misrepresentations, as alleged herein, were unlawful and  
4 in violation of, *inter alia*, Section 5(a) of the FTC Act and 15 U.S.C. § 45(a), Cal. Bus. & Prof.  
5 Code § 22576 (as a result of Google failing to comply with its own posted privacy policies).

6 Plaintiffs and the other Class members suffered injury in fact and lost money or property  
7 as the result of Defendants' unlawful business practices. In particular, Plaintiffs' and the other  
8 Class members' Personal Information was taken and is in the hands of those who will use it for  
9 their own advantage, or is being sold for value, making it clear that such information is of tangible  
10 value.

11 As a result of Defendants' unlawful business practices, which are violations of the UCL,  
12 Plaintiffs and the other Class members are entitled to restitution, disgorgement of wrongfully  
13 obtained profits, and injunctive relief.

14 **Second Claim for Relief**

15 **Violation of California's UCL – Unfair Business Practice**  
16 **(Cal. Bus. & Prof. Code § 17200, *et seq.*)**

17 Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation  
18 contained above as though the same were fully set forth herein.

19 Defendants' choice-of-law provision establishes that California law applies to Plaintiffs'  
20 and the other Class members' claims.

21 By reason of the conduct alleged herein, Defendants engaged in unfair "business  
22 practices" within the meaning of the UCL.

23 Defendants stored the Personal Information of Plaintiffs and the members of their  
24 respective Classes in their electronic and consumer information databases. Defendants  
25 represented to Plaintiffs and the other members of the Class that their Personal Information  
26 databases were secure and that such Personal Information would remain private and be disclosed  
27 only with expressed authorization. Defendants engaged in unfair acts and business practices by  
28

1 representing that they would require expressed consent and authorization from Plaintiffs and the  
2 other Class members prior to the disclosure of Personal Information to third parties.

3 Even without these misrepresentations, Plaintiffs and the other Class members were  
4 entitled to, and did, assume Defendants would take appropriate measures to keep their Personal  
5 Information safe. Defendants did not disclose at any time that Plaintiffs' Personal Information  
6 was vulnerable to unauthorized disclosure because Defendants' data security measures were  
7 inadequate, even though Defendants were in sole possession of that material information, which  
8 they had a duty to disclose.

9 Defendants knew or should have known they did not employ reasonable measures that  
10 would have kept Plaintiffs' and the other Class members' Personal Information secure from  
11 unauthorized disclosure.

12 Defendants engaged in unfair acts and business practices by representing that they would  
13 not disclose this Personal Information without authorization and/or by obtaining that Personal  
14 Information without authorization. Not only did Defendants also violate their commitment to  
15 maintain the confidentiality and security of the Personal Information of Plaintiffs and their  
16 respective Classes, but they failed to comply with their own stated policies and applicable laws,  
17 regulations, and industry standards relating to data security.

18 **Defendants engaged in unfair business practices under the “balancing test.”** The  
19 harm caused by Defendants' actions and omissions, as described in detail *supra*, greatly outweigh  
20 any perceived utility. Indeed, Defendants' failure to follow basic data security protocols and  
21 misrepresentations to consumers about Defendants' data security cannot be said to have had any  
22 utility at all.

23 **Defendants engaged in unfair business practices under the “tethering test.”**  
24 Defendants' actions and omissions, as described in detail *supra*, violated fundamental public  
25 policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 (“The  
26 Legislature declares that ... all individuals have a right of privacy in information pertaining to  
27 them.... The increasing use of computers ... has greatly magnified the potential risk to individual  
28 privacy that can occur from the maintenance of Personal Information.”); Cal. Bus. & Prof. Code

1 § 22578 (“It is the intent of the Legislature that this chapter [including the Online Privacy  
2 Protection Act] is a matter of statewide concern.”). Defendants’ acts and omissions, and the  
3 injuries caused by them, are thus “comparable to or the same as a violation of the law ...” *Cel-*  
4 *Tech Communications, Inc. v. Los Angeles Cellular Telephone Co.* (1999) 20 Cal.4th 163, 187.

5 **Defendants engaged in unfair business practices under the “FTC test.”** The harm  
6 caused by Defendants’ actions and omissions, as described in detail *supra*, is substantial in that it  
7 affects up to 53 million Class members and has caused those persons to suffer actual harms. Such  
8 harms include a substantial risk of identity theft, disclosure of Class members’ Personal  
9 Information to third parties without their consent, diminution in value of their Personal  
10 Information, and consequential out-of-pocket losses for procuring credit freeze or protection  
11 services, identity theft monitoring, and other expenses relating to identity theft losses or protective  
12 measures. This harm continues given the fact that Class members’ Personal Information remains  
13 in Defendants’ possession, without adequate protection, and is also in the hands of those who  
14 obtained it without their consent. Defendants’ actions and omissions violated, *inter alia*, Section  
15 5(a) of the FTC Act, 15 U.S.C. § 45. *See, e.g., F.T.C. v. Wyndham Worldwide Corp.*, 10 F. Supp.  
16 3d 602, 613 (D.N.J. 2014), *aff’d*, 799 F.3d 236 (3d Cir. 2015); *In re LabMD, Inc.*, FTC Docket  
17 No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate  
18 measures to secure Personal Information collected violated § 5(a) of FTC Act); *In re BJ’s*  
19 *Wholesale Club, Inc.*, FTC Docket No. C-4148, FTC File No. 042-3160 (Sept. 20, 2005) (same);  
20 *In re CardSystems Solutions, Inc.*, FTC Docket No. C-4168, FTC File No. 052-3148 (Sept. 5,  
21 2006) (same); *see also United States v. ChoicePoint, Inc.*, Civil Action No. 1:06-cv-0198-JTC  
22 (N.D. Ga. Oct. 14, 2009) (“failure to establish and implement, and thereafter maintain, a  
23 comprehensive information security program that is reasonably designed to protect the security.  
24 confidentiality, and integrity of Personal Information collected from or about consumers” violates  
25 § 5(a) of FTC Act); 15 U.S.C. § 45(n) (defining “unfair acts or practices” as those that “cause[]  
26 or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by  
27 consumers themselves and not outweighed by countervailing benefits to consumers or to  
28 competition.”).

1 Plaintiffs and the other Class members suffered injury in fact and lost money or property  
2 as the result of Defendants' unfair business practices. In addition, their Personal Information was  
3 taken and is in the hands of those who will use it for their own advantage, or is being sold for  
4 value, making it clear that the hacked information is of tangible value.

5 As a result of Defendants' unfair business practices, which are violations of the UCL,  
6 Plaintiffs and the other Class members are entitled to restitution, disgorgement of wrongfully  
7 obtained profits, and injunctive relief.

8 **Third Claim for Relief**

9 **Violation of California's UCL – Fraudulent/Deceptive Business Practice**  
10 **(Cal. Bus. & Prof. Code § 17200, *et seq.*)**

11 Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation  
12 contained above as though the same were fully set forth herein.

13 Defendants' choice-of-law provision establishes that California law applies to Plaintiffs'  
14 and the other Class members' claims.

15 Defendants engaged in fraudulent and deceptive acts and practices with regard to the  
16 services they provided to the Class by representing and advertising that (1) they would maintain  
17 adequate data privacy and security practices and procedures to safeguard Class members'  
18 Personal Information from unauthorized disclosure, release, data breaches, and theft; and (2) they  
19 did and would comply with the requirements of relevant federal and state laws pertaining to the  
20 privacy and security of Class members' Personal Information. These representations were likely  
21 to deceive members of the public, including Plaintiffs and the other Class members, into believing  
22 their Personal Information was securely stored – when it was not – and that Defendants were  
23 complying with relevant law – when they were not.

24 Defendants engaged in fraudulent and deceptive acts and practices with regard to the  
25 services provided to the Class by omitting, suppressing, and concealing the material fact that the  
26 privacy and security protections for Class members' Personal Information was woefully  
27 inadequate. At the time that Class members were using Defendants' services, Defendants failed  
28 to disclose to Class members that their data security systems failed to meet legal and industry

1 standards for the protection of Class members' Personal Information. These representations likely  
2 deceived members of the public, including Plaintiffs and the Class, into believing that their  
3 Personal Information was securely stored – when it was not – and that Defendants were  
4 complying with relevant law and industry standards – when they were not.

5 As a direct and proximate result of Defendants' deceptive practices and acts, Plaintiffs  
6 and the Class were injured and lost money or property, including but not limited to the loss of  
7 their legally protected interest in the confidentiality and privacy of their Personal Information, as  
8 well as the additional losses described *supra*.

9 Defendants knew or should have known that their computer systems and data security  
10 practices were inadequately safeguarding Class members' Personal Information and that the risk  
11 of a data breach or theft was very high.

12 Defendants' actions in engaging in the above-named unlawful practices and acts were  
13 negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members  
14 of the Class.

15 Class members seek relief under Cal. Bus. & Prof. Code § 17200, *et. seq.*, including, but  
16 not limited to, restitution to Plaintiffs and the Class of money or property that Defendants may  
17 have acquired by means of their fraudulent and deceptive business practices, restitutionary  
18 disgorgement of all profits accruing to Defendants because of their fraudulent and deceptive  
19 business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc.  
20 § 1021.5), and injunctive or other equitable relief.

21 **Fourth Claim for Relief**

22 **Negligence**

23 Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation  
24 contained above as though the same were fully set forth herein.

25 Defendants owed a duty to Plaintiffs and the Class to exercise reasonable care in  
26 safeguarding and protecting their Personal Information and keeping it from being compromised,  
27 lost, stolen, misused, and or/disclosed to unauthorized parties.  
28

1 Defendants knew that the Personal Information of Plaintiffs and the Class was personal  
2 and sensitive information that is valuable to identity thieves and other criminals. Defendants also  
3 knew of the serious harms that could occur if the Personal Information of Plaintiffs and the Class  
4 was wrongfully disclosed, that disclosure was not fixed, and/or Plaintiffs and the Class were not  
5 told about the disclosure in a timely manner.

6 By being entrusted by Plaintiffs and the Class to safeguard their Personal Information,  
7 Defendants had a special relationship with Plaintiffs and the Class. Plaintiffs and the Class signed  
8 up for Defendants' services and agreed to provide their Personal Information with the  
9 understanding that Defendants would take appropriate measures to protect it and would inform  
10 Plaintiffs and the Class of any breaches or other security concerns that might call for action by  
11 Plaintiffs and the Class. But, Defendants did not. Defendants not only knew that their data security  
12 was inadequate, they also knew that they did not have the tools to detect and document intrusions  
13 or exfiltration of Plaintiffs' and the Class' Personal Information.

14 Defendants breached their duty to exercise reasonable care in safeguarding and protecting  
15 Plaintiffs' and the Class members' Personal Information by failing to adopt, implement, and  
16 maintain adequate security measures to safeguard that information and prevent unauthorized  
17 disclosure of Plaintiffs' and the other Class members' Personal Information.

18 Defendants also breached their duty to timely disclose that Plaintiffs' and the other class  
19 members' Personal Information had been, or was reasonably believed to have been, improperly  
20 obtained.

21 But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and  
22 the Class, their Personal Information would not have been compromised, stolen, and viewed by  
23 unauthorized persons.

24 Defendants' negligence was a direct and legal cause of the theft of the Personal  
25 Information of Plaintiffs and the Class and all resulting damages.

26 The injury and harm suffered by Plaintiffs and the other Class members was the  
27 reasonably foreseeable result of Defendants' failure to exercise reasonable care in safeguarding  
28 and protecting Plaintiffs' and the other class members' Personal Information. Defendants knew



1 their systems and technologies for processing and securing the Personal Information of Plaintiffs  
2 and the Class had numerous security vulnerabilities.

3 As a result of this misconduct by Defendants, the Personal Information of Plaintiffs and  
4 the Class was compromised – placing them at a greater risk of identity theft and subjecting them  
5 to identity theft – and was disclosed to third parties without their consent.

6 As a direct and proximate result of Defendants’ negligent conduct, Plaintiffs and the other  
7 Class members have suffered injury and are entitled to appropriate relief, including injunctive  
8 relief and damages.

9 **Fifth Claim for Relief**

10 **Invasion of Privacy**

11 Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation  
12 contained above as though the same were fully set forth herein.

13 Defendants’ choice-of-law provision establishes that California law applies to Plaintiffs’  
14 and all Class members’ claims.

15 The California Constitution expressly provides for a right to privacy. Cal. Const. Art. I,  
16 Sec. 1.

17 Google’s terms of use for all times relevant to this matter provided that users’ Personal  
18 Information would not be released to third parties without express consent.

19 Absent their express consent, Plaintiffs and the other Class members used Google+ under  
20 the impression that Personal Information was safeguarded and would not be provided to, or stolen  
21 by, third parties.

22 Plaintiffs and the other Class members had an interest in the protection and non-  
23 dissemination of their Personal Information that Defendants electronically stored, including the  
24 right not to have that Personal Information stolen and used for profit.

25 Absent the express consent of Google+ users, Defendants intentionally intruded on  
26 Plaintiffs’ and the other Class members’ private life, seclusion, and solitude, which is protected  
27 under the California constitution as well as common law.

1 Defendants' wrongful conduct constitutes breach of the social norms underpinning the  
2 constitutionally-protected right to privacy.

3 Defendants' wrongful conduct harmed Plaintiffs and the other Class members.

4 As a direct and proximate result of Defendants' wrongful conduct, Plaintiffs and the other  
5 Class members have suffered injury and are entitled to appropriate relief, including injunctive  
6 relief and damages.

7 **Sixth Claim for Relief**

8 **Breach of Confidence**

9 Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation  
10 contained above as though the same were fully set forth herein.

11 This claim is asserted against Defendants for breach of confidence concerning the  
12 Personal Information that Plaintiffs and the other Class members provided to Defendants in  
13 confidence.

14 At all times during Plaintiffs' and the other Class members' interactions with Defendants,  
15 Defendants were fully aware of the confidential nature of the Personal Information that Plaintiffs  
16 and Class members shared with Defendants.

17 As alleged herein and above, Defendants' relationship with Plaintiffs and Class members  
18 was governed by Google's Terms of Service and the expectation that Plaintiffs' and Class  
19 members' Personal Information would be collected, stored, and protected in confidence by  
20 Defendants, and not disclosed to unauthorized third parties.

21 Plaintiffs and the other Class members provided their respective Personal Information to  
22 Defendants with the explicit and implicit understanding that Defendants would protect and not  
23 permit that Personal Information to be disseminated to any unauthorized third parties.

24 Defendants voluntarily received in confidence Plaintiffs' and the other Class members'  
25 Personal Information with the understanding that that Personal Information would not be  
26 disclosed or disseminated to the public or any unauthorized third parties.

27 Due to Defendants' failure to prevent, detect, and stop the 2018 Data Leaks from  
28 occurring, Plaintiffs' and the other Class members' Personal Information was disclosed and

1 misappropriated to unauthorized third parties beyond their confidence and without their express  
2 permission.

3 As a direct and proximate cause of Defendants' actions and inactions, Plaintiffs and the  
4 other Class members have suffered damages.

5 But for Defendants' disclosure of Personal Information in violation of the parties'  
6 understanding that it would be held in confidence, Plaintiffs and the other Class members'  
7 Personal Information would not have been compromised, stolen, and viewed by unauthorized  
8 persons. Defendants' disclosure was a direct and legal cause of the theft of Plaintiffs' and the  
9 other Class members' Personal Information, as well as the resulting damages.

10 The injury and harm Plaintiffs and the other Class members suffered was the reasonably  
11 foreseeable result of Defendants' unauthorized disclosure of Plaintiffs' and Class members'  
12 Personal Information. Defendants knew their computer systems and technologies for accepting  
13 and securing Plaintiffs' and Class members' Personal Information had numerous security  
14 vulnerabilities, but Defendants continued to collect, store, and maintain Plaintiffs' and Class  
15 members' Personal Information without fixing the vulnerabilities, even after the First Data Leak.

16 As a result of Defendants' misconduct, Plaintiffs' and the other Class members' Personal  
17 Information was compromised – placing them at a greater risk of identity theft and subjecting  
18 them to identity theft and fraud – and disclosed to unauthorized third parties without their consent.  
19 Plaintiffs and the other Class members also suffered diminution in value of their Personal  
20 Information in that it became easily available to hackers on the dark web. Plaintiffs and the other  
21 Class members have also suffered consequential out-of-pocket losses for procuring credit freezes  
22 or protection services, identity theft monitoring, and other expenses relating to identity theft losses  
23 or protective measures.

24 **Seventh Claim for Relief**

25 **Deceit by Concealment or Omission**  
26 **(Cal. Civil Code §§ 1709, 1710)**

27 Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation  
28 contained above as though the same were fully set forth herein.

1 Defendants' choice-of-law provision establishes that California law applies to Plaintiffs'  
2 and the other Class members' claims.

3 As alleged above, Defendants knew that their data security measures were grossly  
4 inadequate by, at the absolute latest, March 2018. At that time, Defendants were on notice of the  
5 software glitch in Google+ that gave outside developers potential access to private Google+ User  
6 profile data – facts that Defendants should have already known given their previous exposures  
7 and security problems.

8 In response to all of these facts, Defendants chose to do nothing to protect Plaintiffs and  
9 the Class or warn them about the security problems. Instead, Defendants chose to conceal the  
10 breach in order to avoid public backlash and a Congressional inquiry. Defendants' actions thereby  
11 allowed third-party application developers to improperly collect the Personal Information of up  
12 to 53 million Google+ users

13 Defendants had an obligation to disclose to all Class members that their Google account(s)  
14 and Personal Information were potentially compromised by the data breach.

15 Defendants made no such disclosure following the First Data Leak. Instead, Defendants  
16 willfully deceived Plaintiffs and the Class by concealing the true facts concerning their poor data  
17 security even though they were obligated to, and had a duty to, disclose those facts.

18 Had Defendants disclosed the true facts about their poor data security, Plaintiffs and the  
19 Class would have taken measures to protect themselves. Plaintiffs and the Class justifiably relied  
20 on Defendants to provide accurate and complete information about Defendants' data security,  
21 which Defendants failed to do.

22 Independent of any representations made by Defendants, Plaintiffs and the Class  
23 justifiably relied on Defendants to provide a service with at least minimally adequate security  
24 measures and to disclose facts undermining that reliance.

25 Rather than disclosing to Plaintiffs and the Class that the Google+ platform had been  
26 compromised by the breach and that Personal Information had been improperly exposed in the  
27 First Data Leak, Defendants continued with business as usual, concealing information relating to  
28 the inadequacy of their security measures from Plaintiffs and the Class.

1 While Defendants represented that they had fixed the vulnerability after the First Data  
2 Leak, they continued to conceal information relating to the inadequacy of their security measures,  
3 which resulted in the Second Data Leak.

4 These actions are “deceit” under Cal. Civil Code § 1710 in that they are the suppression  
5 of a fact, by one who is bound to disclose it, or who gives information of other facts which are  
6 likely to mislead for want of communication of that fact.

7 As a result of this deceit by Defendants, they are liable under Cal. Civil Code § 1709 for  
8 “any damage which [Plaintiffs and the Class] thereby suffer[.]”

9 As a result of this deceit by Defendants, the Personal Information of Plaintiffs and the  
10 Class were compromised, and their Personal Information was disclosed to third parties without  
11 their consent. Plaintiffs and the other Class members also suffered diminution in value of their  
12 Personal Information. Plaintiffs and the Class have also suffered consequential out-of-pocket  
13 losses for procuring credit freeze or protection services, identity theft monitoring, and other  
14 expenses relating to identity theft losses or protective measures.

15 Defendants’ deceit, as alleged herein, is fraud under Civil Code § 3294(c)(3) in that it was  
16 a deceit or concealment of a material fact known to Defendants conducted with the intent on the  
17 part of Defendants of depriving Plaintiffs and the Class of “legal rights or otherwise causing  
18 injury.” As a result, Plaintiffs and the Class are entitled to punitive damages against Defendants  
19 under Civil Code § 3294(a).

20 **Eighth Claim for Relief**

21 **Breach of Contract**

22 Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation  
23 contained above as though the same were fully set forth herein.

24 At all relevant times, Defendants and Plaintiffs mutually assented to, and therefore were  
25 bound by the version of Google’s Terms of Service and Privacy Policy (collectively, the  
26 “Contracts”) that was operative at the time each of the Plaintiffs and other Class members joined  
27 Google+.

1 Throughout the Class Period, Defendants affirmatively stated in the Contracts that they  
2 would not disclose Google+ users' Personal Information without consent and/or notice.  
3 Defendants further represented in the Contracts that they would utilize sufficient data security  
4 protocols and mechanisms to protect Google+ users' Personal Information.

5 None of the Contracts informed and obtained Users' meaningful and lawfully-obtained  
6 consent to share their content and information with third parties without their consent, or disclosed  
7 that such information would be shared if their contacts entered into an agreement which permitted  
8 third parties to collect their contacts' information.

9 Thus, per the provision above, the Contracts did not authorize Defendants to share  
10 Plaintiffs' and the other Class members' Personal Information with third parties without their  
11 consent.

12 Plaintiffs and the other Class members fully performed their obligations under the  
13 Contracts.

14 Defendants breached the Contracts they entered into with Plaintiffs and the other Class  
15 members by failing to safeguard and protect their Personal Information, and improperly allowing  
16 third parties to access their Personal Information without their consent.

17 As a direct and proximate result of Google's breaches of the Contracts between  
18 Defendants and Plaintiffs and the other Class members, Plaintiffs and the other Class members  
19 sustained actual losses and damages, as described in detail *supra*. Plaintiffs and the other Class  
20 members suffered injury-in-fact and lost money or property. In addition, Plaintiffs and the other  
21 Class members' Personal Information was taken and is in the hands of those who will use it for  
22 their own advantage, or is being sold for value, making it clear that the hacked information is of  
23 tangible value.

1 **Ninth Claim for Relief**

2 **Breach of Implied Covenant of Good Faith and Fair Dealing**  
3 **(In the Alternative)**

4 Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation  
5 contained above as though the same were fully set forth herein. This claim is pleaded in the  
6 alternative to the claim for breach of contract.

7 Defendants' choice-of-law provision establishes that California law applies to Plaintiffs'  
8 and the other Class members' claims.

9 Under California law, there is in every contract or agreement an implied promise of good  
10 faith and fair dealing. Such a duty is read into contracts and functions as a supplement to the  
11 express contractual covenants, in order to prevent a transgressing party from engaging in conduct  
12 which (while not technically transgressing the express covenants) frustrates the other party's  
13 rights to the benefit of the contract. Thus, any claim on the part of Defendants that they were  
14 technically permitted to allow the collection and transmittal of Plaintiffs' and the other Class  
15 members' Personal Information must be read in the context of, and give way to, their rights to the  
16 benefit of the contract, including the terms strictly delimiting such activity.

17 Defendants made specific representations to Plaintiffs and the other Class members  
18 regarding Defendants' protection of Users' Personal Information in their Privacy Policy that was  
19 operative at the time each of the Plaintiffs and other Class members joined Google+.

20 A covenant of good faith and fair dealing attaches to Defendants' Privacy Policy.

21 Throughout the Class Period, Defendants affirmatively stated in the Privacy Policy that  
22 they would not disclose Google+ users' Personal Information without their consent and/or notice.  
23 Defendants further represented in the Privacy Policy that they would utilize sufficient data  
24 security protocols and mechanisms to protect Google+ users' Personal Information.

25 Plaintiffs and the other Class members fully performed their obligations under the  
26 contractual provisions in the Privacy Policy.

27 Under the terms of the Privacy Policy, Plaintiffs and the other Class members were  
28 entitled to receive the benefits promised to them by Defendants, including that Defendants would

1 protect their Personal Information, would not disclose their Personal Information to third parties  
2 without their consent, and would keep their Personal Information secure.

3 Defendants were uniquely able to control the rights of their Users, including Plaintiffs and  
4 the other Class members, concerning their privacy, ownership, and control of their content and  
5 information, and whether that content and information would be provided to third parties without  
6 their consent.

7 Defendants surreptitiously took measures to frustrate and undercut Plaintiffs' and the  
8 other Class members' contractual rights concerning their privacy, ownership, and control over  
9 their Personal Information, and whether their content and information would be provided to third  
10 parties without their consent. By doing so, Defendants deprived Plaintiffs and the other Class  
11 members of the benefits under their contracts with Defendants, including the Privacy Policy.

12 As a direct and proximate result of Defendants' breaches of their duty of good faith and  
13 fair dealing, Plaintiffs and the other Class members sustained actual losses and damages, as  
14 described in detail *supra*. Plaintiffs and the other Class members suffered injury-in-fact and lost  
15 money or property. In addition, their Personal Information was taken and is in the hands of those  
16 who will use it for their own advantage, or is being sold for value, making it clear that the hacked  
17 information is of tangible value.

18 **PRAYER FOR RELIEF**

19 WHEREFORE, Plaintiffs, individually and on behalf of the other Class members,  
20 respectfully request that this Court enter an Order:

21 a. Certifying the United States Class, appointing Plaintiffs as Class Representatives,  
22 and appointing the law firms of Franklin D. Azar & Associates and Morgan & Morgan Complex  
23 Litigation Group as Class Counsel;

24 b. Finding that Defendants' conduct was negligent, deceptive, unfair, and unlawful  
25 as alleged herein;

26 c. Enjoining Defendants from engaging in further negligent, deceptive, unfair, and  
27 unlawful business practices as alleged herein;



1 d. Awarding Plaintiffs and the other Class members actual, compensatory, and  
2 consequential damages;

3 e. Awarding Plaintiffs and the other Class members statutory damages and penalties,  
4 as allowed by law;

5 f. Awarding Plaintiffs and the other Class members restitution and disgorgement;

6 g. Requiring Defendants to provide appropriate credit monitoring services to  
7 Plaintiffs and the other class members;

8 h. Awarding Plaintiffs and the other Class members punitive damages;

9 i. Awarding Plaintiffs and the other Class members pre-judgment and post-judgment  
10 interest;

11 j. Awarding Plaintiffs and the other Class members reasonable attorneys' fees costs  
12 and expenses, and;

13 k. Granting such other relief as the Court deems just and proper.

14 **JURY TRIAL DEMANDED**

15 Plaintiffs demand a trial by jury of all claims in this Consolidated Class Action Complaint  
16 so triable.

17 Dated: February 6, 2019

18 /s/ Ivy T. Ngo

Ivy T. Ngo (249860)

Franklin D. Azar & Associates, P.C.

*Counsel for Plaintiffs Olson and Pinkowski*

John A. Yanchunis (*pro hac vice*)

Jonathan B. Cohen (*pro hac vice*)

Ryan J. McGee (*pro hac vice*)

Morgan & Morgan

Complex Litigation Group

Clayeo C. Arnold (65070)

Clayeo C. Arnold, P.C.

*Counsel for Plaintiffs Matic and Harris*