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 Sloot (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.Sloot@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

Page

TABLE OF CONTENTS (*cont.*)

Page

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

I. INTRODUCTION

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

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

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

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

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

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

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

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

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

a. As described in the AP article, with Location History off, Google continues to collect location information through Web & App Activity—a title that reveals nothing about the setting's connection to harvesting location data. Through Web & App Activity, Google logs information relating to a user's activity on Google websites and apps, such as conducting a search on Google Search. A critical component of this information from Google's perspective is a user's location. Nevertheless, until early-to mid-2018, Google's disclosures during account creation made no mention of the fact that location information was collected through Web & App Activity, which is defaulted to "on." And even today the title itself is misleading by failing to disclose any connection to location.

b. Devices running the Android operating system have a device-level location setting. Google tells users that "the types of data we collect depend in part on your device and

account settings. For example, you can turn your Android device's location on or off using the device's settings app." A reasonable conclusion from this disclosure is that "off means off"—*i.e.*, that Google simply will not collect and exploit user location information when a device's location setting is turned off. But that is not true. Instead, Google operates on the principle that "off means coarse"—in other words, Google reduces the *precision* with which it collects and uses a user's information when a device's location setting is off but does not stop the collection and exploitation of that information altogether. Indeed, it is *impossible* for users of Google products and services to prevent Google from exploiting information about their location for financial gain.

c. Google's WiFi settings mislead users about Google's collection and use of location information. There are two relevant settings—WiFi scanning and WiFi connectivity. Only the WiFi scanning setting is presented within location settings, which would lead a reasonable user to believe that turning it off would result in Google no longer discerning a user's location through WiFi scans. But that is not true—even with WiFi scanning off, Google may *still* obtain location information from WiFi scans if WiFi connectivity is on.

d. In recent versions of Android, individual Google apps ask for the user's permission to use their location data. A reasonable inference is that, if the user denies this app-level permission to an app, that app will not be able to use the user's location. But this is not true—Google apps that are denied permission by the user can still obtain location information from other Google apps and products that *have* been granted permission.

e. The "off means coarse" deception also manifests in ads personalization. As explained above, Google serves personalized ads to its users based in part on information Google has about a user's location. Google purports, however, to allow users to opt out of ads personalization by turning off a setting of that name ("GAP"). But contrary to what a reasonable user would expect, turning ads personalization off does not stop Google from presenting ads based on a user's location. Rather, Google will instead

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

f. Users are more likely to disable their device's location setting if they are readily offered such a setting. This was demonstrated by a substantial increase in devices with location turned off in versions of Android that included a location toggle in the device's easily accessed Quick Settings pane. Google viewed the large increase as a problem to be solved, so it removed this setting from the Quick Settings pane of devices it manufactured, and it sought—successfully—to convince other manufacturers using Android to do the same on the basis of false and misleading information.

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

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

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

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

III. FACTUAL ALLEGATIONS

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

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

a. Google sells its own Android devices to consumers in Arizona, and those devices both run Google's proprietary forks of the Android operating system and come preloaded with several Google apps. As part of activating and setting up their phones after purchasing them for consideration, consumers purportedly "consent" to the settings described herein that result in Google's collection of location data. Google's acts, practices, representations, and omissions regarding those settings, including during setup, are thus in connection with the sale of Google's Android phones.

b. Google creates both software that is part of the Android operating system (*i.e.*, proprietary forks) and also Google apps that it causes to be included on Android devices sold by other manufacturers to consumers in Arizona. As part of activating and setting up those devices after purchasing them for consideration, consumers purportedly "consent" to the settings described herein and Google's collection of location data. Google's acts, practices, representations, and omissions regarding those settings are thus in connection with the sale of certain third-party Android phones.

c. Google advertises the devices and software described in (a) and (b), *supra*, to consumers. Google also advertises software that runs on other operating systems (*e.g.*, iOS). Google's acts, practices, representations, and omissions when advertising devices and software are thus in connection with the advertisement of merchandise.

d. Google sells ad placements (*i.e.*, "merchandise") to third parties for consideration (Google's principal business), which advertisements are powered by the fruits of the

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

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

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

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

- Google Pixel family
  - Pixel C (released 2015)
  - Pixelbook (released 2017)
  - Pixel Slate (released 2018)
  - Pixel 1 (released 2016)
  - Pixel 2 (released 2017)
  - Pixel 3 (released 2018)
  - Pixel 4 (released 2019)
- Google Nexus family
  - Nexus One (released January 2010)
  - Nexus S (released December 2010)
  - 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 former Vice President of Product for Maps and current Vice President of Product for Ads, Jack Menzel, 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 Menzel 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 Berlin EUO Tr. at 327:17–18 ("'Service' and 'product' are used interchangeably at Google.").

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

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

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

30. Google causes its preferred versions of Android to be pre-installed on many smartphones, and forbids OEMs from pre-installing any Google apps (such as Search or Maps) on other versions of Android. Google has a large incentive to do this: its own version of Android contains Google Mobile Services ("GMS"), which makes it easier for Google to collect location information from users.[2] Indeed, whenever a user of an Android phone with GMS wants to share their location with a third-party, they must also share it with Google. 2/28/2020 Berlin EUO Tr. at 444:8–445:9; *see also* Ex. 201 (GOOG-GLAZ-00149241) (Google employee expressing confusion about whether sharing location with third-party apps requires also sharing location with Google, and complaining that he cannot find any public disclosures addressing his concern—"So there is no way to give a third party app your location and not Google? This doesn't sound like something we would want on the front page of the NYT.").

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

[2] GMS "is a collection of apps and services that an OEM is required to have to . . . license Android." 9/25/2019 Chai EUO Tr. at 139:1–6. That collection includes "software libraries, APIs, and other 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 Chai EUO Tr. at 83:11–89:14.

39. Location History in particular is central to Google's revenue stream. Among other things, [redacted] Ex. 204 (GOOG-GLAZ-00085882) at 882.

40. "Using [redacted] and Location History, [Google] ha[s] built the world's largest graph of people/places by inferring [redacted]" *Id.*

41. "[redacted] is used by [redacted] clients across the company in Geo, Ads, Search, Android, YouTube, Nest, Waymo, Research, Photos, and Social." *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 ("understanding the Smorgasbord of consents").

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

- "Real people just think in terms of 'location is on', 'location is off' because that's exactly what you have on the front screen of your phone." 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.

- "Some people (including even Googlers) don't know that there is a global switch and a per-device switch." Ex. 208 (GOOG-GLAZ-00055552) at 553.
- [redacted] Ex. 209 (GOOG-GLAZ-00057477) at 477.
- "Today, collection of device usage and diagnostic data is smeared across 5 settings resulting in conditions that are difficult for Googlers, let alone users, to understand." Ex. 210 (GOOG-GLAZ-00057940) at 940.
- Android location settings "can be overly complicated" in context of "recent location requests" in part because "a user cannot turn off location for Google Play Services." 9/25/2019 Chai EUO Tr. at 275:9–277:6.
- [redacted] Ex. 211 (GOOG-GLAZ-00017790) at 790–91.
- [redacted] Ex. 212 (GOOG-GLAZ-00161717) at 717.
- [redacted] Ex. 213 (GOOG-GLAZ-00028891) at 896–97.
- [redacted] Ex. 214 (GOOG-GLAZ-00101814) at 14.
- "So our messaging around [location tracking] is enough to confuse a privacy focused Google-SWE. That's not good." Ex. 215 (GOOG-GLAZ-00163209) at 213.

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

46. Though Google has published a variety of documentation for users, [redacted] *See* Ex. 216 (GOOG-GLAZ-00078009) at 037 [redacted] 059 [redacted] Ex. 214 (GOOG-GLAZ-00101814) at 814 [redacted]

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

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

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

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

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

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

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

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

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

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

56. Even Google's CEO Sundar Pichai was directly involved in the aftermath of the publication of the AP article. Mr. Pichai called a "code yellow" meeting to get "constant" updates on the issues covered by the article from his direct reports, including from Jen Fitzpatrick, the Senior Vice President of Geo and Maps. 3/6/2020 Menzel EUO Tr. at 176:10–178:11.

[3] https://apnews.com/828aefab64d4411bac257a07c1af0ecb/AP-Exclusive:-Google-tracks-your-movements,-like-it-or-not.

57. [redacted]

Ex. 24 (GOOG-GLAZ-00001458) at 464–65. [redacted]

Id. at 466.

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

59. Testimony from Google employees and Google's internal documents confirm the conclusion of the AP story. 7/11/2019 McGriff EUO Tr. at 139:13–17 ("Q. When Location History is turned off, does that affect whether Google stores location data for purposes of other products other than Location History? A. No."). Indeed, [redacted] Ex. 220 (GOOG-GLAZ-00057237) at 238; *see also* Ex. 221 (GOOG-GLAZ-00146003) at 007 [redacted] Ex. 213 (GOOG-GLAZ-00028891) at 894–95 [redacted]

60. Even apart from WAA, if Location History is off, Google still captures a user's precise location. Ex. 222 (GOOG-GLAZ-00069965) at 965 (Google Maps captures details about a user's navigation).

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

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

- "Indeed we aren't very good at explaining this to users. Add me to the list of Googlers who didn't understand how this worked an [sic] was surprised when I read the article . . . we shipped a UI that confuses users"). *Id.* at 290.
- [redacted] Ex. 223 (GOOG-GLAZ-00057861) at 861.
- "The complaint in this article is that if you have Web and App Activity enabled and the location toggle enabled, then your search history entries contain your approximate location at the time you made a query. It's also not possible to remove them by clearing your location history, which is counter-intuitive – you have to clear your search history instead." Ex. 224 (GOOG-GLAZ-00149867) at 868.
- "Definitely confusing from a user point of view if we need googlers [to] explain it to us." *Id.* at 867.
- "I agree with the article. Location off should mean location off, not except for this case or that case." Ex. 18 (GOOG-GLAZ-00001266) at 270.
- "[C]omms and policy are looking for an update on where we are in terms of fixing 'location history' fixes and having one single place to turn off instead of 3." Ex. 20 (GOOG-GLAZ-00001521) at 523.

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

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

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

64. Additionally, until Android Q, an Android user could not directly access the WAA settings on his phone. 7/12/2019 Monsees EUO Tr. at 164:16–166:19.[4] Instead, a user would have to navigate to the device's settings, then to a Google link which took the user to his Google Account, then navigate down to WAA. *Id.*

65. [redacted], David Monsees, [redacted] Ex. 226 (GOOG-GLAZ-00107030) at 030 [redacted][5]

66. Furthermore, Google has, on multiple occasions, changed the quality and granularity of data collected through WAA without disclosing these changes to users. Before 2014, Google collected "coarse" location information from a user's WAA. 7/12/2019 Monsees EUO Tr. at 182:23–194:12. Sometime in 2014 or 2015, Google began collecting precise (or "transactional") location data through WAA. *Id*. In early 2019, Google reverted to collecting only coarse location data from WAA. *See id*. at 183:24–184:10; Ex. 227 (GOOG-GLAZ-00084080) at 1 [redacted]

67. The change to collecting precise location data in 2014 or 2015 was explicitly tied to, and in part driven by, Google's desire to "increas[e] the accuracy of locations served on Search and Ads, in turn improving the search experience and increasing Ads revenue." Ex. 228 (GOOG-GLAZ-00106193) at 194.

68. Notably, Google did not make "any changes to the privacy policy, terms and conditions, help desk or help center website . . . that reflected the change." 7/12/2019 Monsees EUO Tr. at 195:11–

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

[5] Footprints is Google's internal name for the database that stores the information collected by Web & App Activity. 7/12/2019 Monsees 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. And users who ***disable*** WAA still have their activity (and related location information) logged. [redacted] Kevin Berlin, a Staff Privacy Engineer at Google, confirmed this to be true: when a user disables WAA, the user's queries, along with associated IP address and location information, is stored in a database called "Sawmill" and associated with the user's Zwieback cookie ID, instead of their usual GAIA ID. 2/27/2020 Berlin EUO Tr. at 52:22–58:13.[6] This cookie "is established with a life span of 18 months" during which the same Zwieback ID could be traced through time. *Id.* at 55:3–13. Further, the same Zwieback ID is shared across Google's data stores. *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 Chai 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 Berlin 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.

the WiFi Scanning setting controls whether "system apps and third-party apps can request WiFi scans."[7] *Id.* at 117:4–118:5.

72. Google's written disclosures at most suggest to users only that WiFi Scanning (as opposed to WiFi connectivity) is related to location data. Ex. 230 (GOOG-GLAZ-00001105) at 106 ("To help apps get better location info, you can let your device scan for nearby Wi-Fi access points . . . Tap Advanced > Scanning . . . Turn Wi-Fi scanning . . . on or off"). But Google still collects user location data through WiFi connectivity, even where the user has disabled WiFi Scanning.

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

74. However, Google Location Accuracy (GLA; formerly known as Google Location Services) gets location data from WiFi scans when ***either*** the WiFi Scanning setting or WiFi connectivity setting is on. 9/25/2019 Chai EUO Tr. at 88:23–89:10. If WiFi Scanning is ***off***, "Google will periodically collect WiFi scans in order to build the estimated location for where WiFi Access Points are," so long as other toggles (*e.g.*, GLA and WiFi connectivity) are on. *Id.* at 91:2–7. Further, as of at least November 1, 2017, "if Device Location is OFF, but Wifi Scanning (under location settings) is ON, then although Location doesn't request any wifi scans, other system apps CAN get wifi scans (and possibly 3P apps that target SDK 22 and below)." Ex. 43 (GOOG-GLAZ-00031017) at 022.

75. Thus, despite the user attempting to prevent the reporting of WiFi-based location data—and despite the user affirmatively turning the Location Master off—Google continues to collect the users' location data via WiFi connectivity.

---

[7] [redacted] Ex. 231 (GOOG-GLAZ-00109617) at 617. [redacted] *Id.*

[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/.

76. In short, the separation of the WiFi Scanning and WiFi connectivity settings misleads users into providing location data to Google even if they do not want to. Google's disclosures suggest disabling "WiFi Scanning" will prevent Google from scanning nearby WiFi access points. But Google will collect location data via WiFi, so long as GLA is enabled and one of either WiFi scanning or WiFi connectivity is enabled.

77. [redacted] and "a bit of a mess that we are working to clear up." *See* Ex. 43 (GOOG-GLAZ-00031017) at 020–21. [redacted] *Id.* at 021.[9] Even Jen Chai (senior product manager for location and a corporate designee for these topics), does not know how the three relevant location-related settings (Location Master, WiFi Scanning, and WiFi connectivity) interact with each other. *Id.* at 021–22.[10]

78. In addition to deceiving consumers through the WiFi setting described above, by collecting location through WiFi connectivity, Google makes it so a user cannot opt out of this form of location tracking unless the user actually completely disables the WiFi functionality on his or her device—meaning the device cannot connect to the internet through WiFi. *Id.* at 021.

D. Google Uses Its Users' Locations Even When Users Turn Off the Relevant Permissions

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

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

[9] Android P became publicly available on August 6, 2018. https://www.theverge.com/circuitbreaker/2018/8/6/17656294/essential-phone-android-9-pie-update-now-available.

[10] In response to a notice to examine Google under oath pursuant to A.R.S. § 44-1524, Google designated Ms. Chai 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 Chai 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] 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] Ex. 45 (GOOG-GLAZ-00005829) at 829–32 [redacted] Ex. 234 (GOOG-GLAZ-00060013) at 013 [redacted] Ex. 114 (GOOG-GLAZ-00198467) at 469 [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]

[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 IPGeo signals. *See* 2/27/2020 Berlin EUO Tr. at 117:1–3, 119:17–19. IPGeo, in turn, is a service within Google that maps IP addresses to geographic locations. *See id.* at 98:19–99:4.

82. [redacted] Ex. 45 (GOOG-GLAZ-00005829) at 829. In technical terms, [redacted] (Ex. 238 (GOOG-GLAZ-00027688) at 689)—[redacted] Ex. 232 (GOOG-GLAZ-00027697) at 697; *see also* Ex. 214 (GOOG-GLAZ-00101814) at 814 [redacted]

83. [redacted] Ex. 45 (GOOG-GLAZ-00005829) at 829 [redacted]

84. Sundar Pichai—[redacted] *See* Ex. 47 (GOOG-GLAZ-00033771) at 772 [redacted] Sundar [redacted] On information and belief, Mr. Pichai did not direct Google to correct these "borrowed" permissions, nor has Google done so.

85. [redacted] Ex. 235 (GOOG-GLAZ-00150448) at 452 [redacted]

86. In short, Google misleads its users to believe that they have disabled the localized experience for a particular app when in reality their location data from other apps is being used without the users' knowledge and in contradiction to the users' expressed wishes. *Id.* at 450 [redacted]

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

87. At one point, Google claimed that one of its "User Privacy Principles" is that "Location off means OFF": "Don't store or deliver locations to apps in Android or other end points when not requested, needed, or expected by the user." Ex. 239 (GOOG-GLAZ-00037593) at 640. And Google consistently makes representations that location data is collected and stored only when the respective settings are turned on. *E.g.*, Ex. 8 at 1 ("With Location History off, the places you go are no longer stored"); Ex. 72 (GOOG-GLAZ-00000715) at 718 ("The types of data we collect depend in part on your device and account settings. For example, you can turn your Android device's location on or off using the device's settings app").

88. Thus, a reasonable belief for users is that, when they turn their device's Location Master off, Google no longer collects, stores, or uses any location information. [redacted] Ex. 240 (GOOG-GLAZ-00157550) at 550; *see also* Ex. 69 (GOOG-GLAZ-00096793) at 807 (chart explaining that Google will use "coarse location" information even when "a user has said not to use location").

89. Moreover, users of Google's products have absolutely no control over whether Google can use their IP addresses to derive a location and serve ads based on that location. 5/8/2020 Rothfuss EUO Tr. at 271:23–272:1 ("Q. Is it true that a Google user cannot turn off the collection of location data based on his or her IP address? A. Yes, that is correct."); 2/28/2020 Berlin EUO Tr. at 517:15–23 ("Q. Is there anything a user can do to completely prevent [redacted] from passing along some of that user's information -- location information to [redacted]? . . . A. So [redacted] passing location -- no, user cannot control the flow of information from [redacted] to [redacted]."); 5/21/2020 Hennessy Rough EUO Tr. at 98:4–6 ("The user does not for Google have the ability to opt out of the use of IP-derived locations.").

90. Using its IPGeo service, which "approximates user location based on the assignment of IP blocks to geographic areas," Google can assign a location to an individual IP address with (at least) postal code granularity, even when device location is off. *See* Ex. 241 (GOOG-GLAZ-00097091) at 092.

91. [redacted]

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

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

93. As another example, Google infers a user's extremely sensitive home and work locations without consent. Not only does Google still infer these locations when a user turns off Location History (Ex. 84 (GOOG-GLAZ-00079712) at 712 ("[redacted] . . . infers work/home locations . . . even if the user has since turned off location history")), but it also does so when a user turns off *all* of a device's location-related settings. Jack Menzel, Google's former Vice President of Product for Maps and current Vice President of Product for Ads, confirmed the foregoing; he testified that the only way for Google to ***not*** infer a user's home and work is for that user to "set . . . home and work to arbitrary locations." 3/6/2020 Menzel EUO Tr. at 378:14–379:6.

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

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

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

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

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

98. Such a toggle implies that the user has control over whether Google will serve ads based on the user's location. But "[e]ven if a user opts out of ads personalization (GAP off) they can still be targeted based on the finer areas (e.g. CITY or METRO)." Ex. 70 (GOOG-GLAZ-00085629) at 636.

99. Indeed, as confirmed by Karin Hennessy, the product manager for ads privacy and safety, even if a user opts out of ad personalization, Google ***still*** uses the user's real-time location to serve ads. 5/21/2020 Hennessy Rough EUO Tr. at 114:9–115:11. This is, unfortunately, not surprising, as "geo-targeting"—or targeting a user based on his location—is a "critical dimension" of ads. *Id.* at 84:14–19.

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

101. Ads served in the latter category are controlled by a separate DoubleClick setting—one that is not accessible through a user's Google Account. 2/27/2020 Berlin EUO Tr. at 163:6–16, 167:8–22. Instead, users must click on a link in the ad itself, navigate to another website, and turn off the setting there. *Id.*

102. Thus, when a user turns off GAP—expecting that Google will stop showing her ads based on her location—not only does Google continue to present location-targeted ads (now based on "CITY or METRO" areas), but it also continues to serve ads on third-party websites via DoubleClick based on the user's more precise location. 2/27/2020 Berlin EUO Tr. at 172:2–15 (when GAP is off, Google still targets users with ads based on their location through DoubleClick).

103. And even if a user figures out how to turn off the DoubleClick location setting, Google will ***still*** target her via DoubleClick based on her "coarse" location. 2/27/2020 Berlin EUO Tr. at 189:18–190:17.

104. Google employees recognized that this behavior runs counter to users' expectations, and users would "freak out" if they learned the truth. Ex. 70 (GOOG-GLAZ-00085629) at 638 ("[o]ne thing to keep in mind: we probably don't want it to be seen as hiding information from the user. As in: we estimate where you are at the zip code level, but we will not show you very local ads so that you don't freak out").

E. Google Automatically Changes the State of Permissions Without Notifying Users

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

106. For example, in August 2016, Google modified the behavior of the device-level supplemental Web & App Activity setting (sWAA) so that the setting is automatically enabled (*i.e.*, toggled "on") for ***all*** devices associated with a given user, so long as the user has enabled sWAA at the account level. Ex. 79 (GOOG-GLAZ-00057389) at 389; *see also* Ex. 246 (GOOG-GLAZ-00058103) at 104 ("As of Aug 2016, switching the account level sWAA bit will toggle the device-level sWAA for all devices owned by the GAIA" resulting in "a fairly large increase in devices reporting appusage [sic] since Aug").[13] To illustrate the problem, a user who is logged into her Google Account on a laptop may

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

enable sWAA at the account level, without realizing that doing so will now enable sWAA for all of the user's other devices—even if the user previously disabled the device-level setting on her other devices. Worse yet, Google does not notify users of this change—at least not in any disclosures relating to location or privacy settings—much less seek and obtain user consent. Ex. 79 (GOOG-GLAZ-00057389) at 389.

107. In another example, in around 2017, Google unilaterally changed the setting for Location Reporting on Apple iOS devices. Location Reporting ("LR," Location History's corresponding device-level sub-setting that enables uploading of LH data from a specific device when enabled) was defaulted to "off" for new iOS devices. Ex. 78 (GOOG-GLAZ-00070610) at 610. [redacted] *Id.* [redacted] *Id.*; *see also* Ex. 248 (GOOG-GLAZ-00070491) at 491 [redacted]

108. Although Google's purported justification for auto-enabling this setting was to get users into the state that they were in before they bought a new iOS device, Google did nothing to verify whether users actually wanted to leave their LR setting off. 3/6/2020 Menzel EUO Tr. at 286:19–287:24, 290:14–291:24.

109. [redacted] Ex. 249 (GOOG-GLAZ-00125482) at 490 [redacted] Ex. 250 (GOOG-GLAZ-00065187) at 192 [redacted]

---

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

[redacted] Ex. 251 (GOOG-GLAZ-00127414) at 414–16 [redacted]

F. Google Changes the Android User Interface to Increase Location "Attach Rates" 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. As part of its updates to the Android operating system, Google modifies its user interface by, *inter alia*, changing the user-facing text surrounding settings, altering the flow through device settings, and otherwise updating or moving toggles and other settings. [redacted] Ex. 51 (GOOG-GLAZ-00026768) at 769–72 [redacted]

112. One way Google defines the "location attach rate" is "the percent of devices that have the device location setting [*i.e.*, the device-level Location Master] on." 9/25/2019 Chai 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 Chai 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.

the Location Master; [redacted] Ex. 51 (GOOG-GLAZ-00026768) at 772; Ex. 71 (GOOG-GLAZ-00027187) at 196 (identifying "concern[] about privacy" as one of the top two reasons why users turn off location).

114. [redacted] Ex. 51 (GOOG-GLAZ-00026768) at 768–72. [redacted] Ex. 61 (GOOG-GLAZ-00026360) at 360. [redacted] *Id.* at 361 [redacted][15]

115. Nevertheless, Google moved ahead with the decision to remove the location toggle. Accomplishing this removal was simple for Google's own Pixel, as that smartphone is made in-house, [redacted] *See* Ex. 52 (GOOG-GLAZ-00005425) at 428; *see also* Ex. 252 (GOOG-GLAZ-00028327) at 327 [redacted]

116. [redacted] Ex. 52 (GOOG-GLAZ-00005425) at 429. [redacted]

117. [redacted] Ex. 51 (GOOG-GLAZ-00026768) at 785; *see also* 9/25/2019 Chai EUO Tr. at 238:10–239:3; Ex. 253 (GOOG-GLAZ-00028014) at 014–25 [redacted]

[15] The Privacy Working Group is a collection of personnel at Google that offers advice on privacy requirements for Google's products.

[redacted]

118. [redacted] Ex. 254 (GOOG-GLAZ-00115868) at 868 (sheet1, cell G14). [redacted] Ex. 53 (GOOG-GLAZ-00026843) at 850. [redacted] *Id*. at 847–50. [redacted] *See id.* at 846–47.

119. [redacted] Ex. 255 (GOOG-GLAZ-00027518) at 518; Ex. 256 (GOOG-GLAZ-00029585) at 615.

120. Google also successfully pressured LG to move the location toggle to the second page. [redacted] Ex. 257 (GOOG-GLAZ-00032539) at 539.

121. [redacted] Ex. 52 (GOOG-GLAZ-00005425) at 431. [redacted] *Id.* at 426. [redacted] *Id.* at 426. [redacted]

[redacted] *Id.* at 425.

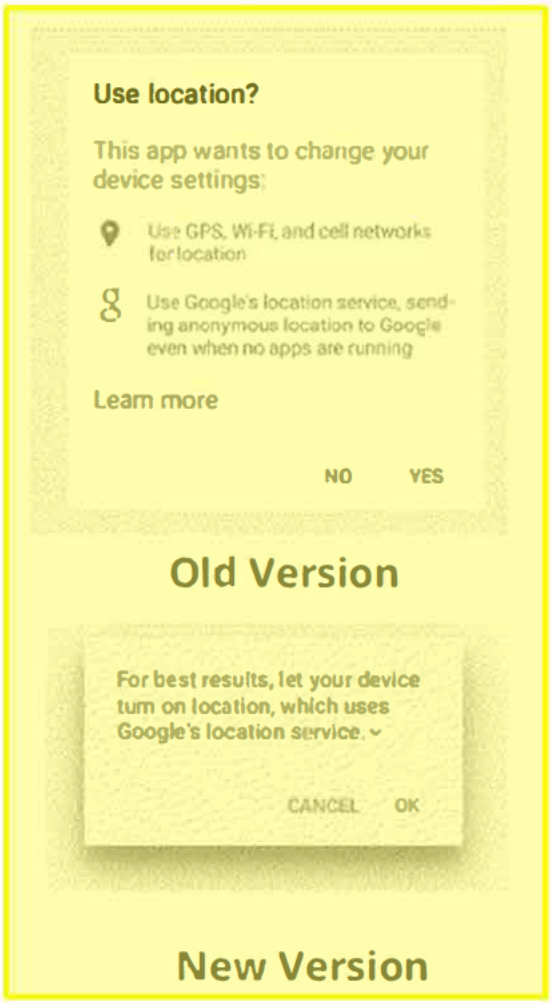
122. [redacted] *See, e.g.*, Ex. 53 (GOOG-GLAZ-00026843) at 844 [redacted]

123. At bottom, Google's efforts were intended to deemphasize the prominence of location settings because Google's own research showed that users are more likely to disable location settings when presented with a clear option to do so. Google tried to convince these carriers and manufacturers to conceal the location settings—or make them less prominent—through active misrepresentations and/or concealment, suppression, or omission of facts available to Google concerning user experience in order to assuage their privacy concerns. In reality, Google was simply trying to boost the location attach rate, which is critical for Google's own advertising revenue.

124. [redacted] Ex. 254 (GOOG-GLAZ-00115868) at 868 (sheet1, rows 12–14). [redacted] *See* Ex. 61 (GOOG-GLAZ-00026360) at 361 [redacted] (emphasis in original).

125. Google also changed the UI of in-app prompts in order to drive up location attach rates at the expense of users' exposure to information. [redacted] Ex. 256 (GOOG-GLAZ-00029585) at 595.

126. [redacted]. *Id.* [redacted]



Id.

127. [redacted] *Id.*

128. Thus, Google was able to increase its location attach rates by misleading OEMs, withholding information from users, and making it more difficult for users to control their own location settings.

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] 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

it has collected and stored. Ex. 36 (GOOG-GLAZ-00000001) at 001–02 ("We'll keep this data in your Google Account until you choose to remove it," "[w]hen you delete data in your Google account, we immediately start the process of removing it from the product and our systems"); *see also* Ex. 202 (Google's Responses to CIDs 1–3) at 79–80 (9/47/2019 response to DFI 10 from the Third CID) ("For users that have Web & App Activity enabled, Google saves their search results and associated location information in the users' Google Accounts. Users can delete that data at any time.").

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

131. While that by itself is misleading and deceptive, what is worse is that Google's user-facing interface displays data being deleted immediately—opposite to what Google actually does. Ex. 59 (GOOG-GLAZ-00031110) at 124 ("[i]f Location History data gets deleted, how long does it take to wipe? Internal: [redacted] External: Stop showing the data in the product UI immediately"). [redacted] Ex. 258 (GOOG-GLAZ-00065293) at 295 [redacted] (emphasis in original).

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

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

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

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

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

- [redacted] Ex. 259 (GOOG-GLAZ-00078007) at 807.
- [redacted] Ex. 216 (GOOG-GLAZ-00078009) at 018.
- [redacted] Ex. 260 (GOOG-GLAZ-00057339) at 340.
- [redacted] Ex. 270 (GOOG-GLAZ-00055829) at 851.
- [redacted] Ex. 261 (GOOG-GLAZ-00099239) at 239.
- [redacted] Ex. 262 (GOOG-GLAZ-00117506) at 506.

135. Google has known about these issues since at least 2012. Ex. 263 (GOOG-GLAZ-00100799) at 800 [redacted]

136. [redacted] Sundar Pichai (CEO of Google and parent Alphabet) [redacted] Ex. 260 (GOOG-GLAZ-00057339) at 339. Mr. Pichai [redacted]

- Simplifying device-level location data settings. *Id.* at 339 [redacted] Sundar [redacted]

[redacted] Ex. 264 (GOOG-GLAZ-00048459) at 478 (stating that the opt-in process for the Google Now product was "reviewed with Sundar").

- [redacted] *Id.*; Ex. 265 (GOOG-GLAZ-00078761) at 761 [redacted] Sundar [redacted]; Ex. 266 (GOOG-GLAZ-00151516) at 517 ("Sundar [redacted]
- The 2018 AP Article and the interaction between WAA and LH. Ex. 23 (GOOG-GLAZ-00001371) at 373 ("Sundar asked that we have a 'Location' code yellow update in Leads" in response to the AP News Cycle); Ex. 267 (GOOG-GLAZ-00035559) at 559 (email chain regarding LH/WAA interaction meeting with Sundar); Ex. 268 (GOOG-GLAZ-00078652) at 52 (notes regarding LH/WAA interaction, including Sundar's opinion).
- [redacted] Ex. 47 (GOOG-GLAZ-00033771) at 72[redacted] Sundar [redacted]
- [redacted] Ex. 269 (GOOG-GLAZ-00073037) at 037–43 ([redacted]
- [redacted].

IV. ARIZONA'S INVESTIGATION INTO GOOGLE'S UNFAIR AND DECEPTIVE ACTS AND PRACTICES

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

138. Thereafter, the AGO served a First Civil Investigative Demand ("CID") on Google on January 30, 2019 to investigate Google's location data collection practices.

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

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

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

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

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

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

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

144. Similarly, when the AGO requested information concerning ad revenue early in the investigation, Google objected that it "does not understand, and the AGO has not provided any guidance, regarding any nexus of revenue from the Android mobile devices and location information." Ex. 202 (Google's Response to CIDs 1–3) at 51 (5/30/2019 response to RFP 19 from the First CID). As detailed herein, the AGO's investigation ultimately shows that Google invests extensive resources toward increasing the "location attach rates" on Android mobile devices in order to increase Google's advertising revenue. Indeed, employing user location data for "geo-targeting" is a "critical dimension" for Google's advertising platforms in order for advertisers "to scope where they are marketing to." 5/21/2020 Hennessy Rough EUO Tr. at 84:15–19.

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

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

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

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

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

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

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

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

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

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

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

[16] Mr. Berlin spoke with Mr. Rothfuss regarding [redacted], but Mr. Rothfuss, the leader of the [redacted] team, later testified that he only spends about 10% of his day-to-day work on [redacted] and led the [redacted] team only because his direct report actually oversees it; indeed, Mr. Rothfuss had very little actual knowledge on the workings of [redacted] and made clear he only exercised a general managerial role. 5/8/2020 Rothfuss 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.

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

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

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

V. CLAIM FOR RELIEF

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

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

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

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

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

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

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

a. Engaging in deceptive and unfair acts and practices by making the deceptive misrepresentation and false promise that "[w]ith Location History off, the places you go are no longer stored," when in fact Google continued to collect and store user location information even with Location History turned off.

b. Concealing, suppressing, or omitting the material fact that Google continued to collect and store user location information even with Location History turned off.

c. Concealing, suppressing, or omitting during account creation the material fact that location information was collected through Web & App Activity—which defaulted to "on."

d. Engaging in deceptive and unfair acts and practices by making the deceptive misrepresentation and false promise that users "can turn [their] Android device's location on or off using the device's settings app" despite the fact that Google continued to collect "coarse" location information even when the device's location is turned off.

e. Concealing, suppressing, or omitting the material fact that Google continued to collect "coarse" location information even when the device's location is turned off.

f. Engaging in deceptive and unfair acts and practices by automatically turning on location-relating settings, including Location Reporting and supplemental Web & App Activity, without informing or obtaining consent from users.

g. Concealing, suppressing, or omitting the material fact that Google automatically turned on location-relating settings, including Location Reporting and supplemental Web & App Activity, without informing or obtaining consent from users.

h. Engaging in deceptive and unfair acts and practices by knowingly maintaining a misleading and diverse array of settings related to location tracking that makes it difficult if not impossible to understand the conditions in which Google will collect location data.

i. Concealing, suppressing, or omitting the material facts about the conditions in which Google will collect location data.

j. Engaging in deceptive and unfair acts and practices by manipulating the User Interface of location settings and information to make it more difficult for users to turn them off—and attempting to convince OEMs to do the same on the basis of false and/or misleading representations.

k. Concealing, suppressing, or omitting the material fact that location settings were on.

l. Engaging in deceptive and unfair acts and practices by failing to disclose that Google apps that have been denied permission to access location data can still obtain that data from other Google apps that have been granted permission.

m. Concealing, suppressing, or omitting the material fact that Google apps that have been denied permission to access location data can still obtain that data from other Google apps that have been granted permission.

n. Engaging in deceptive and unfair acts and practices by knowingly maintaining a confusing and misleading presentation of the WiFi scanning and WiFi connectivity settings that fails to disclose that location data can be obtained through WiFi connectivity even when WiFi scanning is off.

o. Concealing, suppressing, or omitting the material fact that Google obtains location data through WiFi connectivity even when WiFi scanning is off.

p. Engaging in deceptive and unfair acts and practices by continuing to present location-based advertisements to users even after they have opted out of ad personalization, and maintaining two separate settings relating to location-based advertising that users find confusing, to the extent that they are even aware of them at all.

q. Concealing, suppressing, or omitting the material fact that Google would continue to collect and store users' location information unless they disabled two separate settings relating to location-based advertising, and that even with both settings disabled Google would still use user location data to target ads.

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

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

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

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

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

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

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

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

PRAYER FOR RELIEF

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

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

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

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

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

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

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

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 Sloot
Assistant Attorneys General

Guy Ruttenberg (CA Bar No. 207937)
(*pro hac vice* application forthcoming)
Michael Eshaghian (CA Bar No. 300869)
(*pro hac vice* application forthcoming)
RUTTENBERG IP LAW, A PROFESSIONAL CORPORATION
1801 Century Park East, Suite 1920
Los Angeles, California 90067
Telephone: (310) 627-2270
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

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