

STATE OF INDIANA )  
 )  
COUNTY OF MARION )

IN THE MARION SUPERIOR COURT  
CAUSE NO. \_\_\_\_\_

STATE OF INDIANA, )  
 )  
Plaintiff, )  
 )  
v. )  
 )  
GOOGLE LLC, )  
 )  
Defendant. )

**JURY TRIAL DEMANDED**

**COMPLAINT FOR CIVIL PENALTIES, INJUNCTION, RESTITUTION,  
DISGORGEMENT, COSTS AND OTHER RELIEF**

**Table of Contents**

INTRODUCTION ..... 3

PARTIES ..... 6

JURISDICTION AND VENUE ..... 7

FACTUAL ALLEGATIONS ..... 7

    A. Google’s Business Model Relies on Constant Surveillance of Its Users.....7

        1. Overview of Google's Location-Related Settings.....8

        2. Collection of Data Via Google Products and Services.....9

        3. Value of Location Data.....11

    B. Google Consumers Must Navigate Numerous, Conflicting Controls to Protect Their Privacy.....12

        1. Location-Related Google Account Settings..... 12

        2. Location-Related Device Settings..... 14

    C. Google Deceives Consumers Regarding Their Ability to Protect Their Privacy Through Google Account Settings. .... 16

        1. Google Misrepresented and Omitted Material Facts Regarding the Location History and Web & App Activity Settings..... 16

        2. Google Misrepresents and/or Omits Material Facts Regarding Users’ Ability to Control Their Privacy through Google Account Settings. .... 25

        3. Google Misrepresents and Omits Material Facts Regarding the Google Ad Personalization Setting ..... 29

    D. Google Deceives Consumers Regarding Their Ability to Protect Their Privacy Through Device Settings..... 30

    E. Google Deploys Deceptive Practices that Undermine Consumers’ Ability to Make Informed Choices About Their Data..... 32

        1. Dark Patterns in Google Account Settings ..... 33

        2. Dark Patterns in Device Settings. .... 38

CAUSES OF ACTION ..... 42

PRAYER FOR RELIEF ..... 48

JURY DEMAND ..... 50

The State of Indiana (“Indiana”), through the Attorney General Theodore E. Rokita, by Deputy Attorneys General Douglas Swetnam, Vanessa Voigt Gould, and Jennifer Van Dame, brings its Complaint against Google LLC (“Google” or the “Company”) pursuant to the Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5-1 et seq. (“DCSA”) for civil penalties, injunctive relief, consumer restitution, disgorgement, costs and other relief.

### **INTRODUCTION**

1. Indiana’s DCSA “shall be liberally construed and applied to promote its purposes and policies.” Ind. Code § 24-5-0.5-1(a).

2. The purposes and policies of the DCSA include protecting “consumers from suppliers who commit deceptive and unconscionable sales acts” and encouraging “the development of fair consumer sales practices”. Ind. Code § 24-5-0.5-1(b).

3. This action is brought against Google for their use of deceptive and unfair acts and practices to obtain valuable consumer location data, in violation of Ind. Code § 24-5-0.5-3.

4. Google is primarily known as a technology company, which provides a range of consumer products, including the Android operating system, web-based services and applications (like Gmail and the Google Search engine), and hardware such as Pixel and Nexus smartphones. The majority of Google’s revenues, however, derive from targeted advertising and advertising analytics. To support this lucrative arm of its business, Google harvests consumers’ personal data, including location data, when consumers use Google products. In turn, Google uses this data to “target” advertisements to consumers and to evaluate the effectiveness of these advertisements.

5. From at least 2014 through the present, Google has systematically misled, deceived, and withheld material facts from consumers regarding how their location is tracked and used by the Company, and how and to what extent consumers can protect their privacy by stopping Google’s tracking and use of their location. Google leads consumers to believe that they are in

control of what information Google retains about them and how it is used. In reality, there is effectively no way for consumers to prevent Google from collecting, storing, and profiting from their location data.

6. Location data is among the most sensitive information Google collects from consumers. Even a limited amount of such data, aggregated over time, can expose a person's identity and routines. Location can also be used to infer sensitive personal details, such as political or religious affiliation, sexual orientation, income, health status, or participation in support groups, as well as major life events, such as marriage, divorce, and the birth of children.

7. Location data is even more powerful in the hands of Google, a company that has an unprecedented ability to monitor consumers' daily lives due to the ubiquity of Google products in consumers' pockets, homes, and workplaces—essentially everywhere consumers go. Google's technologies allow it to analyze location data from billions of people, along with massive amounts of other data, to derive insights that consumers may not even realize they revealed. Google uses this window into consumers' lives to sell “targeted” advertising that is designed to exert the maximum influence over them, reaping spectacular gains at the expense of consumers' privacy.

8. Google has a powerful financial incentive to obscure the details of its location data collection practices and to make it difficult for consumers to opt out of being tracked. Google's ability to amass data about multitudes of consumers as they move throughout the world translates to improved advertising capabilities for the Company and an outsized share of the multi-billion-dollar digital advertising market. The Company's exhaustive surveillance practices are most effective, and therefore most lucrative, where consumers have no clear idea how to limit Google's access to their personal information.

9. The State of Indiana files this suit to correct the deceptive and unfair practices that Google has used to obtain consumers' location data and to ensure that consumers are able to both understand and control the extent to which their personal data—in particular, their location—is accessed, stored, used, and monetized by the Company.

10. Some of the issues giving rise to this lawsuit became broadly known to the public on August 13, 2018, when the Associated Press (“AP”) reported that Google “records your movements even when you explicitly tell it not to.” The reporting concerned Google’s “Location History” setting, a user control which allows Google to track a consumer’s location. Google promised consumers that “with Location History off, the places you go are no longer stored.” *See* <https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ecb> (last accessed January 21, 2022).

11. The AP story exposed that Google’s promise to consumers was false. Even when consumers had explicitly opted out of location tracking through the Location History setting, Google nevertheless recorded consumers’ locations via other means, including (but not limited to) a separate setting called “Web & App Activity.” When the Web & App Activity setting is enabled on a consumer’s Google Account, Google collects and stores a large swath of data about that consumer, including location data, whenever the consumer interacts with Google products and services. Although the Web & App Activity setting is automatically enabled for all Google Accounts, the Company’s disclosures during Google Account creation did not mention or draw consumers’ attention to this setting until 2018.

12. In the days following the AP report, [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

13. Multiple states subsequently commenced an investigation into Google’s location tracking practices. The states’ investigation revealed that while Google purports to offer consumers meaningful choices as to the data Google collects and uses through customizable controls, Google’s ambiguous, contradictory, and incomplete statements about these controls all but guarantee that consumers will not understand when their location is retained by Google or for what

purposes. In fact, Google's claims to give consumers "control" and respect their "choice" largely serve to obscure the reality that, regardless of the settings they select, consumers have no option but to allow the Company to collect, store, and use their location data.

14. With this suit, the State of Indiana seeks to put a stop to Google's deceptive and unfair practices; to ensure that consumers are no longer coerced into trading away their privacy; to force Google to disgorge all profits and benefits obtained from its unlawful practices; and to impose civil penalties for Google's violations of the DCSA.

### **PARTIES**

15. The Attorney General is authorized to bring actions on behalf of the State of Indiana pursuant to Ind. Code § 4-6-3-2.

16. The Attorney General is authorized to bring this particular action and to seek injunctive and other statutory relief pursuant to Ind. Code § 24-5-0.5-4.

17. Pursuant to Trial Rule 65(C), the State of Indiana by the Attorney General, as a government entity, need not post security to obtain injunctive relief.

18. Google is a Delaware limited liability company with its principal place of business at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

19. Google is also a foreign limited liability company registered with the Indiana Secretary of State.

20. Google regularly markets, advertises, offers, and provides its products and services throughout the United States and to Indiana consumers.

21. On information and belief, the number of Indiana consumers Google regularly engages in consumer transactions with is in the millions.

22. At all relevant times Google acted with the knowledge and understanding that the activities described in this Complaint would affect consumers of Google's products and services throughout the United States, including in Indiana.

## **JURISDICTION AND VENUE**

23. Google was and remains involved in consumer transactions in Indiana, as defined by Ind. Code § 24-5-0.5-2.

24. Google is registered as a foreign limited liability company with the Indiana Secretary of State.

25. Google, having purposefully directed its activities toward Indiana residents as detailed below, is subject to the jurisdiction of an Indiana court pursuant to Ind. Trial R. 4.4(A)(1).

26. Google transacted business within Indiana at all times relevant to this Complaint.

27. Google caused events to occur in Indiana out of which the claims detailed in this Complaint arose.

28. Venue is proper in this Court pursuant to Ind. Trial R. 75(A)(10).

## **FACTUAL ALLEGATIONS**

### **A. Google's Business Model Relies on Constant Surveillance of Google Consumers.**

29. Through its many consumer products, Google collects and analyzes the personal and behavioral data of billions of people. In turn, the Company uses this information to build user profiles and provide analytics that support Google's digital advertising business.

30. On information and belief, Google's advertising products generated nearly \$150 billion in revenue in 2020.

#### **1. Overview of Google's Location-Related Settings.**

31. Google's products include a system of interconnected settings that allow Google to collect a consumer's location data. These settings, individually and collectively, are in many cases deceptive, and their use by Google to collect a consumer's location data is unfair and deceptive.

32. Generally, the settings can be separated into three categories: (1) device-level, (2) account-level, and (3) app-level. Several of these settings are defaulted to allow the collection of location data. As seen with Location History (account-level) and Web & App Activity (account-level), *supra* ¶ 11, the settings can also directly contradict each other, so that when a consumer

disables location tracking on one setting, another setting may still be tracking the consumer's location.

33. Device-level settings are specific settings to an individual device, like a phone or tablet. The device-level settings at issue in this Complaint are specific to the Android operating system and/or devices marketed and sold by Google, like a Chromebook. While a consumer may use the same Google Account on many devices, the device-level settings can be turned on or off for a specific device. For example, a consumer might turn off the device-level location settings on her Pixel phone, but turn on these settings for her tablet.

34. Account-level settings apply to data collected from *any* device signed in<sup>1</sup> to a consumer's Google Account.

35. App-level settings are specific settings for an app. For example, Google Maps has its own app-level settings. An app-level setting can also apply to third-party apps that are installed on an Android device.

36. While there have been changes to settings over the years, below is a table of the settings relevant to this Complaint:

<b>Setting Name</b>	<b>Category</b>	<b>Description</b>
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 consumer's location.
Usage & Diagnostics	Device-level setting	When turned on, this setting purportedly helps Google improve the Android operating system ("OS"). It collects the consumer's IP addresses, which can be used to infer location.
Wi-Fi Scanning	Device-level setting	This setting allows apps and services to obtain Wi-Fi scans even when the Wi-Fi setting is off.

---

<sup>1</sup> A device (or consumer) is "signed in" to Google if the consumer has signed into the consumer's Google Account at device set-up or in connection with a Google app.



Bluetooth Scanning	Device-level setting	Like Wi-Fi Scanning, this setting allows apps and services to obtain Bluetooth scans even when the Bluetooth setting is off.
Location History	Account-level setting	When on, this setting captures all the places where a signed-in consumer goes. This location information is then used to create a personalized map for that consumer. It is a background setting that runs regardless of the apps being used.
Web & App Activity	Account-level setting	When this setting is on, Google saves a consumer's Google activity. For example, when a consumer 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 consumer's location and IP address.
Google Ad Personalization	Account-level setting	When off, this setting purports to prevent Google from targeting a consumer with ads based on the consumer's location.
App-level location permission	App-level setting	When on, this setting gives an app permission to access the corresponding device's location.

2. Collection of Location Data Via Google Products and Services.

37. Much of Google’s location data collection occurs by way of Google’s Android operating system (“Android” or “Android OS”). Android has been used on a majority of smartphones in the United States since approximately 2015.<sup>2</sup> The Android operating system is free and open-source software. However, most Android devices on the market include a suite of Google apps and application programming interfaces (“APIs”)<sup>3</sup> (collectively, “Google Mobile Services”) that are preinstalled on a consumer’s device under a licensing agreement between Google and Android device manufacturers (“OEMs”).

---

<sup>2</sup> The smartphone market is generally split between two operating systems (“OS”), Apple’s “iOS” and Google’s Android OS. Apple’s iOS is used on all iPhone and iPad devices.

<sup>3</sup> An API is a software interface that connects computers or pieces of software to each other.

38. The basic functioning of the Android OS provides Google with a steady stream of location data from Android devices. Through sensors and APIs installed on Android devices,<sup>4</sup> Google can track the precise location of a device and its owner on a continuous basis, using GPS coordinates, cell tower data, Wi-Fi signals, and other signals that the device transmits to Google.

39. Beyond Android devices, Google collects location data through other consumer products including apps and web-based services, such as Google Search, Google Maps, Chrome web browser, YouTube, Google Play Store, and Google Assistant, many of which can be used on both Android and Apple iOS devices (such as iPhones). These products are also critical to Google's ability to extract location data. Google collects and stores consumers' location data when they interact with certain Google apps and services, even when a consumer's location is not needed to support the core functionality of the app or service.

40. On Android devices, certain Google apps are granted permission to collect consumers' location data by default. Other Google apps ask permission from consumers to allow Google to collect location data. On many versions of Android, once apps are permitted to collect a consumer's location data, they may continue to collect and transmit location data to Google unless and until the consumer remembers to revoke permission. And if a consumer elects not to grant permission, an app may continue to prompt the consumer to enable location-related settings.

41. On Android devices, a user can also disable a "master switch" location setting that controls whether the device transmits location data from device sensors to Google. However, if a user takes this step, they cannot use any location-enabled services on their device, including location-enabled services on non-Google apps (such as Uber).

42. Furthermore, even if a consumer disables settings that allow their device to transmit location data to Google, Google *still* continues to estimate a consumer's location by using IP

---

<sup>4</sup> As used herein, the term "Android device" refers to mobile devices that use Google's Android OS and that come pre-installed with Google-licensed software and APIs (Google Mobile Services), including the Google Play Store and Google Play Services API.

address<sup>5</sup> information that is transmitted when the consumer interacts with many Google apps and services.

3. Value of Location Data.

43. Some of Google’s consumer products can be used at no direct financial cost to the consumer. But that does not mean that Google provides these products for free. Instead of charging money for its products, Google collects exhaustive personal data about its consumers when they engage with Google products. Google processes this data to draw inferences about individuals and groups of consumers that it monetizes through advertising and other services.

44. Google’s advertising business is dependent on its collection of this personal data, and location data is particularly valuable information for this business. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] In marketing materials directed at advertisers, Google actively promotes its ability to provide better advertising services through location-based analytics and geo-targeted consumer advertising.

45. Because location data is key to Google’s lucrative advertising business, the Company has a strong financial incentive to dissuade consumers from withholding access to that data. As detailed herein, Google has employed and continues to employ a number of unfair, abusive, and/or deceptive acts, omissions, and/or practices to obtain consumers’ “consent” to be tracked and to make it nearly impossible for consumers to stop Google from collecting their location data when using Google products. These practices include privacy-intrusive default location settings, hard-to-find location settings, misleading descriptions of location settings,

---

<sup>5</sup> An IP address is a unique address that identifies a device on the internet or a local network. IP stands for “Internet Protocol.”

repeated nudging to enable location settings, and incomplete disclosures of Google’s location data collection and processing.

46. In one striking example, [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

**B. Google Consumers Must Navigate Numerous, Conflicting Controls to Protect Their Privacy.**

47. Google consumers must navigate numerous, conflicting settings that purport to control when and how Google collects, stores, and uses their location information. As noted above, account-level settings apply to data collected from *any* device signed in to a consumer’s Google Account. In contrast, device-level settings apply *only* to the specific device on which the setting appears.

1. Location-Related Google Account Settings.

48. Google’s collection and use of location data is subject to at least three Google Account settings: Location History, Web & App Activity, and Google Ad Personalization (“GAP”).

49. Location History<sup>6</sup> is a Google Account feature that captures all the places where a signed-in consumer goes. [REDACTED]

[REDACTED] Location History has existed in some form since approximately 2009. [REDACTED]  
[REDACTED]

---

<sup>6</sup> For purposes of this Complaint, Location History is a specific Google feature and not a generic term for a consumer’s location data.

[REDACTED]

50. [REDACTED]

[REDACTED] Using this information, Google builds a “private map” of all the places a consumer has been, which the consumer can review and edit.

51. The primary value of Location History data for Google, however, lies in its advertising uses. Google [REDACTED]

[REDACTED] These inferences inform what advertising Google will present to that consumer.

52. In addition, Google uses Location History data to provide advertisers with “store conversion” rates—i.e., the number of consumers who have viewed ads and then visited the advertised store. Google’s ability to track consumers in the physical world after they click on digital ads is a unique selling point for its advertising business.

53. Web & App Activity is a separate Google Account setting that collects, stores, and monetizes consumers’ locations. Whereas Location History collects location information on all of a consumer’s movements, Web & App Activity records a consumer’s “transactional location”: that is, the location of a consumer’s device when the consumer is signed in and interacting with certain Google products.<sup>8</sup> For example, when a consumer conducts a search for “chocolate chip cookie recipe” while signed in on the Google Search app, Google collects the consumer’s location at the time of the search, along with details about the search, and stores that information to the Web & App Activity log for that consumer. Later, if the consumer searches for an address on Google

---

<sup>7</sup> As used herein, “precise location” refers to the consumer’s exact longitude and latitude.

<sup>8</sup> A “supplemental” Web & App Activity setting also collects and stores information about the consumer’s interactions with non-Google apps and with non-Google websites on Google’s Chrome browser.

Maps, Google again stores the consumer's location at the time of that search, along with details such as what was searched, to the same log.

54. Google uses Web & App Activity data to make deductions about the consumer's habits and interests for advertising purposes. Google's ability to target ads to consumers based on information about their locations is critical to the success of its 150 billion-dollar advertising business.

55. Location History and Web & App Activity are independent settings. Disabling one setting does not impact whether a consumer's location data is collected and stored pursuant to the other setting. Practically, this means that even if a consumer prevents location tracking by one of these services, Google still tracks and monetizes the consumer's location through the other. Until recently, Google kept the data stored in connection with these settings indefinitely, unless the consumer manually deleted the data.

56. Google also offers consumers a Google Account setting related to personalized advertising—the GAP setting. The GAP setting purports to provide signed-in consumers the ability to opt out of personalized ads served by Google. Google told consumers that leaving this setting enabled would mean that, “Google can show you ads based on your activity on Google services (ex: Search, YouTube), and on websites and apps that partner with Google.” By implication, consumers who do not want Google to serve them ads based on their activity on Google products should be able to opt out by disabling this setting. However, Google continues to target ads to a consumer based on a consumer's location even if the consumer opts out of ads personalization by disabling the GAP setting.

## 2. Location-Related Device Settings.

57. While the Location History, Web & App Activity, and GAP settings apply across all devices associated with a consumer's Google Account, there are additional settings related to location data that apply only to a consumer's specific device. Location-related device settings control whether a specific device can transmit location information to apps, APIs, or other services

on the consumer's device. Android devices have a number of different location-related device settings.

58. First, Android devices have a location "master switch" that controls whether the device can share the device's location with any other apps on the device. When this "master switch" is enabled, apps and services can request and access the device's location. If a consumer disables this setting on their device, then no apps or services can access the device's location.

59. Second, Android devices have "app-specific" location settings. Using these device settings, consumers can grant or deny a specific app, such as Google Maps or Uber, permission to access the device's location. On some versions of Android, apps with permission to access device location could access a consumer's location in the background (i.e., even when the app was not in use).

60. On Android devices, these two types of settings also control the flow of location information to Google. For example, enabling the location "master switch" allows Google to "periodically" collect and use location from the consumer's device in order to improve a Google platform called Google Location Services.<sup>9</sup> [REDACTED]

[REDACTED]

[REDACTED]

61. Android mobile devices also have other settings that purportedly control access to specific types of location data. For example, Android consumers can control whether their device scans for nearby Wi-Fi access points or Bluetooth devices, which can help Google interpret the consumer's location. Certain versions of the Android OS also include "Low Battery" and "High Accuracy" modes that control whether Google uses Wi-Fi, Bluetooth, cellular signals, and Google Location Services, in addition to GPS, to ascertain the consumer's precise location.

62. In order to protect their privacy, consumers must understand the nuanced and interrelated functions of both account-level settings and device-level settings. This complex web

---

<sup>9</sup> Google Location Services is also referred to as Google Location Accuracy.

of settings misleads consumers into believing that they are not sharing their location with Google when in fact they are.

**C. Google Deceives Consumers Regarding Their Ability to Protect Their Privacy Through Google Account Settings.**

63. One way that Google misleads consumers regarding their location data is through Google Account settings. As a result of deceptive and unfair practices with respect to these settings, Google has collected enormous amounts of location data from unwitting consumers and then monetized that data in the service of Google’s advertising offerings without consumers’ knowledge or consent.

**1. Google Misrepresented and Omitted Material Facts Regarding the Location History and Web & App Activity Settings.**

64. Google misrepresented and omitted material information regarding the Location History and Web & App Activity settings from at least 2014 to at least 2019. These misrepresentations and omissions confused consumers about which settings implicate location data, enabling Google to capture, store, and use such data without consumers’ knowledge or consent.

65. For years, on a public webpage regarding Location History, Google assured Android consumers that “[y]ou can turn off Location History at any time. ***With Location History off, the places you go are no longer stored.***” Google similarly explained that Apple consumers could log into their online Google account and select “Stop storing location” in order to turn off Location History, and that turning Location History off would “***stop[] saving new location information.***” Google thus presented Location History as the setting that controlled whether Google stored location information about a consumer. That representation was false.

66. Even when Location History was off, Google continued to collect and store consumers’ locations. Depending on a consumer’s other settings, Google collected and stored a consumer’s location data through Web & App Activity, Google apps on the consumer’s device, Wi-Fi and Bluetooth scans from the consumer’s device, Google’s Location Services feature, the



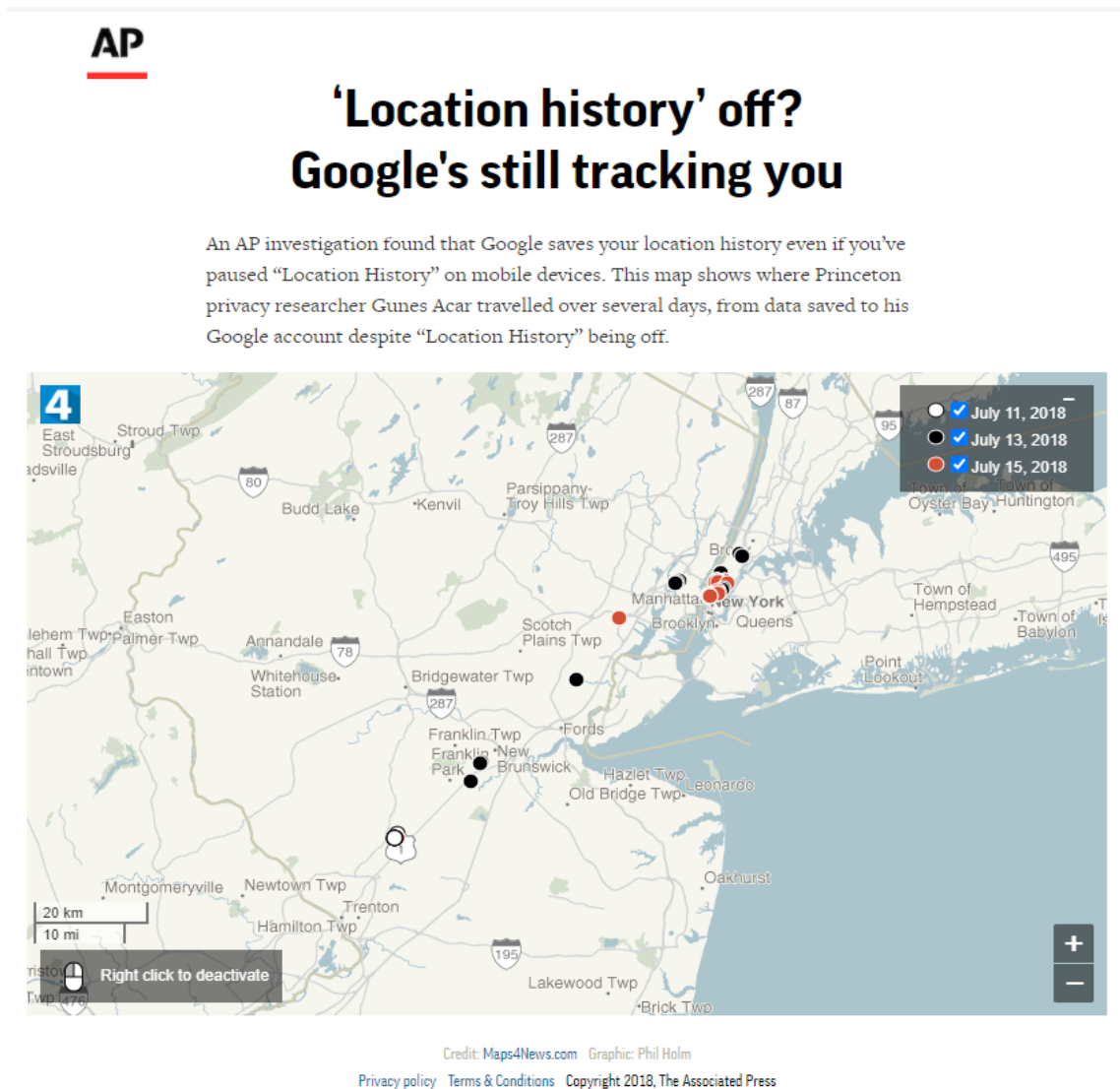
consumer's IP address, and [REDACTED]

67. Google's statements prompting consumers to turn on Location History also falsely implied that this setting alone controlled whether Google stores a consumer's location. For example, at various times, Google told consumers that enabling Location History "lets Google save your location;" allows Google to "store and use" the "places you go;" permits Google to "periodically store your location;" "allows Google to store a history of your location;" or allows Google "to save and manage your location information in your account." These representations omit the material fact that Google collected and saved consumers' location data when using Google products regardless of whether the consumer enabled or disabled Location History.

68. Google's misstatements and omissions regarding Location History were exacerbated by separate misstatements and omissions in connection with the Web & App Activity setting. Specifically, Google did not disclose to consumers that even when Location History is not enabled, the Company still collects, stores, and uses location data through the Web & App Activity feature.

69. As detailed above, Web & App Activity collects location data when a consumer interacts with certain Google products. For example, if a consumer asks Google Assistant to search for the author of a book, Web & App Activity would save the consumer's location and the time when the query was made. Google also collects and stores information that could implicitly reveal a consumer's location, such as which places the consumer inputs into Google Maps.

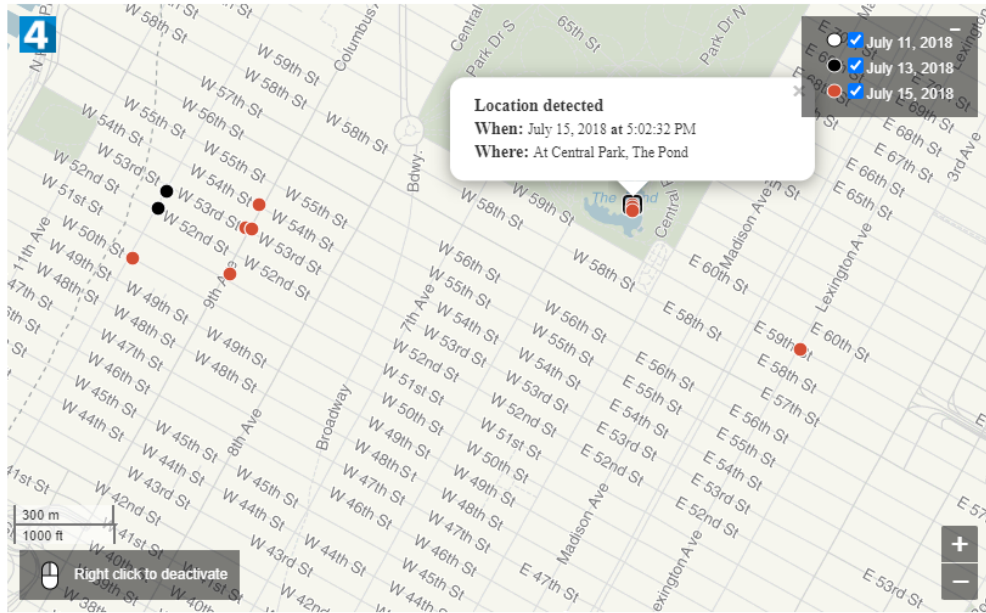
70. The 2018 AP story illustrated the extent of Google’s location tracking through Web & App Activity. The report provided an interactive map of the data Google collected from the AP investigator’s device when Web & App Activity was enabled but Location History was disabled. The resulting map reflected that in only eight hours, Google captured almost two dozen precise, time-stamped GPS coordinates. *See map:*



*See <https://interactives.ap.org/google-location-tracking/> (last accessed January 21, 2022).*

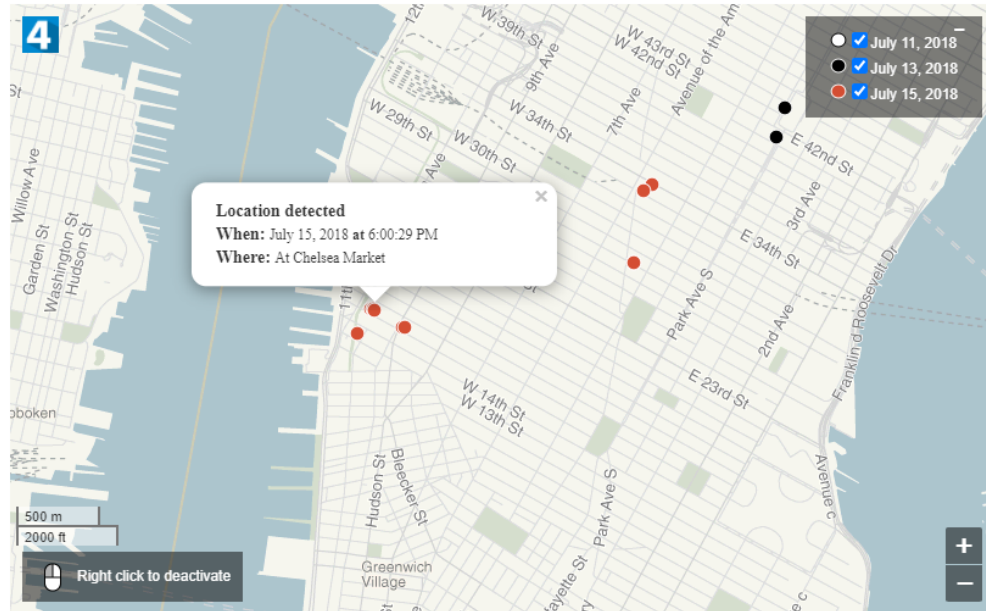
71. Further, the interactive map allowed the viewer to zoom in on more precise locations that Google was tracking, despite Location History being turned off. From the interactive

map, the viewer can see that the researcher spent time at Central Park's The Pond before heading to the Chelsea Market and then to Hell's Kitchen on July 15, 2018. *See example:*



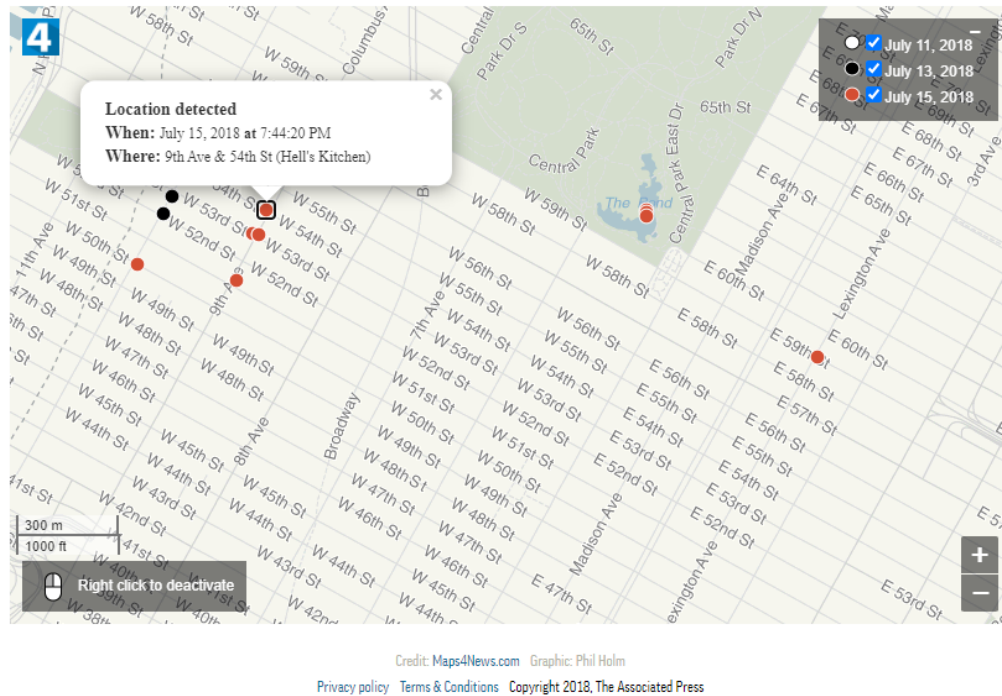
Credit: Maps4News.com Graphic: Phil Holm

Privacy policy Terms & Conditions Copyright 2018, The Associated Press



Credit: Maps4News.com Graphic: Phil Holm

Privacy policy Terms & Conditions Copyright 2018, The Associated Press



See <https://interactives.ap.org/google-location-tracking/> (last accessed January 21, 2022).

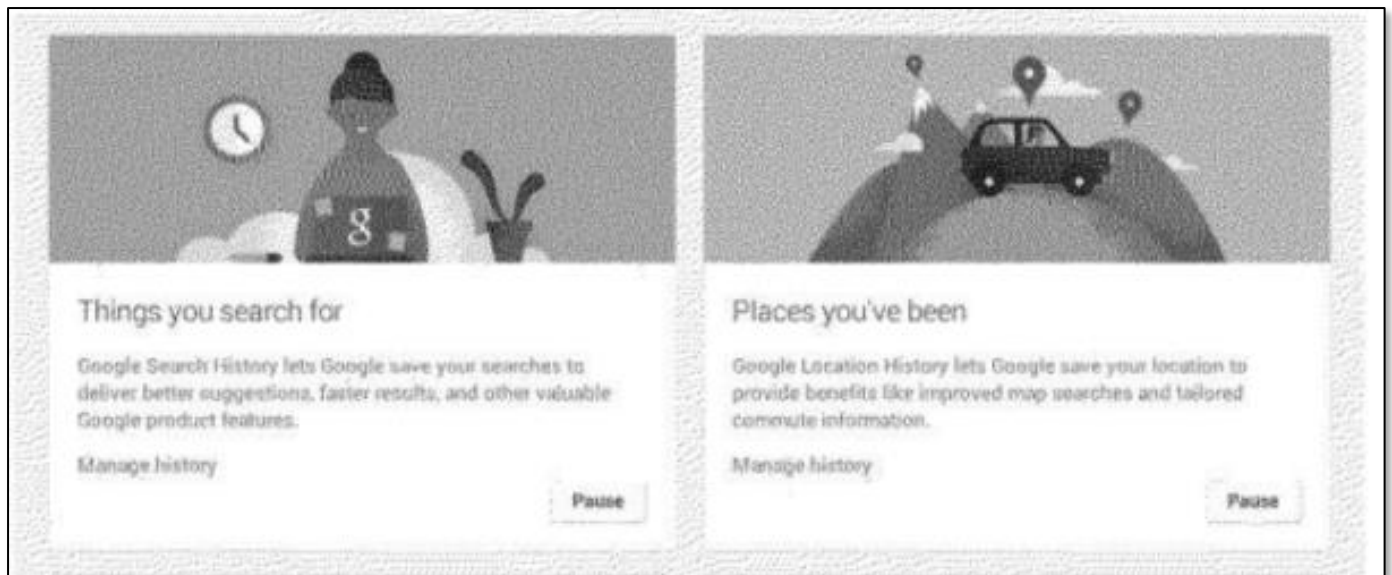
72. Google recognizes that the location of individual consumers over time constitutes sensitive information. Despite this, Google concealed the material fact that the Company collects, stores, and uses location data when Web & App Activity is enabled. Consumers could not avoid Google’s deceptive and unfair storage and use of their location because it occurred without their knowledge.

73. Google concealed from consumers that the Web & App Activity setting controlled Google’s storage and use of their location information in at least three ways.

74. **First**, Google did not disclose the Web & App Activity setting when consumers set up Google Accounts for the first time. At this stage, the Web & App Activity setting is defaulted “on” for new Google Accounts. Thus, a consumer who sets up a Google Account is automatically opted-in to location tracking via Web & App Activity. Until 2018, the Google Account set-up process made no mention of the Web & App Activity setting.

75. Furthermore, Android phones effectively require a consumer to sign in to a Google Account,<sup>10</sup> and Google apps like Search and Maps were (and are) granted location permission on Android devices by default. As a result, Google could begin to track Android consumers' locations without ever presenting consumers with an option to opt out.

76. One of the only ways consumers would even become aware that Web & App Activity was storing location data was if they happened to navigate to a separate webpage where Google recorded data stored under the Web & App Activity setting, called "My Activity." But when consumers first landed on this webpage, Location History was presented as the only setting that related to location data. *See:*

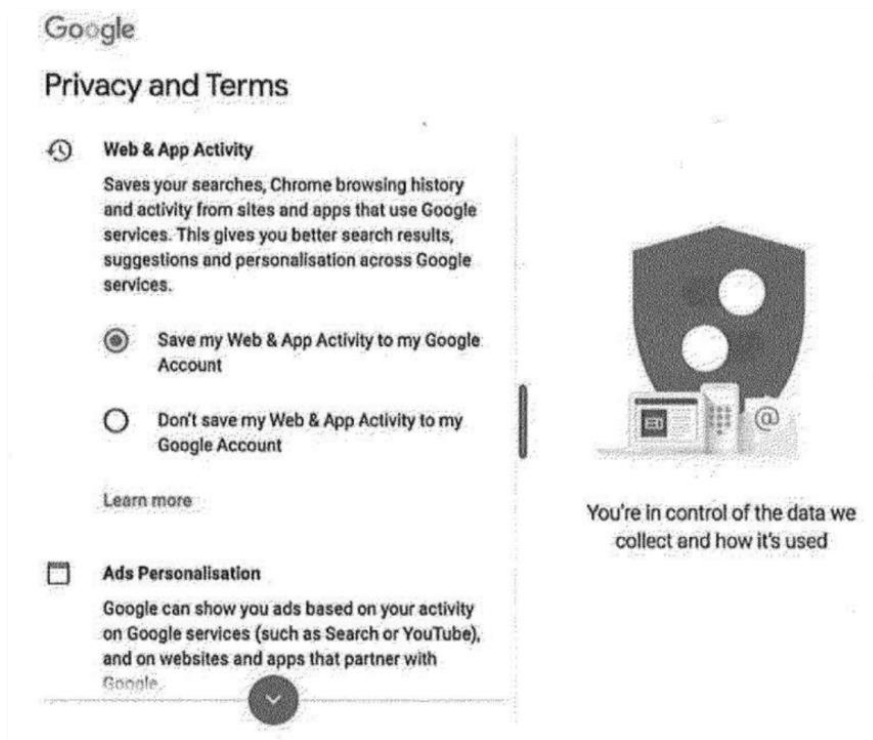


(Text above: "Places you've been[:] Google Location History lets Google save your location to provide benefits like improved map searches and tailored commute information.")

---

<sup>10</sup> A consumer must sign in to a Google Account on their Android device to access the Google Play application ("app") store, which is needed to download new apps or to receive app updates that enable apps to continue to function properly and safely. Once Android consumers sign into their Google Account, consumers must fully remove their Google Account(s) from their device in order to sign their device out of Google.

77. In 2018, Google revised its Google Account set-up process to reference Web & App Activity. However, the Company continued to conceal from new consumers that location data was captured by the setting. Until at least mid-2018, this information was only revealed to new consumers who first clicked on a link to see “More options” and then selected a second link to “Learn More” about the Web & App Activity setting. [REDACTED]



(Text above: “Web & App Activity[:] Saves your searches, Chrome browsing history and activity from sites and apps that use Google services. This gives you better search results, suggestions and personalization across Google services.”)

78. **Second**, Google failed to disclose the Web & App Activity setting to consumers when they set up new devices using existing Google Accounts. The “enabled” or “disabled” status of a consumer’s Web & App Activity setting applies to all devices signed in to the consumer’s

Google Account. Thus, any time a consumer signed any device in to an existing Google Account, Google could begin tracking that device as long as Web & App Activity was enabled on the consumer's Google Account. Because Android devices need to be signed in to Google to use critical functionalities, and consumers sign in to Google at device set-up, Google was able to track Android consumers via Web & App Activity as soon as they set up new devices on their Google Accounts, without notifying those consumers.

79. **Third**, once consumers set up a Google Account or linked new devices to their Google Account, they were unlikely to discover the location tracking nature of Web & App Activity settings. Google did not identify Web & App Activity as a location-related setting in the places where a consumer would expect to find that information. For example, until around 2019, consumers who explored location settings on their Android devices would not find Web & App Activity listed among them. Likewise, a Google webpage titled "Manage your Android's device location settings" described Google's location-based settings and discussed Location History without mention of the Web & App Activity setting.

80. Google's Privacy Policies also omitted mention of the Web & App Activity setting. For instance, the December 18, 2017 version of Google's Privacy Policy lists examples of information about "your actual location" that Google "may collect and process." These examples include a specific mention that "Location History allows Google to store a history of your location data," but makes no reference to the Web & App Activity setting.

81. Putting aside the placement of Google's statements, many of Google's affirmative disclosures regarding Web & App Activity also failed to disclose that this setting authorized Google to store and use location data. Google routinely described the Web & App Activity setting as allowing the Company to store and use Google search history, Chrome web browser activity, and activity on Google apps—without mention of location (unless the user clicked on a link to a pop-up window for more information).

82. In sum, Google misrepresented that disabling Location History stopped Google from storing a consumer’s location and concealed that the Web & App Activity setting also stored location data, which mislead consumers to believe that the Web & App Activity setting did not impact collection, storage, or use of location data; that the Location History setting alone controlled whether Google retained and used location data; and that disabling the Location History setting would prevent Google from retaining and using the consumer’s locations on an ongoing basis.

83. These misrepresentations and omissions were material to Indiana Google consumers, as demonstrated by, among other things, consumers’ and Google’s response to the public revelation in the 2018 AP article that Google “store[s] your location data even if you’ve used a privacy setting that says it will prevent Google from doing so.”

84. Within Google, a self-titled “Oh Shit” meeting was convened the day the AP story was published to begin brainstorming responses to the article. Soon after, Google CEO Sundar Pichai and other senior executives became directly involved in crafting the Company’s response. After the AP story, Google updated its help page to remove the misleading disclosure “With Location History off, the places you go are no longer stored.”

85. The AP article set off a frenzy of negative press coverage. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

86. [REDACTED]

[REDACTED]

[REDACTED]



[REDACTED]

87. In internal discussions, Google employees agreed that Google’s disclosures regarding Location History were confusing. [REDACTED] admitted the disclosures were “definitely confusing.” Another Google employee stated that the consumer interface for Google Account settings “feels like it is designed to make things possible, yet difficult enough that people won’t figure it out.” [REDACTED] admitted, “I did not know Web and App Activity had anything to do with location.”

88. [REDACTED]

[REDACTED] Yet Google did not act to clarify the Web & App Activity and Location History settings until after the Company’s pervasive misconduct was made public.

2. Google Misrepresents and/or Omits Material Facts Regarding Consumers’ Ability to Control Their Privacy through Google Account Settings.

89. Google further misleads consumers about its location tracking practices by misrepresenting and omitting material facts regarding the extent to which Google Account settings prevent Google’s collection and use of location data. Google seemingly offers simple “privacy controls” to attract consumers but continues to exploit consumers’ location data regardless of their choices with respect to these settings.

90. Since at least 2014, Google has made misleading promises that consumers can control the information that Google collects, stores, and uses about them by adjusting their Google Account settings. In numerous iterations of Google’s Privacy Policies and other disclosures, Google has pointed to Google Account settings as features that, for example, allow consumers to make “meaningful choices about how [the information Google collects] is used;” “control the collection of personal information;” “decide what types of data...[they] would like saved with

[their] account when [they] use Google services;” or “make it easier for [them] to see and control activity that’s saved to [their] account and how it’s used.” *See:*



91. Since May 25, 2018, Google’s Privacy Policy has explained that “across our services, you can adjust your privacy settings to control what we collect and how your information is used.” In its Terms of Service and Privacy Policies, Google also represented that it would “respect the choices you make to limit sharing or visibility settings in your Google Account.”

92. As part of setting-up a Google Account, Google expressly tells consumers, “You’re in control. Depending on your account settings, some ... data may be associated with your Google Account and we treat this data as personal information. You can control how we collect and use this data....You can always adjust your controls later or withdraw your consent....”

93. In another example, since 2019, Google has maintained a webpage devoted to explaining “How Google uses location information.” This webpage states that “[i]f Web and App Activity is enabled, your searches and activity from a number of other Google services are saved to your Google Account. The activity saved to Web and App Activity may also include location

information.... Pausing Web & App Activity will stop saving your future searches and activity from other Google services.”

94. In statements like these, Google frames Google Account settings as tools that allow a consumer to control Google’s collection and use of their personal data, including location information. The Company’s reassuring statements about these settings misleadingly state and/or imply that a consumer can stop Google from storing or deploying the consumer’s location information by disabling these settings. However, this is not true.

95. [REDACTED]

96. [REDACTED]

97. Google further misleads consumers by providing consumers only partial visibility into the location data Google collects about them. For example, Google’s current Privacy Policy claims that consumers can manage their privacy because they can “review and control information saved in [their] Google Account” “decide what types of activity [they would] like saved in [their] account,” and “review and control data that’s created when [they] use Google services.” Earlier versions of the Privacy Policy likewise indicate that Google provides “transparency and choice” options that allow consumers to “access, manage, or delete information that is associated with [their] Google Account,” and state that Google provides these tools in order to “be clear about what information [it] collects.” In other disclosures, Google explains that the My Activity webpage “allows [consumers] to review and control data that’s created when [they] use Google services”

and that “My Activity is a central place where [consumers] can view and manage [their] saved activity.”

98. [REDACTED]

99. [REDACTED]

100. Despite claiming to endeavor to “be clear about what information [Google] collects, so that [consumers] can make meaningful choices about how it is used,” [REDACTED]

101. [REDACTED]

102. [REDACTED] Even today, the webpage devoted to explaining “How

Google uses location information” only explains how location data is “saved in [a] Google Account,” [REDACTED]

[REDACTED]

103. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] As a result of Google’s misleading statements with respect to these settings, consumers cannot reasonably avoid Google’s access to and use of their location data.

104. Google is aware that consumers do not understand Google Account settings or how these settings interact with other location-related settings. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

3. Google Misrepresents and Omits Material Facts Regarding the Google Ad Personalization Setting.

105. Google’s deceptive and unfair practices extend to other Google Account settings as well. Specifically, the Company’s Google Ad Personalization (GAP) setting purports to allow consumers to opt out of personalized advertising. Consistent with Google’s other practices, this setting allows consumers to “control” the Company’s use of their location data only to an extent.

106. According to Google, enabling the GAP setting will “[l]et Google use [a consumer’s Google Account activity] to show [the consumer] more relevant ads on [Google’s]

services and on websites and apps that partner with [Google].” In explaining this setting, Google told consumers that they should “let Google know [their] location,” so that “[they] won’t get ads for stores in other regions.”

107. Google’s disclosure misleads consumers to believe they can turn off the GAP setting to prevent Google from using location data to show personalized ads. But this setting only provides an illusion of control. In reality, Google continues to target ads based on a consumer’s location—both on and off Google products—even if the consumer opts out of ads personalization by disabling the GAP setting. [REDACTED]

**D. Google Deceives Consumers Regarding Their Ability to Protect Their Privacy Through Device Settings.**

108. Google further confuses and misleads consumers into sharing location data through deceptive practices that contradict the Company’s representations and consumers’ expectations through location-related device settings. Specifically, Google misrepresents the ability of consumers to control or limit Google’s collection of their location data through their device settings. Google misleads consumers and withholds material facts about device settings in at least three respects.

109. *First*, Google tells consumers that they can control the flow of location data to Google via the device’s location “master switch.” Google includes this “master switch” on Google-licensed Android phones in order to provide this functionality. Furthermore, beginning in its May 2018 Privacy Policy, Google represented that “the types of data [Google] collect[s] depend in part on [the consumer’s] device and account settings. For example, [a consumer] can turn [an] Android device’s location on or off using the device’s setting app.” Google also provided Help pages that explain: “If [a consumer] turn[s] off Location for [a] device, then no apps can use [the consumer’s] device location.”

110. These representations, as well as the Android device setting itself, state and/or imply that when consumers disable the master location setting, Google does not collect, store, or use their location to provide “services” (including ads) to the consumer. However, since at least 2014 through the present, Google has deceived consumers by failing to disclose that regardless of whether the consumer *explicitly forbids* Google from accessing location via a device, Google derives and stores the consumer’s location [REDACTED]

111. Specifically, when a consumer turns the location “master switch” off, believing that they are not sharing location information, Google nevertheless uses the consumer’s IP address [REDACTED] [REDACTED] to infer the consumer’s location. Consumers have no control over whether Google appropriates their location [REDACTED] [REDACTED]

112. **Second**, Google misleads consumers into believing that user’s app-specific device settings can control whether Google obtains their location data. Google includes these settings on Android devices to allow a user to deny device location information to specific apps. Google Help pages explain that on Android devices, a user can choose which apps can access and use a user’s device location. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

113. **Third**, device settings related to specific location signals on Android phones, such as Wi-Fi and Bluetooth, are confusing and conflicting, making it very challenging for consumers to limit Google’s access to this data. For example, Google uses Wi-Fi scans to compute device location more accurately and precisely. Android phones include a “Wi-Fi scanning” setting among other location-related settings. However, even if a consumer turns this setting “off,” Google can still obtain Wi-Fi scans.

114. Simply put, even when a consumer’s mobile device is set to deny Google access to location data, the Company finds a way to continue to ascertain the consumer’s location. Google’s undisclosed practice of bypassing consumers’ location-related device settings constitutes a deceptive and unfair act or practice. Because these practices are not clearly disclosed to consumers and contradict consumer expectations, consumers cannot reasonably avoid Google’s access to and use of their location data.

115. Google employees admit that the Company’s practices contradict consumer expectations. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] “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.”

**E. Google Deploys Deceptive Practices that Undermine Consumers’ Ability to Make Informed Choices About Their Data**

116. Google has relied on, and continues to rely on, deceptive and unfair practices that makes it difficult for consumers to decline location tracking or to evaluate the data collection and processing to which they are purportedly consenting. Such practices are known in academic literature as “dark patterns.”

117. Dark patterns are deceptive design choices that alter the consumer’s decision-making for the designer’s benefit and to the consumer’s detriment. Dark patterns take advantage of behavioral tendencies to manipulate consumers into actions that are harmful to consumers or



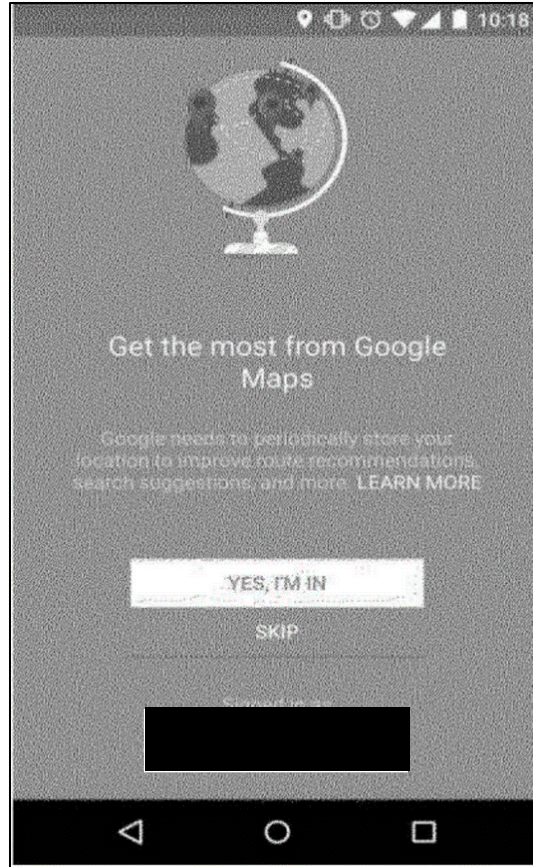
contrary to their intent. Common examples of “dark patterns” include complicated navigation menus, visual misdirection, confusing wording (such as double negatives), and repeated nudging.

118. Because location data is immensely valuable to the Company, Google makes extensive use of dark patterns, including repeated nudging, misleading pressure tactics, and evasive and deceptive descriptions of location features and settings, to cause consumers to provide more and more location data (inadvertently or out of frustration).

1. Dark Patterns in Google Account Settings

119. Some of Google’s deceptive practices with respect to Google Account settings described above reflect the use of dark patterns. For example, Google’s decision to enable by default the privacy-intrusive Web & App Activity feature by default, while failing to disclose this setting, was a deceptive use of design. Through this dark pattern, Google not only misled consumers about the extent of its location tracking, but also made it difficult for consumers to opt out of this tracking.

120. Google also uses dark patterns in “in-product” prompts to enable Google Account settings—i.e., prompts to enable these settings when a consumer begins to use Google apps and services on a device. For example, for at least part of the relevant time period, Google told consumers that certain Google products, such as Google Maps, Google Now, and Google Assistant “need[]” or “depend[] on,” the Location History feature when setting up these products. *See:*



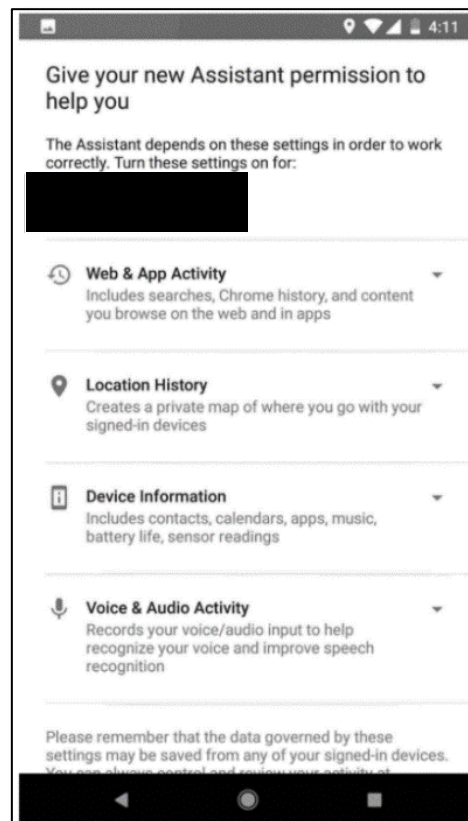
(Text above: “Get the most from Google Maps[:] Google needs to periodically store your location to improve route recommendations, search suggestions, and more”).

121. However, these products could properly function without consumers agreeing to constant tracking. [REDACTED]

[REDACTED] Because Google’s statements falsely implied that consumers are not free to decline to enable Google Account settings if they wished to use a number of (often pre-installed) Google products as they were intended, consumers were left with effectively no choice but to enable these settings.

122. Google also designed the set-up process for certain Google products in a manner that limited consumers’ ability to decide whether to permit Google to track them. In particular, Google prompted consumers to enable Location History and Web & App Activity, along with

multiple other settings, in order to use products like Google Assistant or Google Now. In other words, consumers could only opt in or out of these settings collectively at set-up of the Google product. *See:*



(Text above: “Give your new Assistant permission to help you[.] The Assistant depends on these setting in order to work correctly. Turn these setting on for: . . . Web & App Activity[:] Includes searches, Chrome history, and content you browse on the web and in apps[:] Location History[:] Creates a private map of where you go with your signed-in devices”).

123. By presenting consumers with an “all or nothing” opt-in, Google similarly denied consumers the ability to choose which data-sharing features to enable, unless consumers took the additional and burdensome action of trying to locate and disable these features after set-up.

124. Google also did not (and still does not) give consumers the choice to decline location tracking once and for all. For example, if users decline to enable Location History or Web & App Activity when first prompted in the set-up process for an Android device, Google continues

to repeatedly prompt users to enable these settings when using Google products—despite already refusing consent.

125. [REDACTED]

[REDACTED]

[REDACTED] By repeatedly “nudging” consumers to enable Google Account settings, Google increases the chances that a consumer will enable the setting inadvertently or out of frustration. Google does not and has never provided similarly frequent prompts to opt out of location sharing.

126. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

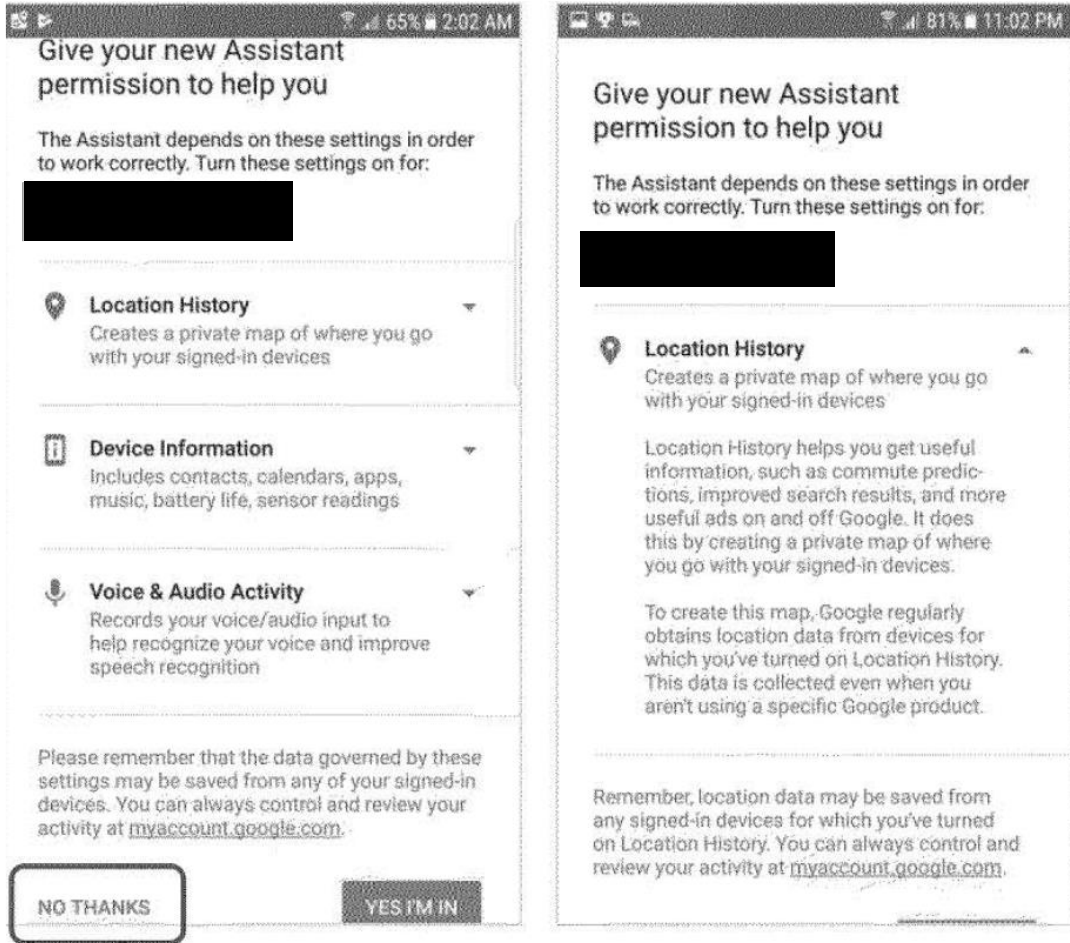
[REDACTED]

[REDACTED]

127. Further, until at least mid-2018, consumers who read Google’s prompts to enable Google Account settings were provided only vague and imbalanced information about the consequences of enabling Google Account settings, unless consumers clicked on links that led to further information.

128. These prompts misleadingly emphasized a few benefits that Location History provided to consumers—such as commute notifications or more personalized search results—without providing a similar emphasis and disclosure about the advertising and monetary benefits

to Google. Indeed, Google only revealed that it used this comprehensive data for advertising purposes in separate linked or drop-down disclosures that consumers would likely never see. *See:*



129. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

130. At relevant times, consumers who paused Location History or deleted Location History entries also received vague warnings implying that disabling or limiting Location History would hinder the performance of Google apps. For example, consumers who disabled Location History were told that doing so “limits functionality of some Google products over time, such as Google Maps and Google Now” and that “[n]one of your Google apps will be able to store location data in Location History.” Consumers who deleted Location History entries were also warned that “Google Now and other apps that use your Location History may stop working properly.” These warnings were misleading because they failed to provide consumers with sufficient information to understand what, if any, services would be limited, and falsely implied that Google products would not function unless the consumer agreed to provide location data on a continuous basis.

2. Dark Patterns in Device Settings.

131. Users who seek to limit Google’s location data collection through Android device settings are also confronted with various dark patterns. For example, consumers may try to disable location settings on their devices, such as through the location “master switch” or the app-specific location permission settings. However, after disabling these settings, consumers are subject to repeated prompting to re-enable location when using a Google app. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

132. Once location settings are re-enabled on a consumer’s device, other Google apps and services can access the consumer’s location, including (in some versions of the Android OS) when the consumer is not interacting with the app. The only way to avoid such access is if the consumer remembers to disable location settings again, a process which the consumer is discouraged to undertake because it requires a number of steps and must be repeated every time a consumer wants to permit (and then deny) Google access to their location.

133. During the relevant time period, Google also actively sought to increase the percentage of consumers who enabled location settings on Android devices by providing vague disclosures and making it more difficult for consumers to disable these settings. For example, in one version of Android, Google offered a toggle that allowed consumers to disable location from a pull-down menu at the top of their screen. This made the setting more easily accessible to consumers. However, Google removed this toggle from Android phones that Google manufactured, [REDACTED]

[REDACTED]

134. [REDACTED]

[REDACTED]

[REDACTED]

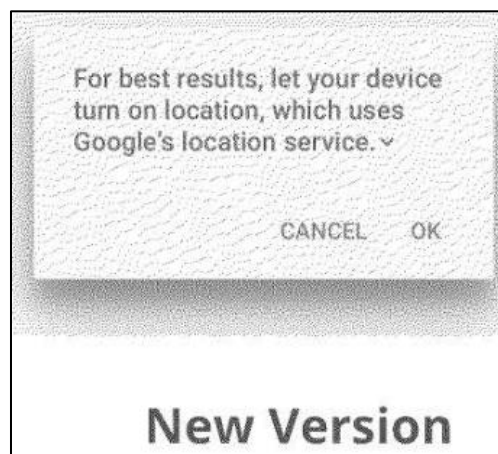
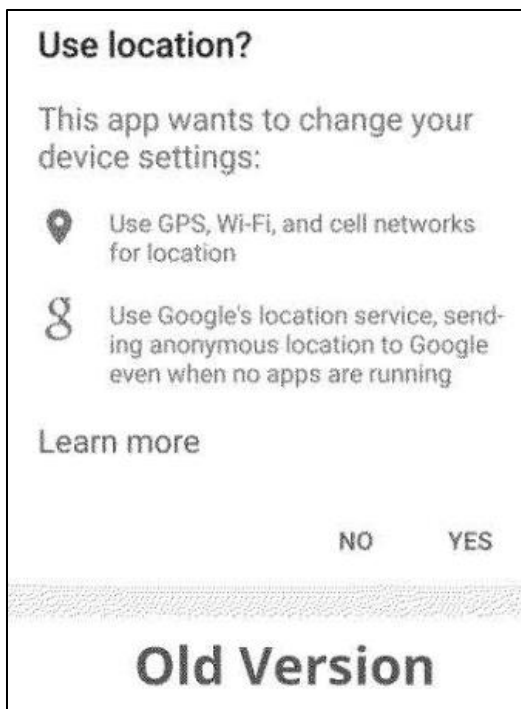
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

135. Around the same time, Google also changed the dialogue box that consumers would see when prompted by Google to enable location, so that more consumers would consent to report their locations to Google. Pursuant to this change, consumers were no longer advised that they were agreeing to persistent tracking of their precise location by Google, as shown below:



136. [REDACTED]

137. Google took these actions because it has profound financial incentives to pressure consumers into enabling location services and other location settings on their devices. Without these settings enabled, Google has a substantially reduced ability to ascertain, extract, and monetize the locations of its consumers.

**CAUSES OF ACTION**

**COUNT I**

**Google Committed Unfair, Abusive, and/or Deceptive Acts, Omissions, and/or Practices in Violation of Ind. Code. § 24-5-0.5-3(a)**

138. The State of Indiana incorporates herein by reference all preceding paragraphs as if fully set forth herein.



139. The DCSA regulates unfair, abusive, and/or deceptive acts, omissions, and/or practices between a supplier and consumer when engaging in consumer transactions. Ind. Code § 24-5-0.5 *et seq.*

140. Under the DCSA, a consumer transaction includes services and other intangibles. Ind. Code § 24-5-0.5-2(1).

141. In supplying Indiana consumers with the products and services, Google was and remains involved in consumer transactions in Indiana, as defined by Ind. Code § 24-5-0.5-2.

142. Google regularly engages in or solicits consumer transactions with Indiana Consumers. As such, Google is a supplier pursuant to Ind. Code § 24-5-0.5-2.

143. The DCSA prohibits a supplier from committing “an unfair, abusive, or deceptive act, omission, or practice in connection with a consumer transaction . . . whether it occurs before, during, or after the transaction. An act, omission, or practice prohibited by this section includes both implicit and explicit misrepresentations”. Ind. Code. § 24-5-0.5-3(a).

144. As alleged herein, Google has regularly engaged in unfair, abusive, and/or deceptive acts, omissions, and/or practices affecting Indiana consumers, in violation of Ind. Code 24-5-0.5-3(a), by collecting, storing, and/or using consumers’ location data without their knowledge and/or consent, or in contravention of consumers’ express actions denying consent.

145. These unfair, abusive, and/or deceptive acts and/or practices include but are not limited to, the following:

- a. Misleading consumers regarding location-related settings and collecting, retaining, and/or using consumers’ location information without their knowledge and/or consent;
- b. Conditioning or appearing to condition consumers’ use of Google products and services, including products and services pre-installed on Android devices, on consumers’ consent to Google’s collection, retention, and/or use of their location data, where that consent and/or data was not needed to provide the basic functionality of the product or service;

- c. Employing consumer interfaces that make it difficult for consumers to deny Google access to and use of their location information, including making location-related consumer controls difficult to find and repeatedly prompting consumers who previously declined or disabled location-related controls to enable those controls; and
- d. Providing incomplete, imbalanced, and/or misleading information about the extent of Google's collection, retention, and/or use of consumers' location data when a consumer enabled location-related device settings or Google Account settings.

146. Further, by engaging in the acts and practices alleged herein, Google made or caused to be made to Indiana consumers, directly or indirectly, explicitly or by implication, misrepresentations including, but not limited to, the following:

- a. That consumers could prevent Google from collecting, retaining, and using their location information by disabling (*i.e.*, turning off) the Location History setting;
- b. That consumers could prevent Google from collecting, retaining, and using their location information by adjusting Google Account settings;
- c. That consumers could review and manage the location information associated with their Google Account and/or retained by Google via the My Activities feature;
- d. That consumers could prevent Google from using their location to target advertisements by disabling the Google Ad Personalization setting;
- e. That consumers could prevent Google from collecting, retaining, and using consumers' location information by disabling location-related device settings; and
- f. That consumers needed to enable Location History and/or Web and App Activity to use certain Google products and services, including products and services pre-installed on Android devices (such as Google Now, Google Assistant, and Google Maps).

147. Further, by failing to disclose the following material facts to consumers, Google engaged in deceptive omissions of these facts in violation of Ind. Code § 24-5-0.5-3(a), including but not limited to the following:

- a. That Google retained and used consumer's location information even with the Location History setting disabled;
- b. That Google retained and used consumers' location information if the Web & App Activity setting was enabled;
- c. That consumers could not prevent Google from retaining and using consumers' location information by adjusting Google Account settings or signing out of Google;
- d. That consumers could not prevent Google from using consumers' location to target advertisements by disabling the Google Ad Personalization setting;
- e. That Google continues to collect and use location information about consumers even when the consumer's device location setting is disabled;
- f. [REDACTED]  
[REDACTED]  
[REDACTED]
- g. That Google products and services, including products and services pre-installed on Android devices (such as Google Now, Google Assistant, and Google Maps), could function properly without Location History and/or Web and App Activity enabled.

148. These unfair, abusive, and/or deceptive acts, omissions, and/or practices were made in connection with a consumer transaction within the meaning of Ind. Code § 24-5-0.5-2(a)(1).

## COUNT II

### **Google Committed Unfair, Abusive, and/or Deceptive Acts, Omissions, and/or Practices in Violation of Ind. Code. § 24-5-0.5-3(b)(1)**

149. The State of Indiana incorporates herein by reference all preceding paragraphs as if fully set forth herein.

150. The DCSA regulates unfair and deceptive practices between a supplier and consumer when engaging in consumer transactions. Ind. Code § 24-5-0.5 *et seq.*

151. Under the DCSA, a consumer transaction includes services and other intangibles. Ind. Code § 24-5-0.5-2(1).

152. In supplying Indiana consumers with the products and services, Google was and remains involved in consumer transactions in Indiana, as defined by Ind. Code § 24-5-0.5-2.

153. Google regularly engages in or solicits consumer transactions with Indiana Consumers. As such, Google is a supplier pursuant to Ind. Code § 24-5-0.5-2.

154. Google, through their acts, omissions, and/or practices related to the collection, retention, and use of consumer location information, represented that their products and/or services had performance, characteristics, uses, and/or benefits they did not have, which the Google knew or reasonably should have known they did not have, in violation of Ind. Code § 24-5-0.5-3(b)(1).

155. These unfair, abusive, and/or deceptive acts and/or practices include but are not limited to, the following:

- a. Misleading consumers regarding location-related settings and collecting, retaining, and/or using consumers' location information without their knowledge and/or consent;
- b. Conditioning or appearing to condition consumers' use of Google products and/or services, including products and services pre-installed on Android devices, on consumers' consent to Google's collection, retention, and/or use of their location data, where that consent and/or data was not needed to provide the basic functionality of the product or service;
- c. Employing consumer interfaces that make it difficult for consumers to deny Google access to and use of their location information, including making location-related consumer controls difficult to find and repeatedly prompting consumers who previously declined or disabled location-related controls to enable those controls; and
- d. Providing incomplete, imbalanced, or misleading information about the extent of Google's collection, retention, or use of consumers' location data when a consumer enabled location-related device settings or Google Account settings.

156. Further, by engaging in the acts and practices alleged herein, Google made or caused to be made to Indiana consumers, directly or indirectly, explicitly or by implication, misrepresentations including, but not limited to, the following:

- a. That consumers could prevent Google from collecting, retaining, and using their location information by disabling (*i.e.*, turning off) the Location History setting;
- b. That consumers could prevent Google from collecting, retaining, and/or using their location information by adjusting Google Account settings;
- c. That consumers could review and manage the location information associated with their Google Account and/or retained by Google via the My Activities feature;
- d. That consumers could prevent Google from using their location to target advertisements by disabling the Google Ad Personalization setting;
- e. That consumers could prevent Google from collecting, retaining, and/or using consumers' location information by disabling location-related device settings; and
- f. That consumers needed to enable Location History and/or Web and App Activity to use certain Google products and services, including products and services pre-installed on Android devices (such as Google Now, Google Assistant, and Google Maps).

157. Further, by failing to disclose the following material facts to consumers, Google engaged in deceptive omissions of these facts in violation of Ind. Code § 24-5-0.5-3(a), including but not limited to the following:

- a. That Google retained and used consumer's location information even with the Location History setting disabled;
- b. That Google retained and used consumers' location information if the Web & App Activity setting was enabled;
- c. That consumers could not prevent Google from retaining and using consumers' location information by adjusting Google Account settings or signing out of Google;

- d. That consumers could not prevent Google from using consumers' location to target advertisements by disabling the Google Ad Personalization setting;
- e. That Google continues to collect and/or use location information about consumers even when the consumer's device location setting is disabled;
- f. [REDACTED]  
[REDACTED]  
[REDACTED]
- g. That Google products and services, including products and services pre-installed on Android devices (such as Google Now, Google Assistant, and Google Maps), could function properly without Location History and/or Web and App Activity enabled

158. These acts, omissions, and/or practices were done in connection with consumer transactions within the meaning of Ind. Code § 24-5-0.5-2(a)(1).

**COUNT III**

**Google Committed Knowing Violations of the Indiana  
Deceptive Consumer Sales Act**

159. The State of Indiana incorporates herein by reference all preceding paragraphs as if fully set forth herein.

160. Google committed the acts alleged in this Complaint with knowledge of their deceptive nature, and therefore committed knowing violations of the DCSA, subjecting it to penalties under Ind. Code § 24-5-0.5-4(g).

**COUNT IV**

**Google's Conduct Constitutes Incurable Deceptive Acts Under the  
Indiana Deceptive Consumer Sales Act**

161. The State of Indiana incorporates herein by reference all preceding paragraphs as if fully set forth herein.

162. The acts alleged in this Complaint are incurable deceptive acts that Google committed as part of a scheme, artifice, or device with intent to defraud or mislead, and therefore committed incurable deceptive acts, subjecting it to penalties under Ind. Code § 24-5-0.5-8.

### **PRAYER FOR RELIEF**

WHEREFORE, the State of Indiana respectfully requests that this Court enter judgment against Google and in favor of the State of Indiana as to the counts described above as follows:

- a. Permanently enjoining Google, its representatives, successors, assigns, officers, agents, servants, employees, and all other persons acting or claiming to act for, on behalf of, or in active concert or participation with Google, from continuing or engaging in the conduct complained of herein;
- b. Ordering Google to pay consumer restitution of money or property acquired by Google as a result of the conduct complained of herein pursuant to Indiana Code §24-5-0.5-4(c)(2), payable to the Office of the Attorney General in an amount to be determined at trial;
- c. Ordering Google to pay disgorgement of all profits and benefits obtained from its unlawful practices complained of herein, payable to the Office of the Attorney General in an amount to be determined at trial;
- d. Ordering the payment of civil penalties for each and every violation of the DCSA complained of herein as permitted by statute pursuant to Indiana Code § 24-5-0.5-4(g) and Indiana Code § 24-5-0.5-8, payable to the Office of the Attorney General in an amount to be determined at trial;
- e. Awarding the State of Indiana the costs of investigation and prosecution of this action pursuant to Indiana Code § 24-5-0.5-4(c)(4); and
- f. Granting any such further relief as the Court deems just and proper.

**JURY DEMAND**

The State of Indiana demands a trial by jury by the maximum number of jurors permitted by law.

Respectfully submitted,

THEODORE E. ROKITA  
Indiana Bar No. 18857-49  
Indiana Attorney General

Date: January 24, 2022

By: /s/ Douglas S. Swetnam  
DOUGLAS S. SWETNAM  
Indiana Bar No. 15860-49  
Douglas.Swetnam@atg.in.gov

/s/ Vanessa Voigt Gould  
VANESSA VOIGT GOULD  
Indiana Bar No. 26719-49  
Vanessa.Voigt@atg.in.gov

/s/ Jennifer Van Dame  
JENNIFER M. VAN DAME  
Indiana Bar No. 32788-53  
Jennifer.VanDame@atg.in.gov

Deputy Attorneys General  
302 West Washington Street  
IGCS – 5th Floor  
Indianapolis, IN 46204  
(317) 232-6294 (Swetnam)  
(317) 232-7979 (Fax)

*Counsel for State of Indiana*