

MARK BRNOVICH
ATTORNEY GENERAL
Firm State Bar No. 14000

Joseph A. Kanefield (State Bar No. 15838)
Brunn W. Roysden III (State Bar No. 28698)
Oramel H. Skinner (State Bar No. 032891)
Michael S. Catlett (State Bar No. 025238)
Christopher Slood (State Bar No. 034196)

Assistant Attorneys General
2005 N. Central Ave.
Phoenix, Arizona 85004
Telephone: (602) 542-8958
Beau.Roysden@azag.gov
O.H.Skinner@azag.gov
Michael.Catlett@azag.gov
Christopher.Slood@azag.gov
ACL@azag.gov

[Additional Counsel on Signature Page]

Attorneys for Plaintiff
State of Arizona ex rel. Mark Brnovich,
Attorney General

THE SUPERIOR COURT OF THE STATE OF ARIZONA
IN AND FOR THE COUNTY OF MARICOPA

STATE OF ARIZONA, *ex rel.* MARK
BRNOVICH, Attorney General,

Plaintiff,

v.

GOOGLE LLC, a Delaware limited liability
company,

Defendant.

) Case No:

) **COMPLAINT FOR INJUNCTIVE AND**
) **OTHER RELIEF**

) Assigned to the Hon: _____

) (Non-classified; Consumer Fraud)

) REQUEST ASSIGNMENT TO COMPLEX
) COURT

) **JURY TRIAL DEMANDED**
) _

TABLE OF CONTENTS

	<i>Page</i>
I. INTRODUCTION	1
II. PARTIES, JURISDICTION, AND VENUE	5
A. Plaintiff	5
B. Defendant.....	5
C. Jurisdiction and Venue.....	5
III. FACTUAL ALLEGATIONS	6
A. Google Engages in Acts and Practices In Connection With the Sale and Advertisement of Merchandise In And Affecting The State of Arizona	6
B. Overview of Google’s Many Location-Related Settings.....	10
C. Google Admits Its Location-Related Settings Are a “Mess” That Mislead and Deceive	12
1. Google Misleads and Deceives Users Through Its Location History and Web & App Activity Settings.	14
2. Google Misleads Users Into Sharing Their Location Via Its Misleading WiFi Scanning and WiFi Connectivity Settings.....	19
D. Google Uses Its Users’ Locations Even When Users Turn Off the Relevant Permissions	21
1. Google Shares Location with Apps That Users Explicitly Forbid From Using Location.....	21
2. Google Collects Location Data Even When Users Turn Their Device Location Off.....	24
3. Google Serves Personalized Ads Based on User Location Even When Users Turn Off Personalization	26
E. Google Automatically Changes the State of Permissions Without Notifying Users.....	27
F. Google Changes the Android User Interface to Increase Location [REDACTED] at the Expense of User Choice and Consent	29

TABLE OF CONTENTS (cont.)

	<i>Page</i>
G. Google Misleads and Deceives Users Regarding Its Deletion of Their Location Information	33
H. Google Has Engaged In Willful Violations Of The Arizona Consumer Fraud Act	34
IV. ARIZONA’S INVESTIGATION INTO GOOGLE’S UNFAIR AND DECEPTIVE ACTS AND PRACTICES	36
V. CLAIM FOR RELIEF	41

1 Plaintiff State of Arizona *ex rel.* Mark Brnovich, Attorney General, for its Complaint against
2 Defendant Google LLC (“Google”), alleges as follows:

3 **I. INTRODUCTION**

4 1. This case concerns Google’s widespread and systemic use of deceptive and unfair
5 business practices to obtain information about the location of its users, including its users in Arizona,
6 which Google then exploits to power its lucrative advertising business.

7 2. The average consumer likely associates Google with its popular products and services
8 including Google Search, Google Maps, the Google Chrome browser, YouTube, and Android, but these
9 products and services are not Google’s principal business.

10 3. From a revenue perspective, Google’s principal business is selling advertisements and
11 displaying them to the users of Google’s products and services.

12 4. This reality is reflected by Google’s financials. In 2019, for example, over 80% of
13 Google’s massive revenues—\$135 billion out of \$161 billion total—were generated by advertising.

14 5. Google’s advertising revenues are driven by the company’s collection of detailed
15 information about its users, including information about where those users are located. Location
16 information allows Google to enable advertisers to target users in a specific geographic location, and it
17 also allows Google to validate the effectiveness of ads by reporting to advertisers how often online ad
18 clicks are converted into real-world store visits.

19 6. Given the lucrative nature of Google’s advertising business, which depends on having
20 detailed location information about its users, Google goes to great lengths to collect its users’ location
21 information. Indeed, according to Harvard Professor Shoshana Zuboff, “Google’s proprietary methods
22 enable it to surveil, capture, expand, construct and claim behavioral” data, “including data that users
23 intentionally choose not to share.” *See* SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM* 80
24 (2019). In this regard, individual users of Google products and services are the targets of a sweeping
25 surveillance apparatus designed to collect their behavioral data *en masse*, including data pertaining to
26 user location. *Id.* at 8–10.

1 7. The tactics Google deploys to surveil its users' locations—including users in Arizona—
2 include willfully deceptive and unfair acts and practices within the meaning of the Arizona Consumer
3 Fraud Act.

4 8. One aspect of Google's deceptive conduct came into public view with the August 2018
5 publication of an Associated Press article entitled, "Google tracks your movements, like it or not." The
6 article discusses Google's Location History service, which enables users to view where they have been.
7 Google provided users the ability to disable Location History. At the same time, Google told users that
8 "with Location History off, the places you go are no longer stored." But the AP article revealed that this
9 statement was blatantly false—even with Location History off, Google would surreptitiously collect
10 location information through other settings such as Web & App Activity and use that information to sell
11 ads.

12 9. Arizona's investigation has revealed that Google's deceptive and unfair conduct extends
13 well beyond its false Location History disclosure. Indeed, such acts and practices pervade Google's
14 seemingly relentless drive to (i) collect as much user location information as possible and (ii) make it
15 exceedingly hard for users to understand what is going on with their location information, let alone opt-
16 out of this morass. This is demonstrated by the following examples:

- 17 a. As described in the AP article, with Location History off, Google continues to collect
18 location information through Web & App Activity—a title that reveals nothing about
19 the setting's connection to harvesting location data. Through Web & App Activity,
20 Google logs information relating to a user's activity on Google websites and apps,
21 such as conducting a search on Google Search. A critical component of this
22 information from Google's perspective is a user's location. Nevertheless, until early-
23 to mid-2018, Google's disclosures during account creation made no mention of the
24 fact that location information was collected through Web & App Activity, which is
25 defaulted to "on." And even today the title itself is misleading by failing to disclose
26 any connection to location.
- 27 b. Devices running the Android operating system have a device-level location setting.
28 Google tells users that "the types of data we collect depend in part on your device and

1 account settings. For example, you can turn your Android device’s location on or off
2 using the device’s settings app.” A reasonable conclusion from this disclosure is that
3 “off means off”—*i.e.*, that Google simply will not collect and exploit user location
4 information when a device’s location setting is turned off. But that is not true.

5 [REDACTED]
6 [REDACTED]
7 [REDACTED]
8 [REDACTED]
9 [REDACTED]
10 [REDACTED]

- 11 c. Google’s WiFi settings mislead users about Google’s collection and use of location
12 information. There are two relevant settings—WiFi scanning and WiFi connectivity.
13 Only the WiFi scanning setting is presented within location settings, which would
14 lead a reasonable user to believe that turning it off would result in Google no longer
15 discerning a user’s location through WiFi scans. [REDACTED]

16 [REDACTED]
17 [REDACTED]

- 18 d. In recent versions of Android, individual Google apps ask for the user’s permission to
19 use their location data. A reasonable inference is that, if the user denies this app-level
20 permission to an app, that app will not be able to use the user’s location. But this is
21 not true—Google apps that are denied permission by the user can still obtain location
22 information from other Google apps and products that *have* been granted permission.
- 23 e. The [REDACTED] deception also manifests in ads personalization. As explained
24 above, Google serves personalized ads to its users based in part on information
25 Google has about a user’s location. Google purports, however, to allow users to opt
26 out of ads personalization by turning off a setting of that name (“GAP”). But contrary
27 to what a reasonable user would expect, turning ads personalization off does not stop
28 Google from presenting ads based on a user’s location. Rather, Google will instead

1 simply present ads based on more general location information. Moreover, Google
2 has a *second* ads service (“DoubleClick”) through which it serves ads on third-party
3 websites. The setting that controls DoubleClick’s service of location-based ads is in a
4 completely separate user interface from the GAP setting. And, like the GAP setting, if
5 a user turns off the DoubleClick setting, Google will still target the user with
6 DoubleClick ads based on the user’s coarse location. Even worse, the DoubleClick
7 setting has no effect on the GAP setting, and vice versa. Thus, a user who thought she
8 had opted out of receiving ads based on her location is wrong on two counts: Google
9 still serves her location-based ads (based on her coarse location) via that same
10 service, and Google also serves location-based ads (based on more precise location
11 signals) via the other service.

- 12 f. Users are more likely to disable their device’s location setting if they are readily
13 offered such a setting. [REDACTED]

14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]

20 10. Users, including in Arizona, have come to rely on Google’s products and services on a
21 daily basis. At the same time, through these deceptive and unfair acts and practices, Google makes it
22 impractical if not impossible for users to meaningfully opt-out of Google’s collection of location
23 information, should the users seek to do so.

24 11. Google has engaged in these deceptive and unfair acts and practices with the purpose of
25 enhancing its ability to collect and profit from user location information. And profited it has, to the tune
26 of over \$134 billion in advertising revenue in 2019 alone. On information and belief, hundreds of
27 millions of dollars of these advertising revenues were generated from ads presented to millions of users
28 in the State of Arizona.

12. Arizona brings this action to put a stop to Google’s deceptive and unfair acts and practices; force Google to disgorge all profits, gains, gross receipts, and other benefits obtained for the period of time when it engaged in any unlawful practice; recover restitution for Arizona consumers; and impose civil penalties for Google’s willful violations of the Arizona Consumer Fraud Act.

II. PARTIES, JURISDICTION, AND VENUE

A. Plaintiff

13. Plaintiff is the State of Arizona, *ex rel.* Mark Brnovich, Attorney General (“Arizona”). The Attorney General is authorized to bring this action in the name of the State under A.R.S. § 44-1521 *et seq.*

B. Defendant

14. Google LLC is a Delaware limited liability company with its principal place of business at 1600 Amphitheatre Parkway, Mountain View, California.

15. Google is a technology company that specializes in Internet-related products and services, which include online advertising technologies, search, cloud computing, and other software and hardware.

16. Google markets and advertises its products and services throughout the United States, and on information and belief the number of Google’s Arizona users is in the millions.

17. Google touts that “[i]n 2019, [it] helped provide \$6.22 billion of economic activity for 28,900 Arizona businesses, publishers, nonprofits, creators, and developers.”¹

18. At all relevant times Google acted with the knowledge and understanding that the activities described in this Complaint would affect users of Google’s products and services throughout the United States, including in the State of Arizona.

C. Jurisdiction and Venue

19. This Court has subject-matter jurisdiction over this matter, including under Article VI, Section 14 of the Arizona Constitution.

¹ <https://economicimpact.google.com/state/az/>.

1 20. This Court may enter appropriate orders both prior to and following a determination of
2 liability pursuant to the Arizona Consumer Fraud Act, A.R.S. § 44-1521, *et seq.*

3 21. Venue is proper in Maricopa County pursuant to A.R.S. § 12-401.

4 III. FACTUAL ALLEGATIONS

5 A. **Google Engages in Acts and Practices In Connection With the Sale and Advertisement of** 6 **Merchandise In And Affecting The State of Arizona**

7 22. Google's deceptive and unfair acts and practices alleged herein are in connection with the
8 sale or advertisement of merchandise for several reasons, including the following:

- 9 a. Google sells its own Android devices to consumers in Arizona, and those devices
10 both run Google's proprietary forks of the Android operating system and come
11 preloaded with several Google apps. As part of activating and setting up their phones
12 after purchasing them for consideration, consumers purportedly "consent" to the
13 settings described herein that result in Google's collection of location data. Google's
14 acts, practices, representations, and omissions regarding those settings, including
15 during setup, are thus in connection with the sale of Google's Android phones.
- 16 b. Google creates both software that is part of the Android operating system (*i.e.*,
17 proprietary forks) and also Google apps that it causes to be included on Android
18 devices sold by other manufacturers to consumers in Arizona. As part of activating
19 and setting up those devices after purchasing them for consideration, consumers
20 purportedly "consent" to the settings described herein and Google's collection of
21 location data. Google's acts, practices, representations, and omissions regarding those
22 settings are thus in connection with the sale of certain third-party Android phones.
- 23 c. Google advertises the devices and software described in (a) and (b), *supra*, to
24 consumers. Google also advertises software that runs on other operating systems
25 (*e.g.*, iOS). Google's acts, practices, representations, and omissions when advertising
26 devices and software are thus in connection with the advertisement of merchandise.
- 27 d. Google sells ad placements (*i.e.*, "merchandise") to third parties for consideration
28 (Google's principal business), which advertisements are powered by the fruits of the

1 deceptive and unfair acts and practices alleged herein relating to collection of user
2 location data. Google's acts, practices, representations, and omissions when selling ad
3 placements to purchasers of such ad placements are thus in connection with the sale
4 of merchandise.

5 e. Google markets (*i.e.*, advertises) its ad business to potential and actual buyers of its
6 advertisements. Google's acts, practices, representations, and omissions when
7 marketing its ad business to potential buyers of ads are thus in connection with the
8 advertisement of merchandise.

9 f. Google's unfair and deceptive acts and practices lead to targeted advertisements to
10 Arizona consumers based on user location data, and Google also tracks "conversions"
11 of such ads to physical store visits. Google's acts, practices, representations, and
12 omissions when serving advertisements to consumers on behalf of the third parties
13 who have purchased such ads, and tracking conversions from such ads, are thus in
14 connection with the advertisement and sale of merchandise by those third parties.

15 23. Google's own "device" offerings include smartphones in the Google Pixel and Google
16 Nexus families of phones. For example, Google has sold and/or advertised the following devices:

- 17 • Google Pixel family
 - 18 ○ Pixel C (released 2015)
 - 19 ○ Pixelbook (released 2017)
 - 20 ○ Pixel Slate (released 2018)
 - 21 ○ Pixel 1 (released 2016)
 - 22 ○ Pixel 2 (released 2017)
 - 23 ○ Pixel 3 (released 2018)
 - 24 ○ Pixel 4 (released 2019)
- 25 • Google Nexus family
 - 26 ○ Nexus One (released January 2010)
 - 27 ○ Nexus S (released December 2010)
 - 28 ○ Galaxy Nexus (released November 2011)

- Nexus 4 (released November 2012)
- Nexus 5 (released November 2013)
- Nexus 6 (released November 2014)
- Nexus 5X (released October 2015)
- Nexus 6P (released September 2015)

24. On information and belief, Google, through agreements with third-party manufacturers such as Samsung and carriers such as Verizon, causes its Android software and apps to be pre-installed on phones and devices that are sold to consumers in Arizona, and which consumers “consent” to as part of the setup process after buying such phones and devices.

25. Google also sells, advertises and/or otherwise offers for consideration various software services to Arizona consumers, either directly or indirectly. For example, Google’s software offerings include the Android operating system (“Android”), Google-authored apps (“Google apps”), Google Accounts, and Google web browsers, such as Chrome. In its privacy policy, Google defines its services as including (i) “Google apps, sites, and devices, like Search, YouTube, and Google Home,” (ii) “Platforms like the Chrome browser and Android operating system,” and (iii) “Products that are integrated into third-party apps and sites, like ads and embedded Google Maps.” Ex. 72 (GOOG-GLAZ-00000715) at 715.

26. In consideration for use of Google’s software products and devices, Google collects, *inter alia*, “information about your location when you use our services, which helps us offer features like driving directions for your weekend getaway or showtimes for movies playing near you.” *Id.* at 718. Google tells consumers it must collect this data “to deliver our services,” “ensure our services are working as intended,” “develop new services,” and “show you personalized ads.” *Id.* at 719. Google’s [REDACTED] confirmed that Google’s products, such as Search and Maps, are only free because Google is able to display ads to users of these products. 3/6/2020 [REDACTED] EUO Tr. at 368:1–369:17; *see also id.* at 370:4–24 (understanding Google’s “products” and “services” to be interchangeable, and giving Google Maps and Search as examples); 2/28/2020 [REDACTED] EUO Tr. at 327:17–18 (“‘Service’ and ‘product’ are used interchangeably at Google.”).

1 27. Google also collects users’ location data from its Android operating system. Google’s
2 Android is a popular smartphone operating system in the United States. Beyond smartphones, Android
3 also runs on various other types of devices, such as tablets, televisions, home appliances, and fitness
4 trackers. Android is also the operating system that is installed on all of Google’s own smartphone
5 devices.

6 28. Android is technically an open-source software, meaning that anyone can take the
7 Android source code, modify it in any way, and install it on a compatible device. Such modifications are
8 called “forks” of Android.

9 29. While third-party smartphone manufacturers (“OEMs”) are technically free to pre-install
10 any Android fork on their phones, a “vast majority” of Android phones sold in the United States install
11 Google’s version of Android. 2/28/2020 [REDACTED] EUO Tr. at 448:9–17.

12 30. Google causes its preferred versions of Android to be pre-installed on many smartphones,
13 and forbids OEMs from pre-installing any Google apps (such as Search or Maps) on other versions of
14 Android. Google has a large incentive to do this: its own version of Android contains Google Mobile
15 Services (“GMS”), which makes it easier for Google to collect location information from users.² Indeed,

16 [REDACTED]

17 [REDACTED] 2/28/2020 [REDACTED] EUO Tr. at 444:8–445:9; *see also* Ex. 201 (GOOG-
18 GLAZ-00149241) [REDACTED]

19 [REDACTED]

20 [REDACTED]

21 [REDACTED]

22 31. The location data that Google collects—from any source—adds an enormous amount of
23 value to Google’s advertising offerings. As explained above, Google is primarily an advertising
24

25 _____
26 ² GMS “is a collection of apps and services that an OEM is required to have to . . . license Android.”
27 9/25/2019 [REDACTED] EUO Tr. at 139:1–6. That collection includes “software libraries, APIs, and other
28 software, including YouTube, Maps, and Google Play.” *Id.* at 138:4–10; *see also*
<https://www.android.com/gms/> (GMS is “a collection of Google applications and APIs that help support
functionality across devices. These apps work together seamlessly to ensure your device provides a great
user experience right out of the box.”).

company—in 2019, Google made \$161 billion in revenue, of which \$135 billion (84%) came from advertising.

32. For instance, one of Google’s advertising offerings is called Store Visits. With this product, Google is able to inform its advertisers how effective their ads are by informing them when viewing an ad online drives a physical store visit. Google is only able to do this by collecting massive amounts of user location data.

B. Overview of Google’s Many Location-Related Settings

33. As explained further below, Google’s products and services include a web of interrelated settings that relate to Google’s collection of a user’s location-related information. These settings, individually and collectively, are in many cases deceptive, and their use by Google to collect users’ location data is unfair and deceptive.

34. The settings fall into three categories: (i) account-level, (ii) device-level, and (iii) app-level. In many instances, these settings are defaulted to enable collection of user location data, unless the user affirmatively disables the settings. In many instances, the settings can conflict with one another, but Google collects user location data regardless. In many instances, locating and/or understanding the appropriate setting is extraordinarily difficult and confusing.

35. Device-level settings are those that are specific to a given hardware device, like a smartphone or tablet. A user may have a single Google Account that is used on multiple devices. For example, a device-level location setting may be turned off for that user’s Pixel phone, but turned on for the user’s tablet.

36. Account-level settings are those that apply to a user’s entire Google Account and are propagated to all devices associated with that Google Account.

37. App-level settings are settings specific to a particular app. An app-level setting can relate to a Google app, such as Google Maps. An app-level setting can also apply to third-party apps that are installed on an Android device.

38. Although these various settings have changed over time (including recently), the following table includes some of the relevant settings today:

Setting Name	Category	Description
Device Location (or Location Master)	Device-level setting	This setting is the main location setting on a device and controls whether a device's location setting is on. When it is on, GPS is used to obtain a user's location.
Google Location Accuracy (formerly known as Google Location Services) ("GLA")	Device-level setting	GLA is a network-based location service that uses signals other than GPS to obtain a user's location. Specifically, GLA obtains location from WiFi, cellular networks and a variety of sensors (barometer, gyroscope, magnetometer, and accelerometer).
Usage & Diagnostics	Device-level setting	When turned on, this setting purportedly helps Google improve the Android operating system ("OS"). It collects the user's IP addresses, which can be used to infer location.
WiFi Scanning	Device-level setting	This setting allows apps and services to be able to obtain WiFi scans even when the WiFi setting is off. Google can use WiFi scans to augment the location information it obtains.
Bluetooth Scanning	Device-level setting	This setting allows apps and services to be able to obtain Bluetooth scans even when the Bluetooth setting is off. Google can use Bluetooth scans to augment the location information it obtains.
App-level location permission	App-level setting	When on, this setting gives an app permission to access the location of the corresponding device's location.
Location History ("LH")	Account-level setting	When on, this setting allows Google to build a comprehensive list of everywhere the user goes with their devices that also have Location Reporting (explained below) turned on, even when the user is not using a Google service. LH also powers a product called Timeline, which is a user-facing product in which users can view and delete the places they have been.
Location Reporting	Device-level setting	This is a sub-setting of LH. When on, it enables the device to report location via Google's Location History setting.
Web & App Activity ("WAA")	Account-level setting	When this setting is on, Google saves a user's Google activity. For example, when a user uses Google Search or Google Maps to search for "restaurants near me," Google collects the search term as well as information about that activity, such as a user's location and IP address. WAA also powers a product called My Activity, which is a user-facing product in which users can view and delete their WAA.
Supplemental Web & App Activity ("sWAA")	Device- and account-level setting	This is a sub-setting to WAA. When it is on, it allows a user's Chrome history and activity from websites and apps that use Google services to be collected.
Google Location Sharing	Account-level setting	This setting allows a Google Account holder to share his real-time location with others.

Setting Name	Category	Description
Google Ad Personalization (“GAP”)	Account-level setting	When off, this setting purports to prevent Google from targeting a user with ads based on the user’s location.

See, e.g., Ex. 202 (Google’s Consolidated Final Responses to the First, Second, and Third CIDs (“Google’s Responses to CIDs 1–3”)) at 17–20 (4/17/2019 response to DFI 7 from the First CID); Ex. 203 (GOOG-GLAZ-00076994) at 7000–002; 9/25/2019 [REDACTED] EUO Tr. at 83:11–89:14.

39. Location History in particular is central to Google’s revenue stream. Among other things,

[REDACTED]

[REDACTED]

[REDACTED] Ex. 204 (GOOG-GLAZ-00085882) at 882.

40.

[REDACTED]

[REDACTED] *Id.*

41.

[REDACTED]

[REDACTED] *Id.*

C. Google Admits Its Location-Related Settings Are a “Mess” That Mislead and Deceive

42. The array of location-related settings described above misleads and deceives users of Google’s products into believing that they are not sharing location information when they actually are. Their use by Google also constitutes unfair acts and practices.

43. Indeed, for years, Google has known that the user experience they designed misleads and deceives users. The evidence obtained from within Google—such as internal emails, presentations, and memos—is overwhelming in this regard. Ex. 56 (GOOG-GLAZ-00002914) (October 2014 presentation regarding “Simplifying Location History Settings (on Android)”); Ex. 205 (GOOG-GLAZ-00055259) at 259 [REDACTED]

44. Google’s own employees have clearly identified the problem:

-

[REDACTED]

[REDACTED] Ex. 206 (GOOG-GLAZ-00055452) at 452.

-

“The current UI feels like it is designed to make things possible, yet difficult enough that people won’t figure it out.” Ex. 207 (GOOG-GLAZ-00077898) at 899.

1 • “Some people (including even Googlers) don’t know that there is a global switch and a
2 per-device switch.” Ex. 208 (GOOG-GLAZ-00055552) at 553.

3 • [REDACTED]
4 [REDACTED] Ex. 209 (GOOG-GLAZ-00057477) at 477.

5 • [REDACTED]
6 [REDACTED] Ex. 210
7 (GOOG-GLAZ-00057940) at 940.

8 • [REDACTED]
9 [REDACTED] 9/25/2019
10 [REDACTED] EUO Tr. at 275:9–277:6.

11 • [REDACTED]
12 [REDACTED]
13 [REDACTED] Ex. 211 (GOOG-GLAZ-
14 00017790) at 790–91.

15 • [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED] Ex. 212 (GOOG-GLAZ-00161717) at 717.

19 • [REDACTED]
20 [REDACTED] Ex. 213 (GOOG-GLAZ-00028891) at 896–97.

21 • [REDACTED]
22 [REDACTED] Ex. 214 (GOOG-GLAZ-00101814) at 14.

23 • “So our messaging around [location tracking] is enough to confuse a privacy focused
24 Google-SWE. That’s not good.” Ex. 215 (GOOG-GLAZ-00163209) at 213.

25 45. Even top-level Google employees do not understand under what conditions Google
26 collects location data. *See, e.g.*, Ex. 43 (GOOG-GLAZ-00031017) at 019–23 [REDACTED]
27 [REDACTED] at the time (9/25/2019 [REDACTED] EUO Tr. at 49:17–50), expressing confusion regarding
28 how three different location-related settings interact).

1 46. Though Google has published a variety of documentation for users, [REDACTED]
2 [REDACTED] See Ex. 216 (GOOG-GLAZ-
3 00078009) at 037 [REDACTED]
4 [REDACTED]
5 [REDACTED] 059 [REDACTED]
6 [REDACTED]
7 [REDACTED] Ex. 214 (GOOG-GLAZ-
8 00101814) at 814 [REDACTED]

9 47. The result of this complex web of settings and purported “consents” is an “overall
10 mess . . . with regards to data collection, consent and storage” (Ex. 209 (GOOG-GLAZ-00057477) at
11 478) that misleads users into handing over their location data to Google.

12 48. Thus, though Google claims to have obtained consent to collect and store its users’ data,
13 that consent is based on a misleading user interface, as well as other unfair and deceptive acts and
14 practices.

15 49. [REDACTED]
16 [REDACTED] See Ex. 217 (GOOG-GLAZ-00046967) at 968 [REDACTED]
17 [REDACTED] And Google even collects data without
18 user consent, as explained more fully below. *E.g.*, Ex. 218 (GOOG-GLAZ-00114667) at 667–68
19 [REDACTED]
20 [REDACTED]

21 **1. Google Misleads and Deceives Users Through Its Location History and Web & App**
22 **Activity Settings**

23 50. While Google obtains its users’ location information through numerous settings and
24 products, two of the primary settings through which Google misleads, deceives, and conceals material
25 facts from users are Location History and Web & App Activity.

1 51. On August 13, 2018, the AP published an exclusive report titled “Google tracks your
2 movements, like it or not” that publicly exposed this deception.³ The article explained how Google
3 “records your movements even when you explicitly tell it not to.”

4 52. Until the AP article was published, Google represented on its public help page regarding
5 Location History that “You can turn off Location History at any time. With Location History off, the
6 places you go are no longer stored.” Ex. 8 (old Google help page titled “Manage or delete your Location
7 History”); *see also* 7/11/2019 [REDACTED] EUO Tr. at 29:10–31:2.

8 53. But that was not true. Even with Location History off, Google still collected and stored
9 location data via (at least) its Web & App Activity setting. Thus, for example, a user who had Location
10 History off and looked up the weather where he lived or searched the web with Google’s Search app
11 would still unknowingly send Google his location.

12 54. The day the AP story was published, Google turned into crisis mode and held a self-
13 styled “Oh Shit” meeting in reaction to the story. Ex. 20 (GOOG-GLAZ-00001521) at 523; Ex. 23
14 (GOOG-GLAZ-00001371) at 373. Discussed at that meeting were “where we are in terms of fixing
15 ‘location history’” and how to simplify Google’s location settings. Ex. 20 (GOOG-GLAZ-00001521) at
16 523.

17 55. Google closely monitored the AP story in a detailed media report which tracked, among
18 other statistics, the volume of mentions of the story on social media (3 days later, that number was
19 62,000 (not including Facebook mentions)), hour-by-hour mentions, the list of media covering the story,
20 and even tweets from specific individuals like politicians and reporters. Ex. 219 (GOOG-GLAZ-
21 00001422).

22 56. Even Google’s [REDACTED] was directly involved in the aftermath of the
23 publication of the AP article. Mr. [REDACTED] called a [REDACTED] meeting to get “constant” updates on the
24 issues covered by the article from his direct reports, including from [REDACTED], the [REDACTED]
25 [REDACTED] 3/6/2020 [REDACTED] EUO Tr. at 176:10–178:11.

26
27
28 ³ <https://apnews.com/828aefab64d4411bac257a07c1af0ecb/AP-Exclusive:-Google-tracks-your-movements,-like-it-or-not>.

1 57. [REDACTED]

2 [REDACTED]
3 [REDACTED]
4 Ex. 24 (GOOG-GLAZ-00001458) at 464–65. [REDACTED]
5 [REDACTED]

6 [REDACTED]. *Id.* at 466.

7 58. After the AP story was published, Google updated its help page to remove the disclosure
8 “With Location History off, the places you go are no longer stored.” Ex. 11 (GOOG-GLAZ-00000927).
9 In other words, Google attempted to “fix” this particular deception only when it was caught.

10 59. Testimony from Google employees and Google’s internal documents confirm the
11 conclusion of the AP story. 7/11/2019 [REDACTED] EUO Tr. at 139:13–17 [REDACTED]
12 [REDACTED]

13 [REDACTED] Indeed, [REDACTED]
14 [REDACTED] Ex. 220 (GOOG-GLAZ-00057237) at 238; *see also* Ex. 221
15 (GOOG-GLAZ-00146003) at 007 [REDACTED]
16 [REDACTED]; Ex. 213 (GOOG-GLAZ-00028891) at 894–95 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]

20 60. [REDACTED]

21 [REDACTED] Ex. 222 (GOOG-GLAZ-00069965) at 965 [REDACTED]
22 [REDACTED].

23 61. Multiple Google employees admit that Google’s disclosures regarding WAA and LH are
24 misleading:

- 25 • “Although I know it works and what the difference between ‘Location’ and ‘Location
26 History’ is, I did not know that Web and App activity had anything to do with location. Also
27 seems like we are not very good at explaining this to users.” Ex. 19 (GOOG-GLAZ-00001288)
28 at 289.

1 • “Indeed we aren’t very good at explaining this to users. Add me to the list of Googlers
2 who didn’t understand how this worked an [sic] was surprised when I read the article . . . we
3 shipped a UI that confuses users”). *Id.* at 290.

4 • [REDACTED]
5 [REDACTED] Ex. 223 (GOOG-
6 GLAZ-00057861) at 861.

7 • “The complaint in this article is that if you have Web and App Activity enabled and the
8 location toggle enabled, then your search history entries contain your approximate location at the
9 time you made a query. It’s also not possible to remove them by clearing your location history,
10 which is counter-intuitive – you have to clear your search history instead.” Ex. 224 (GOOG-
11 GLAZ-00149867) at 868.

12 • “Definitely confusing from a user point of view if we need googlers [to] explain it to us.”
13 *Id.* at 867.

14 • “I agree with the article. Location off should mean location off, not except for this case or
15 that case.” Ex. 18 (GOOG-GLAZ-00001266) at 270.

16 • “[C]omms and policy are looking for an update on where we are in terms of fixing
17 ‘location history’ fixes and having one single place to turn off instead of 3.” Ex. 20 (GOOG-
18 GLAZ-00001521) at 523.

19 62. Completely independent of its connection to Location History, Web & App Activity itself
20 is another source of deceptive and unfair acts and practices and unlawful concealment by Google. Until
21 around early- to mid-2018, Google’s disclosures during account creation made no mention of the fact
22 that location information was collected via WAA, which is defaulted to “on.” 7/12/2019 [REDACTED] EUO
23 Tr. at 175:7–15, 374:1–13.

24 63. Even after Google changed this policy, users had to click on a “Learn More” link to view
25 that disclosure until late 2018, when Google finally disclosed that WAA may include location data
26 collection without users having to click on “Learn More.” *Id.* at 376:15–3. Thus, users who had set up an
27 account prior to 2018 would never receive a disclosure that WAA collects location data when setting up
28 their account on a new device. *Id.* at 381:16–23. The same was true after account setup if a user wanted

1 to enable a Google product that required WAA to be “on”: the WAA disclosure made no mention of
2 location collection. Ex. 225 (GOOG-GLAZ-00101684) at 684 (Google Now setup interface requiring
3 WAA opt-in without disclosing its connection to location).

4 64. Additionally, until Android Q, an Android user could not directly access the WAA
5 settings on his phone. 7/12/2019 [REDACTED] EUO Tr. at 164:16–166:19.⁴ Instead, a user would have to
6 navigate to the device’s settings, then to a Google link which took the user to his Google Account, then
7 navigate down to WAA. *Id.*

8 65. [REDACTED]
9 [REDACTED] Ex. 226 (GOOG-GLAZ-00107030) at 030
10 [REDACTED].⁵

11 66. [REDACTED]
12 [REDACTED]
13 [REDACTED] 7/12/2019 [REDACTED] EUO Tr. at 182:23–194:12.
14 [REDACTED]
15 [REDACTED]. *Id.* [REDACTED] *See id.* at
16 183:24–184:10; Ex. 227 (GOOG-GLAZ-00084080) at 1 [REDACTED]
17 [REDACTED]

18 67. [REDACTED]
19 [REDACTED]
20 [REDACTED] Ex. 228 (GOOG-GLAZ-00106193)
21 at 194.

22 68. Notably, Google did not make “any changes to the privacy policy, terms and conditions,
23 help desk or help center website . . . that reflected the change.” 7/12/2019 [REDACTED] EUO Tr. at 195:11–
24

25 _____
26 ⁴ At least prior to Android Q, the same was true of the Location History setting. *See* 7/12/2019 [REDACTED]
27 EUO Tr. at 165:13–166:4, 170:6–171:1. Android Q, also known as Android 10, was released on
28 September 3, 2019. *See* <https://www.theverge.com/2019/9/3/20842507/google-android-10-q-pixel-release-download-availability>.

⁵ [REDACTED]
[REDACTED] 7/12/2019 [REDACTED] EUO Tr. at 69:15–18.

205:22; Ex. 202 (Google’s Responses to CIDs 1–3) at 92–95 (9/4/2019 response to DFI 23 from the Third CID) (“The relevant parts of Google’s Privacy Policy have not been updated in the timeframe inquired about.”). Rather, the only way users would have been able to see the change is if they happened to notice that their WAA data was suddenly more precise/coarsened via the My Activity tool. Thus, Google actively concealed and suppressed the type of location information it collected from its users.

69. [REDACTED]

[REDACTED] 2/27/2020 [REDACTED] EUO Tr. at 52:22–58:13.⁶ [REDACTED]
[REDACTED] *Id.* at 55:3–13. [REDACTED]
[REDACTED] *Id.* at 58:14–59:2.

70. Thus, even when users explicitly tell Google that they do not want their web and app activity to be tracked, Google ignores those requests and collects that data (including location-related data), thereby deceiving users and promising something it does not deliver.

2. Google Misleads Users Into Sharing Their Location Via Its Misleading WiFi Scanning and WiFi Connectivity Settings

71. One of Google’s location settings is WiFi Scanning. WiFi Scanning and WiFi connectivity are independent settings, and both can be switched off. 9/25/2019 [REDACTED] EUO Tr. at 90:2–7. Whereas the WiFi connectivity setting “allows a connection to WiFi or cuts off a connection to WiFi,”

⁶ “Zwieback” is a term used within Google that refers to a specific cookie that is assigned to “any visitor to Google.com or a Google owned and operated property,” regardless of whether they are signed in or out. 2/27/2020 [REDACTED] EUO Tr. at 57:20–58:13. “GAIA” is the Google account identifier and refers to a signed-in Google user. *Id.* at 157:10–20.

1 the WiFi Scanning setting controls whether “system apps and third-party apps can request WiFi scans.”⁷
2 *Id.* at 117:4–118:5.

3 72. Google’s written disclosures at most suggest to users only that WiFi Scanning (as
4 opposed to WiFi connectivity) is related to location data. Ex. 230 (GOOG-GLAZ-00001105) at 106
5 (“To help apps get better location info, you can let your device scan for nearby Wi-Fi access points . . .
6 Tap Advanced > Scanning . . . Turn Wi-Fi scanning . . . on or off”). [REDACTED]

7 [REDACTED]
8 73. The user interface for the WiFi Scanning setting is housed within location settings, while
9 the WiFi connectivity setting itself is separate.⁸ This leads users to believe that the two functions
10 (scanning and connectivity) are separate, and that if they disable the WiFi Scanning permission on their
11 device, Google no longer collects, uses, or stores location information derived from WiFi scans.

12 74. However, Google Location Accuracy (GLA; formerly known as Google Location
13 Services) gets location data from WiFi scans when *either* the WiFi Scanning setting [REDACTED]
14 [REDACTED] is on. 9/25/2019 [REDACTED] EUO Tr. at 88:23–89:10. If WiFi Scanning is *off*, “Google
15 will periodically collect WiFi scans in order to build the estimated location for where WiFi Access
16 Points are,” so long as other toggles (*e.g.*, GLA and [REDACTED] are on. *Id.* at 91:2–7. Further, as
17 of at least November 1, 2017, [REDACTED]

18 [REDACTED]
19 [REDACTED] Ex. 43 (GOOG-GLAZ-00031017) at 022.

20 75. Thus, despite the user attempting to prevent the reporting of WiFi-based location data—
21 and despite the user affirmatively turning the Location Master off—[REDACTED]

22 [REDACTED]
23
24
25
26 [REDACTED] Ex. 231 (GOOG-GLAZ-00109617) at 617 [REDACTED]

27 [REDACTED] *Id.*

28 ⁸ Depending on the OEM and build of Android, the path can look like Settings > Privacy and safety >
Location > Improve accuracy > WiFi scanning. See <https://www.solveyourtech.com/turn-off-wifi-bluetooth-scanning-location-accuracy-android-marshmallow/>.

1 76. In short, the separation of the WiFi Scanning and WiFi connectivity settings misleads
2 users into providing location data to Google even if they do not want to. Google’s disclosures suggest
3 disabling “WiFi Scanning” will prevent Google from scanning nearby WiFi access points. But Google
4 will collect location data via WiFi, so long as GLA is enabled and one of either WiFi scanning or [REDACTED]
5 [REDACTED] is enabled.

6 77. [REDACTED]
7 [REDACTED] and “a bit
8 of a mess that we are working to clear up.” See Ex. 43 (GOOG-GLAZ-00031017) at 020–21. [REDACTED]
9 [REDACTED] *Id.* at 021.⁹ [REDACTED]
10 [REDACTED]
11 [REDACTED] *Id.* at
12 021–22.¹⁰

13 78. In addition to deceiving consumers through the WiFi setting described above, [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED] *Id.* at 021.

17 **D. Google Uses Its Users’ Locations Even When Users Turn Off the Relevant Permissions**

18 **1. Google Shares Location with Apps That Users Explicitly Forbid From Using**
19 **Location**

20 79. In more recent versions of Android, individual apps ask for the user’s permission to use
21 location data, and users can change this permission through their settings. This permissions structure is
22 called a “run-time” permission model; before this model, Google used an “install-time” model that
23

24 ⁹ Android P became publicly available on August 6, 2018.

25 [https://www.theverge.com/circuitbreaker/2018/8/6/17656294/essential-phone-android-9-pie-update-](https://www.theverge.com/circuitbreaker/2018/8/6/17656294/essential-phone-android-9-pie-update-now-available)
26 [now-available.](https://www.theverge.com/circuitbreaker/2018/8/6/17656294/essential-phone-android-9-pie-update-now-available)

27 ¹⁰ In response to a notice to examine Google under oath pursuant to A.R.S. § 44-1524, Google
28 designated Ms. [REDACTED] to testify, *inter alia*, as to “Google’s practices regarding the collection,
transmission, storage, deletion, usage and/or disclosure of user location data through the Android
operating system.”

sought a user's permission only when the app was installed for the first time. 9/25/2019 [REDACTED] EUO Tr. at 163:3–12, 215:3–216:7. Run-time permissions were introduced with Android Marshmallow. *Id.*¹¹

80. Thus, under the run-time model, Google represents to its users that a given app would not be able to obtain a user's location if the user denies app-level location permissions. Ex. 232 (GOOG-GLAZ-00027697) at 700 [REDACTED]
[REDACTED] Ex. 233 (GOOG-GLAZ-00000381) at 381 (public-facing help page explaining that users “can control which apps can see and use your phone’s location. For example, you could let Google Maps use your phone’s location to give you driving directions, but not share the location with a game or social media app.”).

81. [REDACTED]
[REDACTED]
[REDACTED] Ex. 45 (GOOG-GLAZ-00005829) at 829–32 [REDACTED]
[REDACTED]; Ex. 234 (GOOG-GLAZ-00060013) at 013 [REDACTED]; Ex. 114 (GOOG-GLAZ-00198467) at 469 [REDACTED]
[REDACTED]
[REDACTED];¹² Ex. 235 (GOOG-GLAZ-00150448) at 449 [REDACTED]; Ex. 236 (GOOG-GLAZ-00027379) at 379–83 (indicating that “cross-product data use . . . may hurt user trust if we are providing locations to XYZ via the ULR-loophole when the user has explicitly denied it,” and that Google has been aware of the issue “for 2+ years”); Ex. 237 (GOOG-GLAZ-00096366) at 378 [REDACTED]
[REDACTED].

¹¹ Android Marshmallow was publicly released in October 2015.
<https://www.theverge.com/2015/10/5/9454437/android-6-0-marshmallow-now-available>.

¹² [REDACTED] is a service within Google that returns an estimate of a user's location given multiple inputs, such as the user's device location, Location History, and [REDACTED] signals. *See* 2/27/2020 [REDACTED] EUO Tr. at 117:1–3, 119:17–19. [REDACTED], in turn, is a service within Google that maps IP addresses to geographic locations. *See id.* at 98:19–99:4.

1 82. [REDACTED]

2 [REDACTED] Ex. 45 (GOOG-GLAZ-00005829) at 829. In technical terms, [REDACTED]

4 [REDACTED] (Ex. 238 (GOOG-GLAZ-00027688) at 689)—[REDACTED]

5 [REDACTED] Ex. 232 (GOOG-GLAZ-00027697) at 697; *see also* Ex. 214 (GOOG-
6 GLAZ-00101814) at 814 [REDACTED]

8 83. [REDACTED]

9 [REDACTED] Ex. 45 (GOOG-GLAZ-00005829) at 829 [REDACTED]

11 84. [REDACTED]

12 [REDACTED]. *See* Ex. 47 (GOOG-GLAZ-00033771) at 772 [REDACTED]

15 [REDACTED] On information and belief, Mr. [REDACTED] did not direct
16 Google to correct these “borrowed” permissions, nor has Google done so.

17 85. [REDACTED]

19 [REDACTED] Ex. 235 (GOOG-GLAZ-00150448) at 452

23 86. [REDACTED]

1 **2. Google Collects Location Data Even When Users Turn Their Device Location Off**

2 87. [REDACTED]

3 [REDACTED]
4 [REDACTED] Ex. 239 (GOOG-GLAZ-00037593) at 640. And Google
5 consistently makes representations that location data is collected and stored only when the respective
6 settings are turned on. *E.g.*, Ex. 8 at 1 (“With Location History off, the places you go are no longer
7 stored”); Ex. 72 (GOOG-GLAZ-00000715) at 718 (“The types of data we collect depend in part on your
8 device and account settings. For example, you can turn your Android device’s location on or off using
9 the device’s settings app”).

10 88. Thus, a reasonable belief for users is that, when they turn their device’s Location Master
11 off, Google no longer collects, stores, or uses any location information. [REDACTED]

12 [REDACTED]
13 [REDACTED] Ex. 240 (GOOG-
14 GLAZ-00157550) at 550; *see also* Ex. 69 (GOOG-GLAZ-00096793) at 807 [REDACTED]

15 [REDACTED]
16 89. Moreover, users of Google’s products have absolutely no control over whether Google
17 can use their IP addresses to derive a location and serve ads based on that location. 5/8/2020 [REDACTED]

18 EUO Tr. at 271:23–272:1 [REDACTED]
19 [REDACTED]; 2/28/2020 [REDACTED] EUO Tr. at 517:15–23 [REDACTED]

20 [REDACTED]
21 [REDACTED]
22 [REDACTED]; 5/21/2020 [REDACTED] Rough EUO Tr. at 98:4–

23 6 [REDACTED]
24 90. [REDACTED]
25 [REDACTED]
26 [REDACTED] *See* Ex. 241 (GOOG-GLAZ-00097091) at 092.

27 91. [REDACTED]
28 [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] *See id.; see also* Ex. 242 (GOOG-GLAZ-00101518) at 518 [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

92. [REDACTED]
[REDACTED] Ex. 243 (GOOG-GLAZ-00111292) at
320.

93. [REDACTED]
[REDACTED]
(Ex. 84 (GOOG-GLAZ-00079712) at 712 [REDACTED] even if the user has
since turned off location history”), [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED] 3/6/2020
[REDACTED] EUO Tr. at 378:14–379:6.

94. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] Ex. 244 (GOOG-GLAZ-00031991) at 991. [REDACTED]
[REDACTED]

1 95. In short, Google collects user location data even when users expressly try to turn off
2 location settings and reasonably believe that their locations are no longer being collected.

3 **3. Google Serves Personalized Ads Based on User Location Even When Users Turn**
4 **Off Personalization**

5 96. Google’s culpable conduct is not limited solely to collecting location data in a misleading
6 and deceiving way; it also uses location data for ads in ways that mislead and deceive users, including
7 those in Arizona.

8 97. Google serves ads to its users based in part on location data retrieved from, among other
9 settings, Location History and Web & App Activity. 9/25/2019 [REDACTED] EUO Tr. at 222:10–25. Google
10 purports to allow users to opt-out of this advertisement personalization; in order to do so, Google
11 provides an account-level toggle in a user’s Google Account under “Data & Personalization.” Ex. 245
12 (GOOG-GLAZ-00000415) at 415 (“You can change where you see personalized ads or stop Google
13 from using your activity to personalize ads.”).

14 98. Such a toggle implies that the user has control over whether Google will serve ads based
15 on the user’s location. But [REDACTED]
16 [REDACTED] Ex. 70 (GOOG-GLAZ-00085629) at 636.

17 99. Indeed, as confirmed by [REDACTED]
18 even if a user opts out of ad personalization, Google *still* uses the user’s real-time location to serve ads.
19 5/21/2020 [REDACTED] Rough EUO Tr. at 114:9–115:11. [REDACTED]
20 [REDACTED] *Id.* at 84:14–19.

21 100. Moreover, the “GAP” (Google ad personalization) setting only affects ads served on
22 Google owned-and-operated properties—not ads served on third party websites using Google’s
23 DoubleClick service. *See* 2/27/2020 [REDACTED] EUO Tr. at 172:2–15; 2/28/2020 [REDACTED] EUO Tr. 318:24–
24 319:7.

25 101. [REDACTED]
26 [REDACTED] 2/27/2020 [REDACTED] EUO Tr. at 163:6–16, 167:8–
27 22. [REDACTED]
28 [REDACTED] *Id.*

1 102. [REDACTED]

2 [REDACTED]
3 [REDACTED]
4 [REDACTED] 2/27/2020 [REDACTED] EUO Tr. at 172:2–15 (when GAP is off,
5 Google still targets users with ads based on their location through DoubleClick).

6 103. [REDACTED]

7 [REDACTED] 2/27/2020 [REDACTED] EUO Tr. at
8 189:18–190:17.

9 104. [REDACTED]

10 [REDACTED]
11 [REDACTED]
12 [REDACTED]
13 [REDACTED].
14 **E. Google Automatically Changes the State of Permissions Without Notifying Users**

15 105. Presumably, the entire point of including various toggles and consents on devices and
16 accounts is to give the user control over the state of their device and/or account. However, Google has
17 pushed a variety of updates that automatically change the user’s location settings and defaults without
18 informing the user, much less seeking or obtaining consent.

19 106. For example, in August 2016, [REDACTED]

20 [REDACTED]
21 [REDACTED]
22 [REDACTED] Ex. 79 (GOOG-GLAZ-00057389) at 389; *see also* Ex. 246 (GOOG-GLAZ-00058103) at
23 104 (“As of Aug 2016, switching the account level sWAA bit will toggle the device-level sWAA for all
24 devices owned by the GAIA” resulting in “a fairly large increase in devices reporting appusage [sic]
25 since Aug”).¹³ [REDACTED]

26 _____
27 ¹³ As described above, sWAA is a setting, housed within WAA as a checkbox, that collects data from
28 [REDACTED] in WAA. Ex. 203 (GOOG-GLAZ-00076994) at 7002. This supplemental setting is itself misleading for users. *See* Ex.

[REDACTED]

107. In another example, in around 2017, [REDACTED]

[REDACTED]

[REDACTED] Ex. 78 (GOOG-GLAZ-00070610) at 610. [REDACTED]

[REDACTED]

[REDACTED] *Id.* [REDACTED]

[REDACTED] *Id.*; see also Ex. 248 (GOOG-GLAZ-00070491)
at 491 [REDACTED]

[REDACTED].

108. [REDACTED]

[REDACTED]

[REDACTED] 3/6/2020 [REDACTED] EUO Tr. at 286:19–287:24,
290:14–291:24.

109. [REDACTED]

[REDACTED]

Ex. 249 (GOOG-GLAZ-00125482) at 490 [REDACTED]

[REDACTED]

[REDACTED] Ex. 250 (GOOG-GLAZ-00065187) at 192 [REDACTED]

[REDACTED]

[REDACTED]

247 (GOOG-GLAZ-00126368) at 384 [REDACTED]
[REDACTED]

Ex. 251

(GOOG-GLAZ-00127414) at 414–16

F. Google Changes the Android User Interface to Increase Location [REDACTED] at the Expense of User Choice and Consent

110. Google invests tremendous resources trying to persuade users to hand over their precise location data. Increasing the number of users who do is a significant driver of ad revenue for Google. As a result, Google deliberately tries to minimize opportunities for users to disable location settings, and Android’s architecture is designed to conceal the opportunities that do exist.

111. [REDACTED]

Ex. 51 (GOOG-GLAZ-00026768) at 769–72

112. [REDACTED]

9/25/2019 [REDACTED] EUO Tr. at 199:4–6.

[REDACTED]. Ex. 51 (GOOG-GLAZ-00026768) at 770. [REDACTED]

Id. at 769–77.¹⁴

113. One change to the Android UI was a change to the Quick Settings (“QS”) panel on Android KitKat. The QS panel becomes visible when a user pulls down from the top of the screen at almost any point on an Android device. 9/25/2019 [REDACTED] EUO Tr. at 202:15–22. The panel includes toggles for various popularly used settings, such as WiFi. The QS panel previously included a toggle for

¹⁴ Android KitKat was publicly released on October 31, 2013. *See* <https://googleblog.blogspot.com/2013/10/android-for-all-and-new-nexus-5.html>.

1 the Location Master; [REDACTED]
2 [REDACTED] Ex. 51 (GOOG-GLAZ-00026768) at 772; Ex. 71 (GOOG-
3 GLAZ-00027187) at 196 [REDACTED]
4 [REDACTED]
5 114. [REDACTED]
6 [REDACTED] Ex. 51 (GOOG-GLAZ-00026768) at
7 768–72. [REDACTED]
8 [REDACTED] Ex. 61 (GOOG-GLAZ-
9 00026360) at 360. [REDACTED]
10 [REDACTED] *Id.* at 361 [REDACTED]
11 [REDACTED]¹⁵
12 115. [REDACTED]
13 [REDACTED]
14 [REDACTED] *See* Ex. 52 (GOOG-
15 GLAZ-00005425) at 428; *see also* Ex. 252 (GOOG-GLAZ-00028327) at 327 [REDACTED]
16 [REDACTED]
17 116. [REDACTED]
18 [REDACTED]
19 [REDACTED] Ex. 52 (GOOG-GLAZ-
20 00005425) at 429. [REDACTED]
21 [REDACTED]
22 117. [REDACTED]
23 [REDACTED]
24 [REDACTED] Ex. 51 (GOOG-GLAZ-00026768) at 785; *see also*
25 9/25/2019 [REDACTED] EUO Tr. at 238:10–239:3; Ex. 253 (GOOG-GLAZ-00028014) at 014–25 [REDACTED]
26
27
28

¹⁵ [REDACTED]
[REDACTED]

1 [REDACTED]
2 [REDACTED]
3 118. [REDACTED]
4 [REDACTED]
5 [REDACTED] Ex. 254 (GOOG-GLAZ-00115868) at 868 (sheet1, cell
6 G14). [REDACTED]
7 [REDACTED]
8 [REDACTED] Ex. 53 (GOOG-GLAZ-00026843) at 850. [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED] *Id.* at 847–50. [REDACTED]
12 [REDACTED] *See id.*
13 at 846–47.
14 119. [REDACTED]
15 [REDACTED]
16 [REDACTED] Ex. 255 (GOOG-GLAZ-00027518) at 518; Ex. 256
17 (GOOG-GLAZ-00029585) at 615.
18 120. [REDACTED]
19 [REDACTED] Ex.
20 257 (GOOG-GLAZ-00032539) at 539.
21 121. [REDACTED]
22 [REDACTED] Ex.
23 52 (GOOG-GLAZ-00005425) at 431. [REDACTED]
24 [REDACTED]
25 [REDACTED] *Id.* at 426. [REDACTED]
26 [REDACTED]
27 *Id.* at 426. [REDACTED]
28

[REDACTED]

[REDACTED] *Id.* at 425.

122. [REDACTED]

[REDACTED] *See, e.g.*, Ex.

53 (GOOG-GLAZ-00026843) at 844 [REDACTED]

[REDACTED]

123. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

124. [REDACTED]

[REDACTED] Ex. 254 (GOOG-GLAZ-00115868) at

868 (sheet1, rows 12–14). [REDACTED]

[REDACTED] *See* Ex. 61 (GOOG-GLAZ-00026360) at 361 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] (emphasis in original).

125. [REDACTED]

[REDACTED]

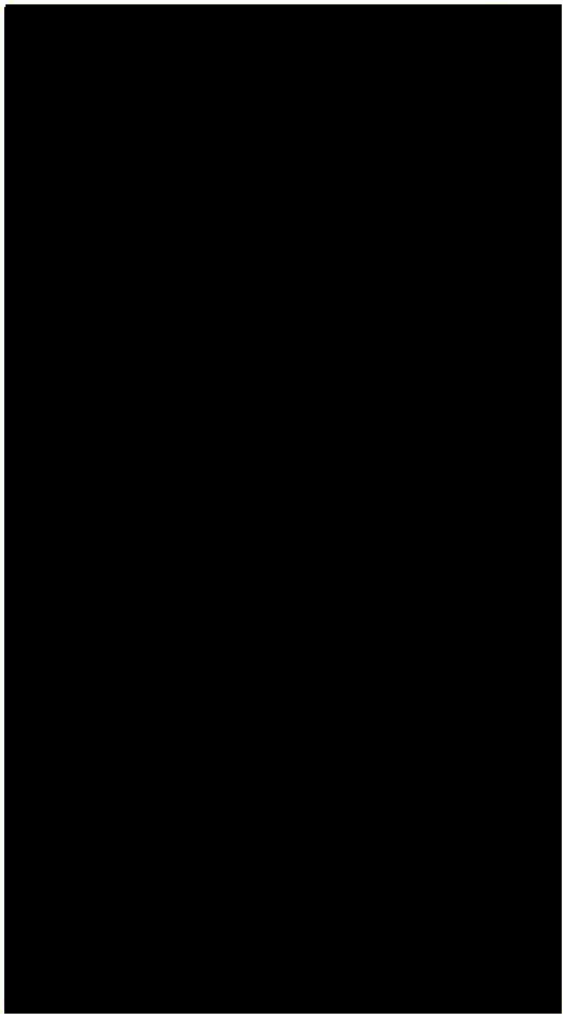
[REDACTED]

[REDACTED] Ex. 256 (GOOG-GLAZ-00029585) at 595.

126. [REDACTED]

[REDACTED] *Id.* [REDACTED]

[REDACTED]



Id.

127. [REDACTED]

[REDACTED] *Id.*

128. [REDACTED]

[REDACTED]

[REDACTED]

G. Google Misleads and Deceives Users Regarding Its Deletion of Their Location Information

129. Google admits that, until at least as late as 2015, [REDACTED]
[REDACTED] Ex. 214 (GOOG-GLAZ-00101814) at 814. At some
subsequent time, Google started purporting to offer users control over whether and how Google retains
their information. In particular, Google now represents that users are able to delete the location data that

1 it has collected and stored. Ex. 36 (GOOG-GLAZ-000000001) at 001–02 (“We’ll keep this data in your
2 Google Account until you choose to remove it,” “[w]hen you delete data in your Google account, we
3 immediately start the process of removing it from the product and our systems”); *see also* Ex. 202
4 (Google’s Responses to CIDs 1–3) at 79–80 (9/47/2019 response to DFI 10 from the Third CID) (“For
5 users that have Web & App Activity enabled, Google saves their search results and associated location
6 information in the users’ Google Accounts. Users can delete that data at any time.”).

7 130. But while users may believe that Google deleted their location data, Google nonetheless
8 retains that data for much longer.

9 131. While that by itself is misleading and deceptive, what is worse is that Google’s user-
10 facing interface displays data being deleted immediately—opposite to what Google actually does. Ex. 59
11 (GOOG-GLAZ-00031110) at 124 [REDACTED]

12 [REDACTED]
13 [REDACTED]
14 [REDACTED] Ex. 258 (GOOG-GLAZ-00065293) at 295 [REDACTED]
15 [REDACTED]
16 [REDACTED]

17 [REDACTED] (emphasis in original).

18 **H. Google Has Engaged In Willful Violations Of The Arizona Consumer Fraud Act**

19 132. Google’s many violations of the Arizona Consumer fraud act were willful, *i.e.* it knew or
20 should have known its conduct was of the nature prohibited by the Arizona Consumer Fraud Act.

21 133. Google willfully misleads and deceives users into enabling collection of their location
22 data and using and storing their location data in ways users do not know or understand. Google also
23 willfully engages in unfair acts and practices, including through the conduct described above.

24 134. Some of this evidence was described above, and more is set forth here and below:

- 25 • [REDACTED]
26 [REDACTED] . . . We have location as a product umbrella that includes Location History, [REDACTED], and
27 a bunch of other stuff that’s super messy. And it’s a Critical User Journey to make sense out of
28 this mess.” Ex. 209 (GOOG-GLAZ-00057477) at 477–78.

1 • [REDACTED] Ex. 259 (GOOG-GLAZ-00078007) at 807.

2 • [REDACTED]

3 [REDACTED]

4 [REDACTED] Ex. 216 (GOOG-GLAZ-00078009) at 018.

5 • [REDACTED]

6 [REDACTED] Ex.

7 260 (GOOG-GLAZ-00057339) at 340.

8 • [REDACTED]

9 [REDACTED] Ex. 270 (GOOG-GLAZ-00055829) at 851.

10 • [REDACTED]

11 [REDACTED]

12 [REDACTED]

13 [REDACTED] Ex. 261 (GOOG-GLAZ-00099239) at 239.

14 • [REDACTED]

15 [REDACTED]

16 [REDACTED] Ex. 262 (GOOG-GLAZ-

17 00117506) at 506.

18 135. Google has known about these issues since at least 2012. Ex. 263 (GOOG-GLAZ-

19 00100799) at 800 [REDACTED]

20 [REDACTED]

21 [REDACTED]

22 136. [REDACTED]

23 [REDACTED]

24 [REDACTED] Ex. 260 (GOOG-GLAZ-00057339) at 339.

25 [REDACTED]

26 • Simplifying device-level location data settings. *Id.* at 339 [REDACTED]

27 [REDACTED]

1 [REDACTED] Ex. 264 (GOOG-GLAZ-00048459) at 478

2 [REDACTED]
3 • [REDACTED] *Id.*; Ex. 265 (GOOG-GLAZ-00078761) at 761

4 [REDACTED] Ex. 266 (GOOG-GLAZ-
5 00151516) at 517 [REDACTED]

6 [REDACTED]
7 • The 2018 AP Article and the interaction between WAA and LH. Ex. 23 (GOOG-GLAZ-
8 00001371) at 373 [REDACTED] asked that we have a ‘Location’ [REDACTED] update in Leads” in
9 response to the AP News Cycle); Ex. 267 (GOOG-GLAZ-00035559) at 559 (email chain
10 regarding LH/WAA interaction meeting with [REDACTED]); Ex. 268 (GOOG-GLAZ-00078652) at 52
11 (notes regarding LH/WAA interaction, including [REDACTED] opinion).

12 • [REDACTED] Ex.
13 47 (GOOG-GLAZ-00033771) at 72 [REDACTED]

14 • [REDACTED] Ex. 269 (GOOG-GLAZ-00073037) at 037–43 [REDACTED]

15 [REDACTED]
16 [REDACTED]
17 • [REDACTED]

18 **IV. ARIZONA’S INVESTIGATION INTO GOOGLE’S**
19 **UNFAIR AND DECEPTIVE ACTS AND PRACTICES**

20 137. The Arizona Attorney General’s Office (“AGO”) first became aware of Google’s
21 potential violations of the Arizona Consumer Fraud Act in connection with the collection of user
22 location data after the Associated Press published the article entitled, “Google tracks your movements,
23 like it or not.”

24 138. Thereafter, the AGO served a First Civil Investigative Demand (“CID”) on Google on
25 January 30, 2019 to investigate Google’s location data collection practices.

26 139. Google has impeded the AGO’s investigation for months on end.

27 140. For months, beginning with service of the First CID, Google was uncooperative with the
28 AGO’s investigation. Despite the extensive and highly technical nature of the information sought by the

1 AGO—both in the First CID and in two subsequent CIDs up to that point—Google at first produced
2 only 402 documents totaling 1543 pages (mostly poor-quality reproductions of publicly available
3 information) and failed to substantively respond to *any* of the AGO’s Demands for Information. Over
4 these months, the AGO repeatedly expressed its frustrations to Google. Repeatedly, Google promised to
5 deliver information but failed to follow through.

6 141. As it relates to products operating on the Android operating systems, Google insisted for
7 months that it could not provide (and did not have) responsive information or documents apart from
8 Google’s own Pixel-branded phones. For months, Google also claimed it did not have documents or
9 information concerning the collection of user location data on devices using the Android operating
10 systems (outside of those installed on Pixel devices), or concerning the operation of any of Google’s
11 own apps installed on non-Pixel phones. Google’s reason was that it purportedly had no control over
12 how third-party OEMs modified the open-source Android software. The AGO’s investigation later
13 confirmed that Google’s positions were inaccurate and misleading. Google witness [REDACTED] testified
14 that he was the [REDACTED]
15 [REDACTED] in the Android operating software that is responsible for computing location. 3/6/2020
16 [REDACTED] EUO Tr. at 67:20–70:11. Mr. [REDACTED] confirmed unequivocally that this FLP was not necessarily
17 designed for Google-branded smartphones, but more broadly for “Android devices more generally.” *Id.*
18 at 71:7–17.

19 142. As other witnesses explained, while Android is an open-source software, Google
20 exercises control over what version of Android a vast majority of OEMs install on their devices: if any
21 OEMs want to install Google’s library of very popular apps (included in GMS, which include, for
22 example, Google Maps and Search), OEMs must install Google’s preferred version of Android.
23 2/28/2020 [REDACTED] EUO Tr. at 448:9–17; 9/25/2019 [REDACTED] EUO Tr. at 139:1–140:21. Google perpetuates
24 its location data collection through any phone—made by Google or not—that has GMS installed.
25 2/28/2020 [REDACTED] EUO Tr. at 444:8–445:17, 448:9–17; *see also* 9/25/2019 [REDACTED] EUO Tr. at 64:6–13.

26 143. In other words, contrary to Google’s long-standing position in the investigation, Google
27 very much has information and documents concerning the collection of user location data from
28 “Android devices more generally” because, among other things, Google designed and controls that

1 collection process through the FLP in the Android operating system. Indeed, Google collects data about
2 the number of devices reporting Location History not only from all Android devices, but also from iOS
3 devices. 3/6/2020 [REDACTED] EUO Tr. at 122:6–124:2.

4 144. Similarly, when the AGO requested information concerning ad revenue early in the
5 investigation, Google objected that it “does not understand, and the AGO has not provided any
6 guidance, regarding any nexus of revenue from the Android mobile devices and location information.”
7 Ex. 202 (Google’s Response to CIDs 1–3) at 51 (5/30/2019 response to RFP 19 from the First CID). [REDACTED]

8 [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]

12 5/21/2020 [REDACTED] Rough EUO Tr. at 84:15–19.

13 145. Google also took it upon itself to dictate the scope of the AGO’s investigation. For
14 example, for months Google insisted that the AGO’s investigation was somehow limited to the facts
15 identified in the AP news article, while refusing to provide any other information or documents, even as
16 the AGO repeatedly instructed Google otherwise. Similarly, Google insisted that the AGO’s
17 investigation is somehow limited to a one-year period. Google initially agreed to search for documents
18 covering only a six-month time period and, even as to that time period, Google refused to do any kind of
19 meaningful search or production.

20 146. For months, Google also refused to provide testimony under oath as to any of the topics
21 identified by the AGO. For example, on May 11, 2019, the AGO served a subpoena seeking testimony
22 from Google’s person most knowledgeable as to twenty topics identified in the subpoena. Google
23 refused to provide testimony on the topics identified by the AGO and, instead, Google identified its own
24 topics for which it was willing to provide testimony. But even as to those topics, Google did not provide
25 straightforward testimony.

26 147. More fundamentally, for months, Google tried to cabin all questioning of its witnesses to
27 the *inner* workings of *either* Location History *or* Web & App Activity. The AGO’s investigation
28 ultimately revealed that much of the location related data for Google products and services is provided

1 by (or though) a group known as [REDACTED], which is based in Switzerland. [REDACTED] (and its components)
2 serve over 250 internal products and services (*i.e.*, “clients”) at Google. Those clients are often grouped
3 into two categories: consumer facing (*e.g.*, Location History) and monetization (*i.e.*, ads). *See* 5/8/2020
4 [REDACTED] EUO Tr. at 167:19–169:25; 3/6/2020 [REDACTED] EUO Tr. at 398:18–401:17. Location History and
5 Web & App Activity are user-facing settings. By restricting questions to the inner workings of either of
6 those settings, Google tried to evade any questioning as to how user location data is collected or used
7 more broadly.

8 148. The AGO finally obtained more cooperation when the AGO threatened to file a petition
9 to judicially enforce Google’s compliance with outstanding discovery requests in late August 2019—
10 over eight months after the AGO served its First CID.

11 149. Yet even after Google increased its cooperation, it still consistently hamstrung the AGO’s
12 investigation by still failing to live up to promises it made. For example, Google repeatedly promised
13 production of documents and written responses by certain deadlines but regularly failed to produce them
14 on time, or even at all. Google similarly promised to make witnesses available for examination by
15 certain dates, and then failed to comply with its own unilaterally set timetable.

16 150. When the AGO subpoenaed Google for testimony specifically addressing Google’s
17 broader location practices—a subject spanning 17 topics—Google designated just a single witness,
18 [REDACTED], who was far from prepared. Mr. [REDACTED] was not knowledgeable about subjects that are
19 fundamental to Google’s ability to obtain a user’s location—all of which he was designated to testify
20 about—such as [REDACTED], Google’s ability to collect location information from signed-out users, [REDACTED],
21 Google’s aggregation of location data, and a white paper titled “Google, Android, the end of Notice-and-
22 Choice.” 2/27/2020 [REDACTED] EUO Tr. at 59:17–61:15, 115:4–17, 124:17–125:5, 144:15–19, 194:17–
23 195:2; 2/28/2020 [REDACTED] EUO Tr. at 447:15–22, 448:18–449:19, 450:2–451:10, 458:24–459:5. This is
24 not surprising: Mr. [REDACTED] spent only 20 minutes speaking to a single non-lawyer [REDACTED] as
25
26
27
28

1 part of his preparation (all regarding one specific subject), with the remaining time spent speaking to
2 lawyers.¹⁶ 2/27/2020 [REDACTED] EUO Tr. at 34:1–35:7, 115:18–23.

3 151. Mr. [REDACTED] did not know the answers to many questions that fell squarely within his
4 designated topics, and he referred the AGO to Mr. [REDACTED] for answers. But when Mr. [REDACTED] was
5 later deposed, he also claimed ignorance. In one clear example, Mr. [REDACTED] claimed he discussed “the
6 inputs into [REDACTED]” with Mr. [REDACTED] to prepare for his EUO, but when Mr. [REDACTED] was asked, “Do
7 you know what the inputs to [REDACTED] are?” he responded, “I do not.” 2/27/2020 [REDACTED] EUO Tr. at
8 115:18–23; 5/8/2020 [REDACTED] EUO Tr. at 115:11–17. In another example, Mr. Berlin explained that
9 prior to coarsening user locations to 3 square kilometers in certain instances (as it apparently does
10 today), Google coarsened user locations to 1 square kilometer, but he did not know what Google’s
11 coarsening policy was prior to the 1-square-kilometer policy—he referred the AGO to Mr. [REDACTED] for
12 the answer to that question. 2/27/2020 [REDACTED] EUO Tr. at 125:2–12. However, Mr. [REDACTED] was
13 unknowledgeable even about the 1-square-kilometer policy. 5/8/2020 [REDACTED] EUO Tr. at 61:7–18,
14 102:17–103:6.

15 152. Indeed, Mr. [REDACTED] referred the AGO to yet another Google employee, [REDACTED]
16 [REDACTED] who is located in Zurich and is supposedly actually knowledgeable about the relevant Google
17 technologies. *E.g.*, 5/8/2020 [REDACTED] EUO Tr. at 57:9–12, 59:25–60:17, 61:3–62:4, 79:10–80:12,
18 115:15–20; *see also id.* at 111:22–24 (“Q. Who is the person or group of people at Google most familiar
19 with [REDACTED] A. [REDACTED]”).

20 153. In another attempt to get testimony on [REDACTED] on July 31, 2019 and again on January 10,
21 2020, the AGO served a subpoena for an EUO of [REDACTED] who was had been identified at an earlier
22 examination as leading the [REDACTED] team. Google refused to comply. At some point, Mr. [REDACTED]
23 [REDACTED] apparently replaced Mr. [REDACTED] as the head of [REDACTED]. Google failed to disclose that
24

25
26 ¹⁶ Mr. [REDACTED] spoke with Mr. [REDACTED] regarding [REDACTED], but Mr. [REDACTED], the leader of the [REDACTED]
27 team, later testified that he only spends about 10% of his day-to-day work on [REDACTED] and led the [REDACTED]
28 team only because his direct report actually oversees it; indeed, Mr. [REDACTED] had very little actual
knowledge on the workings of [REDACTED] and made clear he only exercised a general managerial role.
5/8/2020 [REDACTED] EUO Tr. at 28:4–21, 59:18–60:17, 61:3–6, 64:24–65:7, 70:16–71:6, 72:16–74:8,
106:6–19.

1 information to the AGO for nearly ten months, until this was revealed at the EUO of Mr. [REDACTED]. Mr.
2 [REDACTED] has also not been examined, nor has anyone communicated with Mr. [REDACTED] in preparation
3 for providing testimony to the AGO.

4 154. [REDACTED]
5 [REDACTED]. None of the designated Google witnesses were
6 prepared to explain these features or the documents describing those features.

7 155. In short, the AGO's pre-suit investigation has been prejudiced by Google's uncooperative
8 conduct, delay tactics, and general failure to comply with the AGO's discovery demands. Even so, the
9 AGO's investigation to date has uncovered and confirmed the wrongdoing alleged herein.

10 V. CLAIM FOR RELIEF

11 ARIZONA CONSUMER FRAUD ACT (A.R.S. § 44-1521, et seq.)

12 156. Arizona realleges and incorporates by reference all prior paragraphs as though fully set
13 forth herein.

14 157. The Arizona Consumer Fraud Act provides that "[t]he act, use or employment by any
15 person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise,
16 misrepresentation, or concealment, suppression or omission of any material fact with intent that others
17 rely upon such concealment, suppression or omission, in connection with the sale or advertisement of
18 any merchandise whether or not any person has in fact been misled, deceived or damaged thereby, is
19 declared to be an unlawful practice." A.R.S. § 44-1522(A).

20 158. Google is a "person" within the meaning of A.R.S. § 44-1521(6).

21 159. The Google products and services described in this Complaint, including but not limited
22 to Google apps, sites, and devices, Google Accounts, Google ads, and platforms like Google Chrome
23 and Android, are "merchandise" within the meaning of A.R.S. § 44-1521(5).

24 160. Google has systematically engaged in activities with a tendency or capacity to deceive
25 consumers. Google engaged in unlawful practices by employing deception, deceptive or unfair practices,
26 false pretenses, false promises, misrepresentations, or concealment, suppression or omission of material
27 facts with intent that others rely upon such concealment, suppression or omission, in connection with the
28 sale and advertisement of Google products and services.

1 161. In particular, and as described above, Google’s unlawful practices, in violation of the
2 Arizona Consumer Fraud Act, include the following:

- 3 a. Engaging in deceptive and unfair acts and practices by making the deceptive
4 misrepresentation and false promise that “[w]ith Location History off, the places you
5 go are no longer stored,” when in fact Google continued to collect and store user
6 location information even with Location History turned off.
- 7 b. Concealing, suppressing, or omitting the material fact that Google continued to
8 collect and store user location information even with Location History turned off.
- 9 c. Concealing, suppressing, or omitting during account creation the material fact that
10 location information was collected through Web & App Activity—which defaulted to
11 “on.”
- 12 d. Engaging in deceptive and unfair acts and practices by making the deceptive
13 misrepresentation and false promise that users “can turn [their] Android device’s
14 location on or off using the device’s settings app” despite the fact that [REDACTED]
15 [REDACTED]
16 [REDACTED]
- 17 e. Concealing, suppressing, or omitting the material fact that [REDACTED]
18 [REDACTED].
- 19 f. Engaging in deceptive and unfair acts and practices by [REDACTED]
20 [REDACTED]
21 [REDACTED]
- 22 g. Concealing, suppressing, or omitting the material fact that [REDACTED]
23 [REDACTED]
24 [REDACTED]
- 25 h. Engaging in deceptive and unfair acts and practices by knowingly maintaining a
26 misleading and diverse array of settings related to location tracking that makes it
27 difficult if not impossible to understand the conditions in which Google will collect
28 location data.

- 1 i. Concealing, suppressing, or omitting the material facts about the conditions in which
2 Google will collect location data.
- 3 j. Engaging in deceptive and unfair acts and practices by [REDACTED]
4 [REDACTED]
5 [REDACTED]
6 [REDACTED]
- 7 k. Concealing, suppressing, or omitting the material fact that location settings were on.
- 8 l. Engaging in deceptive and unfair acts and practices by failing to disclose that Google
9 apps that have been denied permission to access location data can still obtain that data
10 from other Google apps that have been granted permission.
- 11 m. Concealing, suppressing, or omitting the material fact that Google apps that have
12 been denied permission to access location data can still obtain that data from other
13 Google apps that have been granted permission.
- 14 n. Engaging in deceptive and unfair acts and practices by knowingly maintaining a
15 confusing and misleading presentation of the WiFi scanning and WiFi connectivity
16 settings that [REDACTED]
17 [REDACTED]
- 18 o. Concealing, suppressing, or omitting the material fact that [REDACTED]
19 [REDACTED]
- 20 p. Engaging in deceptive and unfair acts and practices by continuing to present location-
21 based advertisements to users even after they have opted out of ad personalization,
22 and maintaining two separate settings relating to location-based advertising that users
23 find confusing, to the extent that they are even aware of them at all.
- 24 q. Concealing, suppressing, or omitting the material fact that Google would continue to
25 collect and store users' location information unless they disabled two separate
26 settings relating to location-based advertising, and that even with both settings
27 disabled Google would still use user location data to target ads.
- 28

1 r. Engaging in deceptive and unfair acts and practices by misleading users into
2 believing that Google immediately deletes their location-related data when, in reality,
3 Google keeps the data long afterwards.

4 s. Concealing, suppressing, or omitting the material fact that Google did not
5 immediately delete location-related data, and in reality, kept the data long afterwards.

6 162. With respect to its concealment, suppression, and omission of material facts described
7 above, Google intends that users rely on the concealment, suppression, or omission.

8 163. Consumers in Arizona have in fact been the subject of deception, deceptive/unfair
9 acts/practices, false pretense and promises, misrepresentations, and concealment, suppression, or
10 omission of material facts described above.

11 164. Google's purpose in engaging in these unlawful practices is simple: increasing revenue
12 and profit. Google generates over one hundred billion dollars of revenue and tens of billions of dollars of
13 profit every year from advertising, including, on information and belief, hundreds of millions of dollars
14 from ads shown to users in Arizona. These advertising profits are driven in large part by Google's ability
15 to collect and store its users' location data, which enables Google to sell advertisers on the ability to
16 target ads to users in particular locations. It also enables Google to track "conversions" of ad clicks to
17 store visits. Google therefore goes to great lengths to collect location information from its users,
18 including by engaging in the unlawful activities alleged in this Complaint. Those unlawful activities
19 were done in connection with the sale or advertisement of merchandise within the meaning of A.R.S.
20 § 44-1522(A).

21 165. While engaging in the unlawful acts and practices alleged in this Complaint, Google has
22 at all times acted "willfully" as defined by A.R.S. § 44-1531: Google knew or should have known that
23 its conduct was of the nature prohibited by the Arizona Consumer Fraud Act.

24 166. Google's violations present a continuing harm and the unlawful acts and practices
25 complained of here affect the public interest.

26 167. Google's actions to date have failed to fully address the misleading and deceptive nature
27 of its business activities and the company continues to engage in acts prohibited by the Arizona
28 Consumer Fraud Act.

1 **PRAYER FOR RELIEF**

2 WHEREFORE, Arizona respectfully requests that the Court enter Judgment against Google as
3 follows:

4 A. Order Google to disgorge all profits, gains, gross receipts, and other benefits obtained by
5 means of any unlawful practice as alleged herein, pursuant to A.R.S. §44-1528(A)(3);

6 B. Order Google to pay full restitution to consumers, pursuant to A.R.S. §44-1528(A)(2);

7 C. Order Google to pay Arizona a civil penalty of not more than \$10,000 for each willful
8 violation of the Arizona Consumer Fraud Act, pursuant to A.R.S. § 44-1531;

9 D. Enter an injunction against Google, permanently prohibiting it from continuing the
10 unlawful acts and practices alleged in this Complaint or doing any acts in furtherance of such unlawful
11 acts of practices, pursuant to A.R.S. § 44-1528(A)(1);

12 E. Order Google to pay Arizona its costs of investigation and prosecution of this matter,
13 including its reasonable attorneys' fees, pursuant to A.R.S. § 44-1534; and

14 F. Award Arizona such further relief as the Court deems just and proper under the
15 circumstances.

16
17 Dated: May 27, 2020

MARK BRNOVICH
ATTORNEY GENERAL
By: /s/ Brunn W. Roysden III
Joseph A. Kanefield
Brunn W. Roysden III
Oramel H. Skinner
Michael S. Catlett
Christopher Sloom
Assistant Attorneys General

22 Guy Ruttenberg (CA Bar No. 207937)
23 (*pro hac vice* application forthcoming)
Michael Eshaghian (CA Bar No. 300869)
24 (*pro hac vice* application forthcoming)
RUTTENBERG IP LAW, A PROFESSIONAL
25 CORPORATION
1801 Century Park East, Suite 1920
26 Los Angeles, California 90067
Telephone: (310) 627-2270
27 guy@ruttenbergiplaw.com
mike@ruttenbergiplaw.com

David H. Thompson (DC Bar No. 450503)
(*pro hac vice* application forthcoming)
Peter A. Patterson (DC Bar No. 998668)
(*pro hac vice* application forthcoming)
COOPER & KIRK PLLC
1523 New Hampshire Ave NW
Washington, DC 20036
Telephone: (202) 220-9600
dthompson@cooperkirk.com
ppaterson@cooperkirk.com

28 *Attorneys for Plaintiff State of Arizona ex rel. Mark Brnovich, Attorney General*