

CAUSE NO. _____

THE STATE OF TEXAS,	§	IN THE DISTRICT COURT OF
Plaintiff,	§	
	§	
v.	§	VICTORIA COUNTY, TEXAS
	§	
GOOGLE LLC,	§	
Defendant	§	____ JUDICIAL DISTRICT

PLAINTIFF’S ORIGINAL PETITION

TO THE HONORABLE JUDGE OF SAID COURT:

Plaintiff, STATE OF TEXAS, acting by and through the Attorney General of Texas, KEN PAXTON (the “State”), complains of Defendant GOOGLE LLC (“GOOGLE,” the “Company,” or the “Defendant”), and for causes of action would respectfully show as follows:

INTRODUCTION

Google has become one of the richest companies in the world, in part, by deceiving Texans and profiting off their confusion. Specifically, Google has systematically misled, deceived, and withheld material facts from users in Texas about how their location is tracked and used and how to stop Google from monetizing their movements. More to the point, while many Texans may reasonably believe they have disabled the tracking of their location, the reality is that Google has been hard at work behind the scenes logging their movements in a data store Google calls “Footprints.” But while footprints generally fade, Google ensures that the location information it stores about Texans is not so easily erased.

Google leads its users to believe that they can easily control what location information the Company retains about them and how it is used. For example, Google has touted a setting called “Location History” as allowing users to prevent Google from tracking their location. Given Google’s representations, a reasonable user would expect that turning a setting called “Location

History” off means their location history is no longer tracked. But even with Location History off, Google deceptively continues to track users’ location history unless they successfully navigate a counterintuitive labyrinth of seemingly unrelated settings. And even if a user does survive the Google gauntlet of privacy controls to successfully disable all the appropriate location-related settings available to them, [REDACTED]

[REDACTED]. As Google employees themselves have recognized, this is “[d]efinitely confusing from a user point of view.”

One might wonder why it is so important to Google to mine its users’ personal information. The answer is that the majority of Google’s revenues derive from business-facing services—namely, targeted advertising and advertising analytics. And to support this lucrative arm of its business, Google harvests personal data—including locational data—which the Company uses both to market to its users and to evaluate the effectiveness of the advertisements it serves.

Under this model, every Texan Google user is a potential unwitting profit center. Yet, as Google knows, [REDACTED] the Company collects. Aggregated over time, this data paints an intimate mosaic that can effectively reveal a person’s identity and routines. Location data, for example, can be used to infer an individual’s home address, political or religious affiliation, sexual orientation, income, health status, and participation in support groups. It can also suggest major life events, such as marriage, divorce, and the birth of children.

Location data is even more powerful in the hands of Google due to the near ubiquity of Google products in users’ pockets, homes, and workplaces. The prevalence of Google technology allows the Company to derive detailed insights about users they may not even realize they have

revealed—especially when those users are misled to believe they have disabled the collection of sensitive information like location history.

The upshot is that Google uses its window into millions of Texans’ personal lives to sell “targeted” advertising designed to exert the maximum influence over those users. In so doing, the Company has reaped spectacular gains at the expense of Texans’ privacy. Indeed, Google has generated hundreds of millions—if not billions—of dollars of advertising revenues from ads presented to users in Texas alone.

Google, therefore, has a powerful financial incentive to obscure the details of its location-tracking practices and to make it difficult for users to opt out. Google’s ability to amass troves of data about its users as they move throughout Texas translates into improved advertising capabilities and an outsized share of the multibillion-dollar digital-advertising market.

Google’s incentive to cash in on the collection of Texans’ movements is inherently in conflict with its ethical obligations as one of the world’s most powerful technology companies. Indeed, Google correctly admits that “Users are not the experts in privacy and security, it’s actually Google,” and that “Google should be telling users what’s wrong, we should point out the anomalies, and guide users through their settings.”¹ Moreover, Google has long understood that its design choices deceive reasonable users. In one 2014 internal presentation, for instance, Google employees considered a specific scenario in which a Google user would reasonably be deceived by Google’s design choices. The example involved a hypothetical individual who “opted out of Google location” but then finds that, nevertheless, “Google maps has house-level accurate

¹ L. Newman, *The Privacy Battle to Save Google From Itself* (November 1, 2018), available at <https://www.wired.com/story/google-privacy-data/>.

location,” leaving the user wondering—in Google’s words—“how does Google know my location? I thought I said no!”

Despite Google’s obvious understanding of its obligation to users and the ongoing risk of deception, the truth is that Google’s exhaustive surveillance practices are most effective and profitable to Google when users have no meaningful awareness of the intimate details they are sharing, how their data is used and monetized, and no clear idea of how to limit Google’s access to details about their personal lives. As such, when given a choice between (a) doing the right thing by its Texan users and (b) using false, deceptive, and misleading practices to fuel profits—Google ignored its obligations to Texans and chose profits.

This is demonstrated by an August 13, 2018, Associated Press (“AP”) article, which revealed that Google “records your movements even when you explicitly tell it not to.”² The reporting concerned Google’s “Location History” setting, discussed above. As reported by the AP, Google had promised users that “with Location History off, the places you go are no longer stored.”

That promise was false and deceptive. Specifically, even when users had explicitly opted out of location tracking through the Location History setting, Google nevertheless recorded users’ locations via other means, including (but not limited to) a separate and seemingly unrelated setting called “Web & App Activity.” When the Web & App Activity setting is enabled, Google collects and stores a large swath of data, including location data, whenever the user interacts with Google products and services. Notably, although the Web & App Activity setting is automatically enabled for all Google Accounts, Google’s disclosures during Google Account creation did not even mention it until 2018.

² Ryan Nakashima, *Google tracks your movements, like it or not*, AP NEWS, August 13, 2018, available at <https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ecb>.

In the days following the AP report, many users disabled one or both of these location-related settings, presumably having learned for the first time that Google was keeping an alarmingly meticulous record of their whereabouts over days, weeks, months, and years. Even Google employees expressed surprise upon learning that the Company was collecting location data under the auspices of the seemingly unrelated Web & App Activity setting.

Google's ambiguous, contradictory, and incomplete statements about these controls all but guarantee that users do not understand when their location is retained by Google or for what purposes. In fact, Google's claims to give users "control" and to respect their "choice" largely serve to obscure the reality that, regardless of the settings users select, Google is likely still hard at work collecting, storing, and monetizing the very location data users seek to keep private.

DISCOVERY CONTROL PLAN

1. The discovery in this case is intended to be conducted under Level 3 pursuant to Tex. R. Civ. P. 190.4.
2. This case is not subject to the restrictions of expedited discovery under Tex. R. Civ. P. 169 because the State's claims include a claim for nonmonetary relief and claims for monetary relief, including penalties and attorneys' fees and costs in excess of \$1,000,000.

PUBLIC INTEREST

3. Plaintiff has reason to believe that Defendant has engaged in, and will continue to engage in, the unlawful practices set forth below. Plaintiff has further reason to believe Defendant has caused and will cause adverse effects to consumers in Texas, to legitimate business enterprises which lawfully conduct trade and commerce in this state, and to the State of Texas. Therefore, the Consumer Protection Division of the Office of the Attorney General of the State of Texas is of the opinion that these proceedings are in the public interest.

JURISDICTION

4. This action is brought by Attorney General KEN PAXTON in the name of the State of Texas and in the public interest under the authority granted him by section 17.47 of the Texas Deceptive Trade Practices-Consumer Protection Act, TEX. BUS. & COM. CODE ANN. § 17.41 et seq. (“DTPA”) upon the grounds that Defendant has engaged in false, deceptive, and misleading acts and practices in the course of trade and commerce as defined in, and declared unlawful by, subsections 17.46(a) and (b) of the DTPA. In enforcement suits filed pursuant to section 17.47 of the DTPA, the Attorney General is further authorized to seek civil penalties, redress for consumers, and injunctive relief.

DEFENDANT

5. Google LLC is a Delaware limited liability company with its principal place of business at 1600 Amphitheatre Parkway, Mountain View, California, 94043.
6. 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.
7. Google markets, advertises, offers, and provides its products and services throughout the United States, and the number of Google’s Texas users is likely in the millions.

VENUE

8. Venue of this suit lies in Victoria County, Texas because, under DTPA subsection 17.47(b), Defendant and its agents have done business in Victoria County, Texas by offering its goods and services to consumers and businesses in Victoria County, Texas.

TRADE AND COMMERCE

9. Defendant has, at all times described below, engaged in conduct which constitutes “trade”

and “commerce” as those terms are defined by subsection 17.45(6) of the DTPA.

ACTS OF AGENTS

10. Whenever in this Petition it is alleged that Defendant did any act, it is meant that Defendant performed or participated in the act or Defendant’s officers, agents, or employees performed or participated in the act on behalf of and under the authority of the Defendant.

NOTICE BEFORE SUIT

11. The Consumer Protection Division informed Defendant in general of the alleged unlawful conduct described below at least seven days before filing suit, as may be required by subsection 17.47(a) of the DTPA.

FACTUAL ALLEGATIONS

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

12. Google’s business is profiting from user data. Through its many consumer products and services, 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. Google’s advertising products generated nearly \$150 billion in revenue in 2020.

1. **Google Collects Location Data Via the Android OS and Google Apps and Services.**

13. 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 world and approximately half of smartphones in the United States since at least 2015.³ The Android operating system is free and open-source software. However, most

³ 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.

Android devices on the market include a suite of Google apps and application programming interfaces (“APIs”)⁴ (collectively, “Google Mobile Services”) that are preinstalled on a user’s device under a licensing agreement between Google and Android device manufacturers (“OEMs”).

14. 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,⁵ 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 are transmitted by the device to Google.
15. Google’s other consumer products include 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 users’ location data when they interact with certain Google apps and services, even when a user’s location is not needed to support the core functionality of the app or service.
16. On Android devices, certain Google apps are granted permission to collect users’ location data by default. Other Google apps ask permission from users to allow Google to collect location data. On many versions of Android, once apps are permitted to collect a user’s location data, they may continue to collect and transmit location data to Google unless the

⁴ An API is a software interface that connects computers or pieces of software to each other.

⁵ 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.

user remembers to revoke permission. And if a user elects not to grant permission, an app may continue to prompt the user to enable location settings until the user relents.

17. Furthermore, even if a user disables the settings that allow their device to transmit location data to Google, Google still approximates that user's location by using IP address⁶ information that is transmitted when the user interacts with many Google apps and services.

2. Location Data Is Highly Valuable to Google.

18. Some of Google's consumer products can be used at no direct financial cost to the user. But that is simply because it is the user that is for sale. Instead of charging money for its products, Google collects exhaustive personal data about its users when they engage with Google products, including their browsing history, location data, and information from their email. Google processes this data to draw inferences about individuals and groups of users that it monetizes through advertising and other business-facing services.
19. Google's advertising business is dependent on its collection of this personal data, and location data is particularly valuable. [REDACTED]
[REDACTED] In marketing materials directed at advertisers, Google actively publicizes its ability to provide better advertising services through location-based analytics and geo-targeted consumer advertising.
20. Because location data is key to Google's lucrative advertising business, the Company has a strong financial incentive to dissuade users from withholding access to that data. As detailed herein, Google has employed and continues to employ a number of deceptive practices to make it nearly impossible for users to stop Google from collecting their

⁶ An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol."

location data when using Google products. These practices include privacy-intrusive default location settings, hard-to-find location settings, misleading descriptions of location settings, repeated nudging to enable location settings, and incomplete or imbalanced disclosures of Google's location-data collection and processing.

21. In one striking example, Google dramatically reworded a pop-up window that prompted users to enable a setting so that the prompt no longer disclosed on its face that enabling the setting allowed Google to continuously collect the user's location. [REDACTED]

[REDACTED]. *See infra* § E(2).

The roll-out of this vague prompt [REDACTED]

[REDACTED].

B. Google Cloaks Its Location Monitoring in a Web of Unrelated Settings.

22. Google misleads its users by presenting them with a maze of settings the users must navigate should they dare to try to keep their whereabouts private. Aside from the sheer number of confusing settings, Google's deception lies in the reality that many of the settings ostensibly have nothing to do with location, some are activated by default, and some are simply insufficient to protect one's privacy, despite what Google leads users to believe. Google promises a path to its users out of the Google-created blizzard of location harvesting; however Google made sure to plant deceptive sign posts masquerading as privacy settings so no reasonable user could likely escape becoming a Google profit center.
23. At the highest level, Google's settings can be classified into two categories: Google Account settings and device-level settings. Google Account settings apply to data collected

from *any* device signed in⁷ to a user's Google Account. In contrast, device settings apply *only* to the specific device on which the setting appears. Below is a brief description of the settings most pertinent to Google's deceptive practices regarding location tracking.

1. Location-Related Google Account Settings.

24. Google's collection and use of location data is purportedly subject to at least three Google Account settings: Location History, Web & App Activity, and Google Ads Personalization ("GAP").

25. Location History is a Google Account feature that captures all the places where a signed-in user goes. [REDACTED]

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

[REDACTED]

[REDACTED]. Using those various signals, Google can track a user's precise location,⁸ [REDACTED]

26. [REDACTED]

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

27. The primary value of Location History data for Google lies in its profitability for advertising uses. Google links location data with other user data to draw inferences about

⁷ A device (or user) is "signed-in" to Google if the user has signed into the user's Google Account at device set-up or in connection with a Google app.

⁸ As used herein, "precise location" refers to the user's exact longitude and latitude.

the user including, for example, [REDACTED]

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

28. In addition, Google uses Location History data to provide advertisers with “store conversion” rates—i.e., the rate at which users who view an ad actually visit the advertised store. Google’s ability to follow their users’ movements in the physical world after they click on digital ads is a unique selling point for its advertising business.
29. Web & App Activity is a separate Google Account setting that collects, stores, and monetizes user location. Whereas Location History passively collects location information on all of a user’s movements, Web & App Activity records a user’s “transactional location”—i.e., the location of a signed-in user’s device when the user is interacting with certain Google products.⁹ For example, when a signed-in user conducts a search for “chocolate chip cookie recipe” on the Google Search app, Google collects the user’s location at the time of the search, along with details about the search, and stores that information to the user’s Web & App Activity log. Later, if the user searches for an address on Google Maps, Google again stores the user’s location at the time of that search, along with details about what was searched, to the same log.
30. Google uses Web & App Activity data to deduce user habits and interests for advertising purposes. Google’s ability to target ads to users based on information about their locations is critical to the success of its billion-dollar advertising business. From in or around 2015 to in or around 2019, Google used the Web & App Activity setting to log a user’s precise latitude and longitude.

⁹ A “supplemental” Web & App Activity setting also collects and stores information about the user’s interactions with non-Google apps and with non-Google websites on Google’s Chrome browser.

31. Because Location History and Web & App Activity are independent settings, disabling one does not impact whether a user's location is collected and stored by the other. In other words, even if a user attempts to prevent location tracking by disabling one of these settings, Google still tracks and monetizes that user's location through the other. And until recently, Google kept the data stored in connection with these settings indefinitely, unless the user manually deleted the data.
32. Google also offers users a Google Account setting related to personalized advertising—the GAP setting. The GAP setting purports to provide signed-in users the ability to opt out of personalized ads served by Google. Google told users that with this setting enabled, “Google can show you ads based on your activity on Google services (ex: Search, YouTube), and on websites and apps that partner with Google.”

2. Location-Related Device Settings.

33. Location-related device settings control whether a specific device transmits location information to apps, APIs, or other services on the user's device. Android devices have multiple location-related device settings.
34. 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 user disables this setting on their device, then no apps or services can access the device's location.
35. Second, Android devices have “app-specific” location settings. Using these settings, users 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 user's location in the background—i.e., even when no apps requiring location were in active use.

36. On Android devices, these two types of settings control the flow of location information to Google. For example, enabling the location “master switch” allows Google to collect and use location information from the user's device to improve an internal Google platform called Google Location Services.¹⁰ [REDACTED]

[REDACTED]

[REDACTED].

37. Android mobile devices also have other settings that purportedly give users control over other types of data collection that Google uses to determine the users' location. For example, Android users can control whether their device scans for nearby Wi-Fi access points or Bluetooth devices, both of which technologies Google uses to determine a user'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 user's precise location.
38. This complex web of settings misleads users into believing that they are not sharing their location with Google when, in fact, they are.

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

39. One way that Google misleads users regarding their location data is through the Google Account settings described above. As a result of deceptive practices with respect to these settings, Google has collected enormous amounts of location data from unwitting Texans

¹⁰ Google Location Services is also referred to as Google Location Accuracy.

and monetized that data in the service of Google's advertising offerings without Texans' knowledge or consent.

1. Google Misrepresented the Characteristics of the Location History and Web & App Activity Settings.

40. Google misrepresented and omitted material information regarding the Location History and Web & App Activity settings until at least 2019. These misrepresentations and omissions confused users about which settings implicate location data, making it more likely that Google would capture, store and profit from such data without users' knowledge or consent.
41. For years, Google assured Android users on a public webpage 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 users 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 represented Location History as the setting that, when turned off, empowered users to prevent Google from storing or saving their personal location information.
42. That representation was false. Even when Location History was off, Google deceptively continued to collect and store users' locations through other means. Namely, depending on a user's other settings, Google collected and stored location data through Google's Location Services feature, Web & App Activity, Google apps on the user's device, Wi-Fi and Bluetooth scans from the user's device, the user's IP address, and [REDACTED].
43. Google's statements prompting users to turn on Location History also falsely implied that

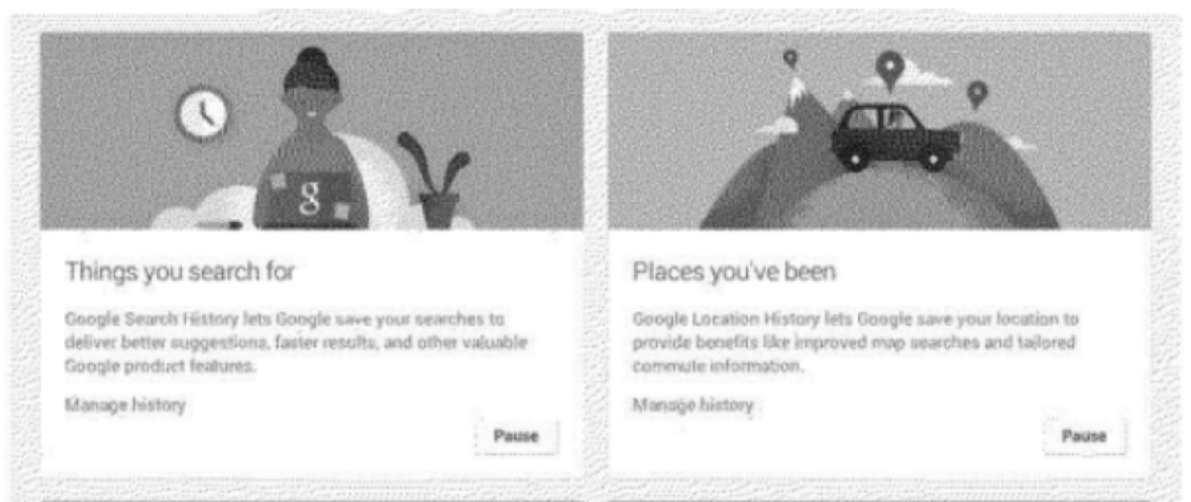
times, Google told users that enabling Location History “lets Google save your location;” allows Google to “store and use” the “places you go;” permits Google to “periodically store your location;” “allows Google to store a history of your location;” or allows Google “to save and manage your location information in your account.” Like Google’s statements on its webpages, these statements obscured the fact that the Location History setting does not alone control whether Google collects and saves a user’s location data.

44. Google’s misleading statements and omissions regarding Location History were exacerbated by separate misleading statements and omissions in connection with the Web & App Activity setting. Specifically, Google did not disclose to users that even when Location History is disabled, the Company still collects, stores, and uses location data through the Web & App Activity feature. This despite the fact that Google knew that location information is uniquely sensitive.
45. As alleged above, Web & App Activity collects location data when a user interacts with certain Google products. For example, if a user asks Google Assistant to search for the author of a book, Web & App Activity would save the user’s location and the time when the query was made—even with Location History off. Google also collects and stores information that could implicitly reveal a user’s location, such as the places a user inputs into Google Maps.
46. The 2018 AP story illustrated the extent of Google’s location tracking through Web & App Activity. The report provided a visual 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.

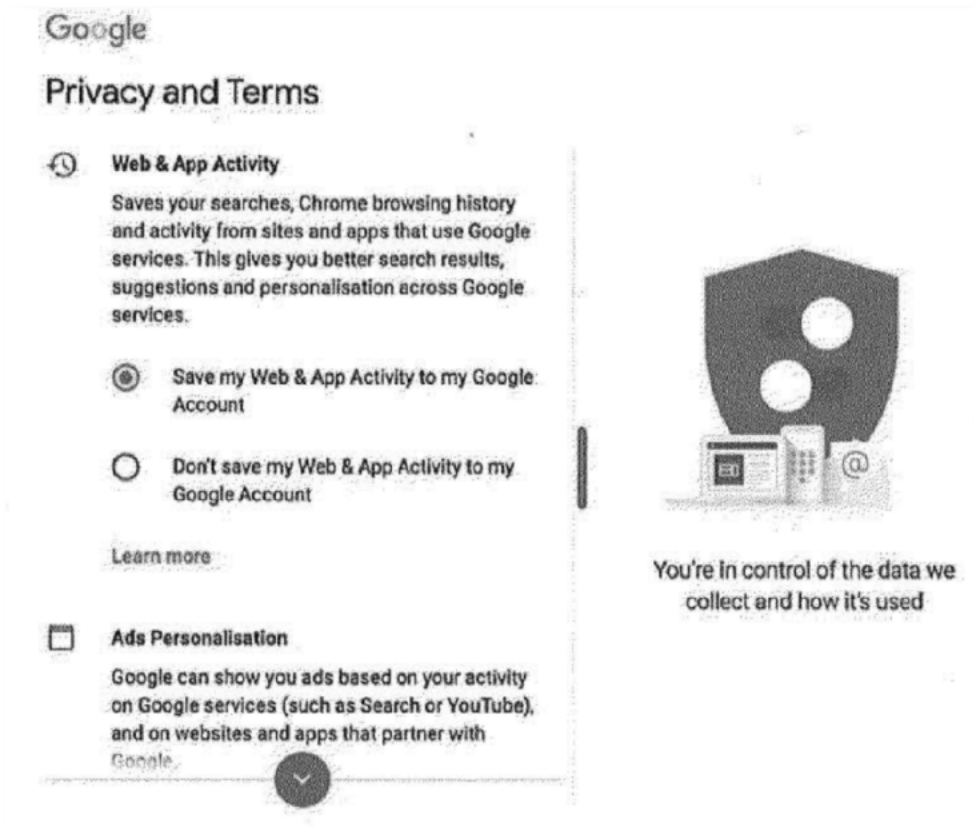
47. Google recognizes that the mosaic of the locations of individual users over time constitutes sensitive information. Despite this, Google concealed the fact that the Web & App Activity setting controlled Google's storage and use of location information. Moreover, users could not reasonably avoid Google's deceptive storage and use of their location because it occurred without their knowledge.
48. First, Google failed to disclose the Web & App Activity setting when users set up Google Accounts for the first time. Yet at this stage, the Web & App Activity setting is defaulted "on" for all Google Accounts. Thus, a user who sets up a Google Account is unknowingly automatically opted-in to location tracking (via Web & App Activity) unless the user learns about and affirmatively changes this setting. But until 2018, the Google Account set-up process made no mention of the Web & App Activity setting.
49. Furthermore, Android phones effectively require a user to sign in to a Google Account,¹¹ and Google apps like Search and Maps are granted location permission on Android devices by default. As a result, a new Android user could create a new Google Account, be automatically opted in to the Web & App Activity surveillance program, and then defaulted into granting location permissions to multiple Google apps, meaning Google could track that user's location across the user's Google Account and through several apps without even disclosing the existence of the setting or ever presenting the user with an option to opt out.

¹¹ A user 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. On information and belief, once Android users sign in to their Google Account, users can not sign out of Google. If they do not want to be signed in, their only option is to fully remove their Google Account(s) from their device.

50. One of the only ways users 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 users first landed on this webpage, Location History was presented as the only setting that related to location data. *See:*



51. In 2018, Google revised its Google Account set-up process to include the option to disable Web & App Activity. However, the Company still deceptively concealed from new users the fact that location data was captured by the setting. Until at least mid-2018, this information was only revealed to new users who first clicked on a link to see “More options” to customize settings and then selected a second link to “Learn More” about the Web & App Activity setting. [REDACTED]
- [REDACTED]
- [REDACTED]



52. Second, Google failed to disclose the Web & App Activity setting to users when they set up new devices using existing Google Accounts. A user's Web & App Activity "enabled" or "disabled" status applies to all devices signed in to the user's Google Account. Thus, any time a user signed in to an existing Google Account on any device, Google could begin tracking that device as long as Web & App Activity was enabled on the user's Account. Because Android devices need to be signed in to a Google Account to use critical functionalities and because users sign in to Google at Android device set-up, Google was able to track Android users via Web & App Activity as soon as they set up new devices on their Google Accounts. Users did not receive a separate notification that Google had begun storing the location of the new device via the Web & App Activity setting.
53. Third, Google did not identify Web & App Activity as a location-related setting in the places where a user would expect to find that information. For example, until around 2019, users 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," which described Google's location-based settings, discussed Location History without mention of the Web & App Activity setting. 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.
54. Finally, 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 things like Google search history and activity on Google apps—without mention of location (unless the user clicked on a link to a pop-up window for more information). Yet Google stores Web & App Activity data in, among other places, a data store it calls Footprints. It is difficult to imagine a more misleading incongruence than an arrangement where users are told they can prevent the storage of their location history by disabling a setting called Location History while the Company continues to store the users' location history in a data store called Footprints using a setting that the Company does not clearly advertise as implicating location history.

55. These design choices all reinforce Google's underlying deception that disabling Location History was sufficient to prevent Google from storing a user's location history, as Google promised. The name "***Location*** History" gives users every reason to believe that the setting controls the collection of their ***location*** history while nothing about the name "***Web & App*** Activity" gives users a reason to believe that setting tracks one's ***location*** history. Even a reasonable user would be misled and deceived. And that is even before considering Google's false promise that "with Location History off, the places you go are no longer stored."
56. In sum, Google misrepresented that disabling Location History stopped Google from storing a user's location and concealed that the Web & App Activity setting also stored location data. This tended to mislead users to believe that the Web & App Activity setting did not impact the collection, storage, or use of location data; that the Location History setting alone controlled whether Google retained and used location data; and that the

Location History setting would prevent Google from retaining and using the user's historical locations on an ongoing basis.

57. Both the gravity and the flagrance of these misrepresentations are demonstrated by 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." 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 being caught red-handed by the AP story, Google updated its help page to remove the false promise that "With Location History off, the places you go are no longer stored."

58. [REDACTED]
[REDACTED]
[REDACTED]. At its peak, the number of users who disabled at least one of these settings increased by over 500%. [REDACTED]
[REDACTED].

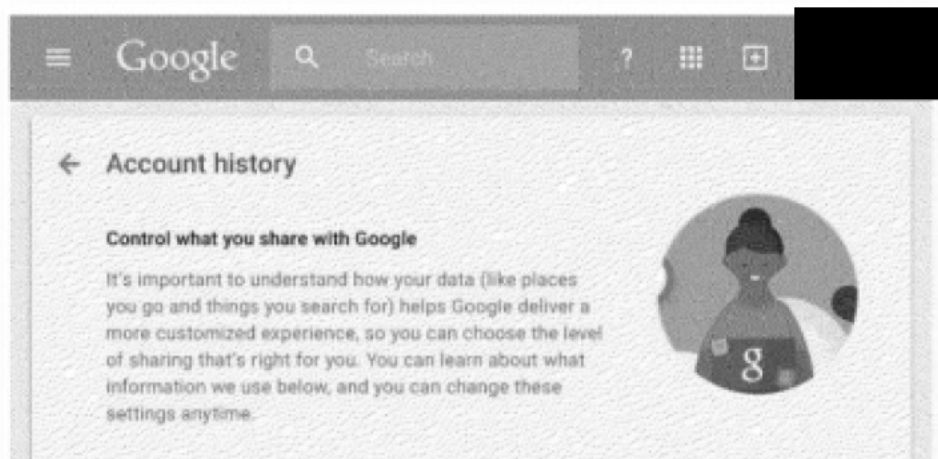
59. Internally, Google employees agreed that Google's disclosures regarding Location History were "definitely confusing" and that the user interface for Google Account settings "feels like it is designed to make things possible, yet difficult enough that people won't figure it out." One IT specialist at Google admitted, "I did not know Web and App Activity had anything to do with location."

60. Even before the AP article was published, however, [REDACTED]
[REDACTED]. Yet Google did not act to

correct this misleading impression or attempt to clarify the Web & App Activity and Location History settings until after the Company's misconduct was made public.

2. Google Misrepresents the Characteristics of its Other Google Account Settings.

61. Google also misleads users 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 Account settings offer seemingly simple "privacy controls" to attract users and lull them into a sense of security, but Google continues to exploit users' location data regardless of the choices users make with respect to these settings.
62. For years, Google has made misleading promises that users 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 users 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:*



63. 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 has also represented that it would “respect the choices you make to limit sharing or visibility settings in your Google Account.”
64. As part of setting up a Google Account, Google expressly tells users, “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....”
65. 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.”

66. In statements like these, Google frames Google Account settings as tools that allow a user to easily control Google’s collection and use of their personal data. The Company’s reassuring statements about these settings misleadingly imply that a user can stop Google from storing or deploying the user’s location information by disabling these settings.
67. But this is not true. [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED].
68. In other words, while touting user’s ability to control personal-data collection through Google Account settings, Google flouts that control by continuing to collect, store, and use location data regardless of whether the user disables these settings.
69. Google further misleads users by providing them only partial visibility into the location data Google collects. For example, Google’s current Privacy Policy claims that users can manage their privacy because they can “review and control information saved in [their] Google Account” and “decide what types of activity [they would] like saved in [their] account.” Earlier versions of the Privacy Policy likewise indicated that Google provides “transparency and choice” by allowing users to “access, manage, or delete information that is associated with [their] Google Account,” and stated 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 [users] to review and control data that’s created when [they] use Google services” and that “My Activity is a central place where [users] can view and manage [their] saved activity.”

70. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]. Users can delete this subset of location data, as well as Location History. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED].

71. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED].

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

73. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED].

74. Until May 2018, Google did not disclose in its Privacy Policy [REDACTED]
[REDACTED], who cannot prevent this form of data collection. 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]
[REDACTED].

75. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED].

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

76. Google is aware that users do not understand Google Account settings or how these settings
interact with other location-related settings. Google employees themselves admit that
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED].

3. Google Misrepresented the Characteristics of the Google Ad Personalization Setting.

77. Google's deceptive practices extend to the GAP setting as well. The GAP setting purportedly allows users to opt out of personalized advertising. Similar to Google's other practices, this setting allows users to "control" the Company's use of their location data only to an extent.
78. Google has explained that enabling the GAP setting will "Let Google use [a user's Google Account activity] to show [the user] more relevant ads on [Google's] services and on websites and apps that partner with [Google]." In connection with explaining this setting, Google told users that they should "let Google know [their] location," so that "[they] won't get ads for stores in other regions."
79. The GAP setting and Google's disclosures indicate that a user has control over whether Google will serve "personalized" ads based on the user's location. But this setting only provides an illusion of control. In reality, Google continues to target ads based on a user's location—both on and off Google products—even if the user opts out of ads personalization by disabling the GAP setting.
80. Rather than curing its deception, Google chose not to disclose to users who disable ad personalization that Google would continue to serve targeted ads based on the user's location anyways.

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

81. Google further confuses and misleads users into sharing more location data than they intended through deceptive practices that contradict the Company's representations and users' expectations regarding location-related device settings. Google conceals from users

that, even when they deny Google permission to access their location via device settings, Google continues to collect and store the users' location regardless of the user's explicit attempt to block Google's access to that information. Google misleads users in at least three respects.

82. **First**, Google tells users that they can control the flow of location data via the location “master switch.” Google includes this “master switch” on Google-licensed Android phones in order to provide this functionality. Furthermore, beginning with its May 2018 Privacy Policy, Google has represented that “the types of data [Google] collect[s] depend in part on [the user’s] device and account settings. For example, [a user] can turn [an] Android device’s location on or off using the device’s setting app.” Google also provided Help pages explaining how to turn off Android device location, including explanations such as: “If [a user] turn[s] off Location for [a] device, then no apps can use [the user’s] device location.” Today, Google tells users: “[Users] can allow Google and other apps to provide [users] with useful features based on where [a] device is located” “if [the user] choose[s] to turn on [the] device location.”
83. These representations, as well as the Android device setting itself, mislead users to believe that if they disable the master location setting, Google does not collect, store, or use their location to provide “services” (including ads) to the user. However, for years, including through today, Google has deceived users by failing to disclose that regardless of whether the user *explicitly forbids* Google from accessing location via a device, Google derives and stores the user’s location [REDACTED].
84. Specifically, when a user turns the location “master switch” off, believing that they are not sharing location information, Google nevertheless uses the user’s IP address [REDACTED]

[REDACTED] to infer the user's location. [REDACTED]

[REDACTED]

[REDACTED].

85. **Second**, app-specific device settings are also ineffective. Google includes these settings on Android devices to allow a user to deny device location information to specific apps. Further, Google provides Help pages explaining that, on Android devices, a user can choose which apps can access and use a user's device location. But contrary to what Google leads users to expect, Google still determines a user's approximate location [REDACTED]

[REDACTED]

[REDACTED], even when a user has denied location access to the app.

86. Yet, in disclosures up to at least 2019, Google claimed that IP addresses revealed only the *user's country*, and that Google would merely use this information to provide search results and identify the correct language—with no mention of advertising. Even today, on its webpage explaining “How Google uses location information,” the Company downplays the accuracy and precision with which it infers a user's location based on the user's IP address. The Company proffers only that IP addresses are “roughly based on geography” and allow Google to “get some information about your general area.”

87. **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 users to limit Google's access to this data when they intend to. 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, if this setting is “off,” Google can still obtain Wi-Fi scans. If a user has enabled a separate “Wi-Fi

connectivity” setting along with Google Location Services, Google continues to access and use Wi-Fi scanning to locate the user, even if Wi-Fi scanning was disabled by the user.

88. Simply put, even when a user’s mobile device is set to deny Google access to location data, the Company finds a way to continue to ascertain the user’s location. Google’s undisclosed practice of bypassing users’ location-related device settings constitutes a deceptive act or practice.

89. Because these practices are not clearly disclosed to users and contradict user expectations, users cannot reasonably avoid Google’s access to and use of their location data. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

As one Google employee correctly summed up user beliefs, “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 Users’ Ability to Make Informed Choices About Their Data.

90. In addition to misrepresenting the extent of user control and choice over location-data collection, Google has relied on, and continues to rely on, deceptive practices that make it difficult for users to decline location tracking or to evaluate the data collection and processing to which they are purportedly consenting.

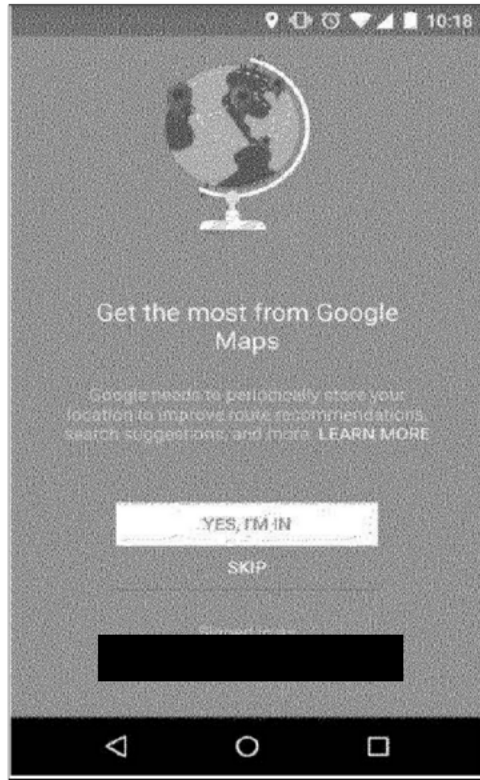
91. Such practices are known in academic literature as “dark patterns.” Dark patterns are deceptive design choices that alter the user’s decision-making for the designer’s benefit

and to the user's detriment. Dark patterns take advantage of behavioral tendencies to manipulate users into actions that are harmful to users 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.

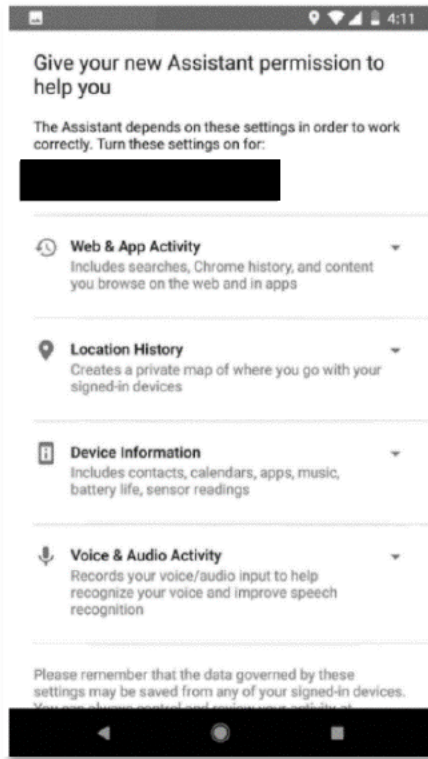
92. Because location data is immensely profitable to Google, the Company makes extensive use of dark patterns, including repeated nudging, misleading pressure tactics, and evasive and deceptive descriptions of features and settings, to cause users to provide more and more data (inadvertently or out of frustration), and to impede them from protecting their privacy.

1. Dark Patterns Exist in Google Account Settings.

93. Some of Google's deceptive practices with respect to Google Account settings already alleged above reflect the use of dark patterns. For example, Google's decision to enable by default the privacy-intrusive Web & App Activity feature, while failing to disclose this setting, was a deceptive design. By enabling privacy intrusive settings and then hiding those settings, Google not only misled users about the extent of its location tracking, but also made it more difficult for users to refuse this tracking.
94. Dark patterns are also evidenced in Google's presentation of "in-product" prompts to enable Google Account settings—i.e., prompts to enable these settings when a user begins to use Google apps and services on a device. For example, for at least part of the relevant time period, Google told users during setup that certain Google products, such as Google Maps, Google Now, and Google Assistant "need[]" or "depend[] on," the Location History feature. *See:*



95. However, these products could properly function without users agreeing to constant tracking. For example, Maps and Google Now did not “need” Location History to perform their basic functions and, in fact, both products would continue to function if the user later took a series of actions to disable Location History. Because Google’s statements falsely implied that users 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, users were left with effectively no choice but to enable these settings.
96. Google also designed the set-up process for certain Google products in a manner that limited users’ ability to decide whether to permit Google to track them. In particular, Google prompted users to enable Location History and Web & App Activity, along with multiple other settings, in order to use products like Google Assistant or Google Now. *See:*



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

98. Google also did not (and still does not) give users the choice to decline location tracking once and for all. If users decline to enable Location History or Web & App Activity when first prompted in the set-up process for an Android device, for instance, they are later shown further prompts to enable these settings when using Google products—despite already refusing consent to these services.

99. [REDACTED]

[REDACTED]

[REDACTED]. By repeatedly

“nudging” users to enable Google Account settings, Google increases the chances that a

user will relent and enable the setting inadvertently or out of frustration. Google does not and has never provided similarly frequent prompts to opt *out* of location sharing.

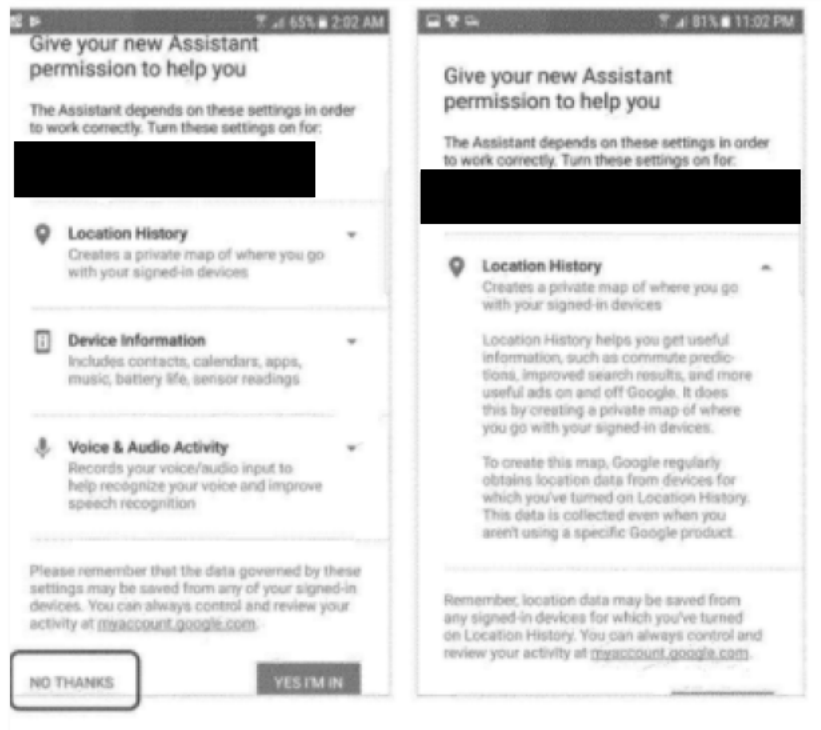
100.

[REDACTED]

101. Further, until at least mid-2018, users who read Google’s prompts to enable Google Account settings regarding location issues were provided only vague and imbalanced information about the effects enabling Google Account settings, until users clicked on discrete links that led to further information.

102. These prompts misleadingly emphasized a few benefits that Location History provided to users—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 were hard to find.

See:



103. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

104. At relevant times, users 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, users 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.” Users 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 users with sufficient information to understand what, if any, services would be limited, and they falsely implied that Google products would not function unless the user agreed to provide location data on a continuous basis.

2. Dark Patterns Exist in Device Settings.

105. Users who seek to limit Google’s location data collection through device settings also face an uphill battle to protect their privacy as a result of Google’s deceptive design practices. For example, users may try to limit Google’s surveillance of their location through the location “master switch” or the app-specific location permission settings. However, after disabling these settings, users are subject to repeated pressuring to re-enable location tracking when using various Google apps. One Google employee complained, [REDACTED]
- [REDACTED]
- [REDACTED]
106. Furthermore, once location is re-enabled on a user’s device, other Google apps and services can access the user’s location, including (in some versions of the Android OS) when the user is not interacting with the app. The only way to avoid such access is if the user remembers to disable location again, a process which the user is discouraged to undertake because it requires a number of steps and must be repeated every time a user wants to permit (and then deny) Google access to their location.
107. During the relevant time period, Google also actively sought to increase the percentage of users who enabled location settings on Android devices by providing vague disclosures

and making it more difficult for users to disable these settings. For example, in one version of Android (called KitKat),¹² Google offered a toggle that allowed users to disable location from a pull-down menu at the top of their screen. This made the setting more easily accessible to users. However, Google removed this toggle from Android phones that Google manufactured, [REDACTED]

[REDACTED]

[REDACTED]

108.

[REDACTED]

[REDACTED]

[REDACTED]

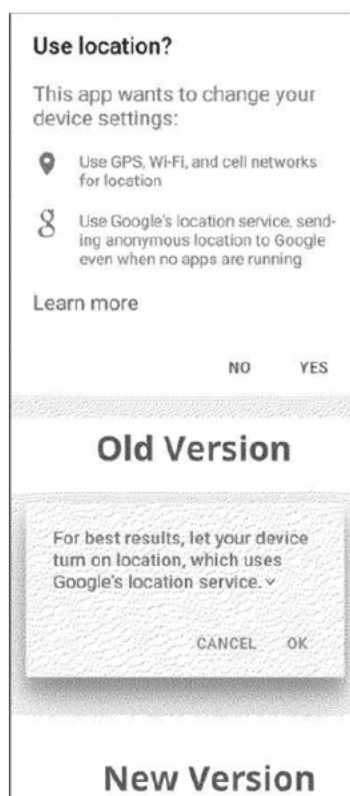
[REDACTED]

[REDACTED]

[REDACTED].

¹² Android KitKat was publicly released on October 31, 2013.

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



110. [REDACTED]
- [REDACTED]
- [REDACTED].
111. Google took these actions because it has profound financial incentives to pressure users into enabling location services and other location settings on their devices. Without these settings enabled, Google had a substantially reduced ability to ascertain, extract, and monetize the locations of its users.

FALSE, MISLEADING, OR DECEPTIVE ACTS

112. Defendant, as alleged above and detailed below, has in the course of trade and commerce engaged in false, misleading and deceptive acts and practices declared unlawful in §§17.46(a) and (b) of the DTPA. Such acts include:

A. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have or that a person has a sponsorship, approval, status, affiliation, or connection which he does not have, in violation of DTPA § 17.46(b)(5), including by representing, directly or by implication, that:

1. The Location History setting controlled whether Google retained and used users' location information
2. That disabling the Location History setting would prevent Google from retaining and using users' location information going forward;
3. The Web & App Activity setting did not impact Google's collection, storage, or use of location information;
4. Users could prevent Google from retaining and using their location information by disabling Google Account settings;
5. Users could review and manage all location data associated with their Google Account and/or otherwise retained by Google for its commercial use;
6. Users had a choice about or could control whether Google collected their location information;
7. Users could prevent Google from using their location to target advertisements by disabling Google Account settings;

8. Users could prevent Google from collecting, storing, and using users' location by adjusting device settings that control whether device location is enabled;
 9. Users could prevent Google from collecting, storing, and using users' location by adjusting device settings that control whether device location is shared with specific Google apps;
- B. Representing that an agreement confers or involves rights, remedies, or obligations which it does not have or involve, or which are prohibited by law, in violation of § 17.46(b)(12); and
- C. Failing to disclose information concerning goods or services which was known at the time of the transaction with the intent to induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed in violation of § 17.46(b)(24), including failing to disclose the following material facts:
1. Google continued to collect and store users' location information even with Location History disabled (i.e., turned off);
 2. Location information was collected through the Web & App Activity feature;
 3. Users cannot not prevent Google from retaining and using users' locations by adjusting Google Account settings;
 4. Users cannot prevent Google from using their location to target advertisements by disabling Google Account settings;
 5. Google continues to collect location information even when a device's

location is turned off; and

6. Google apps that are denied permission to access location data can still obtain that data from other sources available to Google, [REDACTED].

TRIAL BY JURY

113. Plaintiff herein requests a jury trial and will tender the jury fee to the County District Clerk's office pursuant to TEX. R. CIV. P. 216 and the TEX. GOV'T CODE ANN. § 51.604.

PRAYER FOR RELIEF

114. Plaintiff further prays that Defendant be cited according to law to appear and answer herein; that after due notice and hearing a TEMPORARY INJUNCTION be issued; and upon final hearing a PERMANENT INJUNCTION be issued, restraining and enjoining Defendant, Defendants' officers, agents, servants, employees and attorneys and any other person in active concert or participation with Defendant from violating the DTPA.
115. In addition, Plaintiff respectfully prays that this Court will:
 - A. Order Defendant to pay restitution to restore all money or other property taken from identifiable persons by means of unlawful acts or practices, or in the alternative award judgment for damages to compensate for such losses;
 - B. Adjudge against Defendant civil penalties in favor of Plaintiff in the amount of not more than \$10,000 per violation of the DTPA;
 - C. Order Defendant to pay Plaintiff's attorney fees and costs of court pursuant to the TEX. GOVT. CODE, § 402.006(c);
 - D. Order Defendant to pay both pre-judgment and post judgment interest on all awards

of restitution, damages or civil penalties, as provided by law.

116. Plaintiff further prays that this court grant all other relief to which Plaintiff may show itself entitled.

Respectfully submitted,

NORTON ROSE FULBRIGHT US LLP

NORTON ROSE FULBRIGHT US LLP

/s/ Marc B. Collier

Marc B. Collier

Texas State Bar No: 00792418

Marc.collier@nortonrosefulbright.com

Julie Searle

Texas State Bar No: 24037162

Julie.Searle@nortonrosefulbright.com

Chris Cooke

(pro hac to be sought)

Christopher.cooke@nortonrosefulbright.com

Sean Patrick McGinley

Texas State Bar No: 24116740

Sean.patrick.mcginley@nortonrosefulbright.com

Chase Sippel

Texas State Bar No. 24126753

Chase.sippel@nortonrosefulbright.com

98 San Jacinto Blvd., Suite 1100

Austin, Texas 78701

(512) 474-5201 – Tel

(512) 536-4598 – Fax

Vic Domen

Vic.domen@nortonrosefulbright.com

(pro hac to be sought)

799 9th Street NW, Suite 1000

Washington, DC, 20001

(202) 662-0200 – Tel

/s/ Joseph Graham

Joseph Graham

Texas State Bar No: 24044814

Joseph.graham@nortonrosefulbright.com

M. Miles Robinson

Texas State Bar No. 24110288

Miles.robinson@nortonrosefulbright.com

Fulbright Tower

1301 McKinney, Suite 5100

Houston, Texas 77010-3095

(713) 651-5151 – Tel

(713) 651-5246 – Fax

/s/Ronald B. Walker

Ronald B. Walker

State Bar No. 20728300

rwalker@walkerkeeling.com

WALKER KEELING LLP

101 W. Goodwin, Ste. 400

Post Office Box 108

Victoria, Texas 77902

Tel. (361) 576-6800

Fax (361) 576-6196

KEN PAXTON
Attorney General

/s/ Shawn E. Cowles

Brent Webster, First Assistant Attorney
General of Texas

Brent.Webster@oag.texas.gov

Grant Dorfman, Deputy First Assistant
Attorney General

Grant.Dorfman@oag.texas.gov

Murtaza Sutarwalla, Deputy Attorney
General for Legal Counsel

Murtaza.Sutarwalla@oag.texas.gov

Aaron Reitz, Deputy Attorney General
For Legal Strategy

Aaron.Reitz@oag.texas.gov

Shawn E. Cowles, Deputy Attorney
General for Civil Litigation

Shawn.Cowles@oag.texas.gov

Nanette DiNunzio, Associate Deputy
Attorney General for Civil Litigation

Nanette.Dinunzio@oag.texas.gov

Ralph Molina, Special Counsel to the
First Assistant Attorney General

Ralph.Molina@oag.texas.gov

Steve Robinson, Chief,
Consumer Protection Division
Steven.Robinson@oag.texas.gov

Pedro Perez, Deputy Chief,
Consumer Protection Division

Pedro.Perez@oag.texas.gov

Jennifer Roscetti, Deputy Chief,
Consumer Protection Division

Jennifer.Roscetti@oag.texas.gov

Brad Schuelke, Assistant Attorney General,
Consumer Protection Division

Brad.Schuelke@oag.texas.gov

James Holian, Assistant Attorney General,
Consumer Protection Division

James.Holian@oag.texas.gov

Patrick Abernethy, Assistant Attorney
General, Consumer Protection Division

Patrick.Abernethy@oag.texas.gov

Jacob Petry, Assistant Attorney General,
Consumer Protection Division

Jacob.Petry@oag.texas.gov

Jameson Joyce, Assistant Attorney General,
Consumer Protection Division

Jameson.Joyce@oag.texas.gov

Tamra Fisher, Assistant Attorney General,
Consumer Protection Division

Tamra.Fisher@oag.texas.gov

OFFICE OF THE ATTORNEY GENERAL OF TEXAS

P.O. Box 12548

Austin, TX 78711-2548

(512) 936-1674

Attorneys for Plaintiff State of Texas