IN THE SUPERIOR COURT OF THE DISTRICT OF COLUMBIA Civil Division

DISTRICT OF COLUMBIA

a municipal corporation 441 4th Street, N.W. Washington, D.C. 20001,

Plaintiff,

Case No.:

v.

GOOGLE LLC,

1600 Amphitheatre Parkway, Mountain View, California, 94043,

Defendant.

JURY TRIAL DEMANDED

COMPLAINT FOR VIOLATIONS OF THE CONSUMER PROTECTION PROCEDURES ACT

Table of Contents

INTRO]	DUCTION	1
PARTII	ES	3
JURISD	DICTION AND VENUE	4
FACTU	AL ALLEGATIONS	4
Α. (Google's Business Model Relies on Constant Surveillance of Google Users	4
1.	Google Collects Location Data Via the Android OS and Google Apps and Services.	. 5
2.	Location Data Is Highly Valuable to Google.	6
	Google Users Must Navigate Numerous, Conflicting Controls to Protect Their tion Data.	7
1.	Location-Related Google Account Settings	7
2.	Location-Related Device Settings	9
	Google Deceives Users Regarding Their Ability to Protect Their Privacy Throug	
1.	Google Misrepresented and Omitted Material Facts Regarding the Location History and Web & App Activity Settings.	l 1
2.	Google Misrepresents and Omits Material Facts Regarding Users' Ability to Control Their Privacy through Google Account Settings	17
3.	Google Misrepresented and Omitted Material Facts Regarding the Google Ad Personalization Setting	
	Google Deceives Users Regarding Their Ability to Protect Their Privacy Throug	
	Google Uses Deceptive Practices that Undermine Users' Ability to Make med Choices About Their Data	24
1.	Dark Patterns in Google Account Settings	24
2.	Dark Patterns in Device Settings.	29
F. (Google Engages in Deceptive and Unfair Trade Practices in the District	32
CAUSE	S OF ACTION	32
PRAYE	R FOR RELIEF	36
HIRVE	DEMAND	36

INTRODUCTION

- 1. This is an action by the above-captioned plaintiff, the District of Columbia (the "District"), by and through the Office of the Attorney General, against Defendant Google LLC ("Google" or the "Company") for the Company's use of deceptive and unfair practices to obtain valuable consumer location data, in violation of the District's Consumer Protection Procedures Act ("CPPA"), D.C. Code § 28-3901, et seq.
- 2. Since at least 2014, Google has deceived consumers regarding how their location is tracked and used by the Company and consumers' ability to protect their privacy by stopping this tracking. Google leads consumers to believe that consumers are in control of whether Google collects and retains information about their location and how that information is used. In reality, consumers who use Google products cannot prevent Google from collecting, storing, and profiting from their location.
- 3. Google is primarily known as a technology company that provides a range of consumer products, including 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 digital advertising. 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.
- 4. Location data is among the most sensitive information Google collects from consumers. Even a limited amount of such data, gathered over time, can expose a person's identity and routines. Location can also be used to infer 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.
- 5. 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 near ubiquity of Google

products in consumers' pockets, homes, and workplaces—essentially everywhere consumers go. Google's technologies allow it to analyze massive amounts of location data from billions of people, and to derive insights that consumers may not even realize they revealed. Google uses this window into consumers' lives to sell advertising that is "targeted" to consumers according to personal details Google has learned about them, including their demographics, habits, and interests.

- 6. 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 consumers translates to better advertising capabilities and a greater share of the multi-billion-dollar digital advertising market. Google has generated tens of millions of dollars of advertising revenues from ads presented to consumers in the District alone.
- 7. 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. The District files this suit to correct the deceptive and unfair practices that Google has used and uses to obtain consumers' location data, and to ensure that consumers are able to understand and control the extent to which their location data is accessed, stored, used, and monetized by the Company.
- 8. Some of the issues giving rise to this lawsuit became broadly known to the public on August 13, 2018, when the Associated Press ("AP") revealed in an article 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."
- 9. The AP story exposed that Google's promise to consumers was false. Even when consumers explicitly opted out of location tracking by turning the Location History setting off, Google nevertheless recorded consumers' locations via other means, including (but not limited to) a separate setting called "Web & App Activity." Web & App Activity collects and stores data

about a consumer, including location data, when the consumer interacts with Google products and services. Although the Web & App Activity setting is automatically turned "on" for all Google Accounts, the Company's disclosures during Google Account creation did not mention or draw consumers' attention to the setting until approximately 2018.

10. In the days following the AP report,

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.

- 11. The District subsequently commenced an investigation into Google's location tracking practices. The District's investigation revealed that Google also offers other settings that purport to give consumers control over the location data Google collects and uses. But Google's misleading, ambiguous, and incomplete descriptions of these settings all but guarantee that consumers will not understand when their location is collected and retained by Google or for what purposes. And, in reality, regardless of the settings they select, consumers who use Google products have no option but to allow the Company to collect, store, and use their location.
- 12. With this suit, the District 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 CPPA.

PARTIES

13. Plaintiff the District of Columbia, a municipal corporation empowered to sue and be sued, is the local government for the territory constituting the seat of the government for the United States. The District brings this action through its chief legal officer, the Attorney General for the District of Columbia. The Attorney General has general charge and conduct of all legal business of the District and all suits initiated by and against the District and is responsible for

upholding the public interest. D.C. Code § 1-301.81(a)(1). The Attorney General is specifically authorized to enforce the District's consumer protection laws, including the CPPA.

- 14. Google LLC is a Delaware limited liability company with its principal place of business at 1600 Amphitheatre Parkway, Mountain View, California, 94043.
- 15. Google is a technology company that specializes in Internet-related products and services, which include online advertising technologies, search, cloud computing, and other software and hardware. Google markets, advertises, offers, and provides its products and services throughout the United States, and to consumers in the District.
- 16. At all relevant times Google acted with the knowledge and understanding that the activities described in this Complaint would affect users of Google's products and services throughout the United States, including in the District.

JURISDICTION AND VENUE

- 17. This Court has jurisdiction over the subject matter of this case pursuant to D.C. Code §§ 11-921 and 28-3909.
- 18. This Court has personal jurisdiction over Google pursuant to D.C. Code § 13-423(a).

FACTUAL ALLEGATIONS

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

19. Google is an advertising company, but its business is user¹ data. Through its many consumer products and services, Google collects and analyzes the personal 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. On information and belief, Google's advertising products generated nearly \$150 billion in revenue in 2020.

4

¹ For purposes of this Complaint, the terms "consumer" and "user" are used interchangeably to refer to a consumer who has used or uses Google's products and services.

- 1. <u>Google Collects Location Data Via the Android OS and Google Apps and Services.</u>
- 20. 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 2015.² The Android operating system is free and open-source software. However, most Android devices on the market include a suite of Google applications ("apps") and application programming interfaces ("APIs")³ (collectively, "Google Mobile Services") that are preinstalled on a user's device pursuant to licensing agreements between Google and Android device manufacturers ("OEMs").
- 21. 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,⁴ Google can track the precise location of a device on a continuous basis, using GPS coordinates, cell tower data, Wi-Fi signals, and other signals that the device transmits to Google.
- 22. 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 accessed on both Android and Apple iOS devices (such as iPhones), as well as through web browsers. These products are 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.
- 23. 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

² The smartphone market is generally split between two operating systems, Apple's "iOS" and Google's Android OS. Apple's iOS is used on all iPhone and iPad devices.

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

⁴ 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.

location data. On many versions of Android, once Google apps are permitted to collect a user's location data, they may continue to transmit that data to Google unless the user remembers to revoke permission. And if a user declines to grant permission, an app may continue to prompt the user to enable location-related permission settings.

- 24. 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). In addition, the user is not fully shielded from tracking by Google. Google *still* continues to estimate a user's location by using IP address⁵ information that is transmitted when the user interacts with Google apps and services.
 - 2. <u>Location Data Is Highly Valuable to Google.</u>
- 25. Some Google 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. Google collects exhaustive personal data about its users when they engage with these products. Google then processes this data to draw inferences about users that it monetizes through advertising.
- 26. Google's advertising business depends on its collection of this personal data, and location data is particularly valuable information for this business.

In marketing materials directed at advertisers, Google actively publicizes its ability to provide more effective advertising through geo-targeting and location-based analytics.

27. Because location data is key to Google's lucrative advertising business, the Company has a 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 and unfair practices to obtain users' "consent" to be tracked and to make it nearly impossible for users to stop

⁵ An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol."

Google from collecting their location data. 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 disclosures of Google's location data collection and processing.

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

See infra §

E(2). The roll-out of this vague prompt

B. Google Users Must Navigate Numerous, Conflicting Controls to Protect Their Location Data.

- 29. Google users must navigate numerous, conflicting settings that supposedly control when and how Google collects, stores, and uses their location information. At the highest level, these settings can be classified into two categories: Google Accounts settings and device settings. Google Account settings apply to data collected from any device that is signed in 6 to a Google Account. In contrast, device settings apply *only* to the specific device on which the setting appears and do not require a user to be signed into a Google Account.
 - 1. Location-Related Google Account Settings.
- 30. 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").
- 31. Location History is a Google Account feature that captures all the places where a signed-in user goes.

⁶ 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 on their device.

	. Location History has existed
in some form	since approximately 2009.
	Using those various signals, Google can track a user's precise location, ⁷
32.	
	Using this information, Google builds a "private
map" of all th	ne places a user has been, which the user can review and edit.
33.	The value of Location History data for Google, however, lies in its advertising uses.

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

Google

- 34. In addition, Google uses Location History data to provide advertisers with "store conversion" rates—i.e., the number of users who have viewed ads and then visited the advertised store. Google's ability to track users' physical locations after they click on digital ads is a unique selling point for its advertising business.
- 35. Web & App Activity is a separate Google Account setting pursuant to which Google collects, stores, and monetizes users' locations. Whereas Location History collects information on all of a user's movements, Web & App Activity records a signed-in user's "transactional location:" that is, the location of a signed-in user's device when the user interacts with certain Google products.⁸

⁷ As used herein, "precise location" refers to the user's exact longitude and latitude.

⁸ 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.

- 36. 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 such as what was searched, to Web & App Activity. Google uses Web & App Activity data to make deductions about the user for advertising purposes.
- 37. Location History and Web & App Activity are independent settings. Disabling one setting does not impact whether location data is collected and stored pursuant to the other setting. This means that even if a user prevents location tracking by one of these services, Google still tracks and monetizes the user's location through the other. Until recently, Google kept the data stored in connection with these settings indefinitely, unless the user manually deleted the data.
- 38. 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 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, users who do not want Google to serve them ads based on their activity on Google services should be able to opt out by disabling this setting. However, Google continues to target ads to a user based on a user's location even if the user opts out of ads personalization by disabling the GAP setting.

2. <u>Location-Related Device Settings.</u>

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

- 40. First, Android devices have a location "master switch" that controls whether the device can share the device's precise location with any apps or services on the device. When this "master switch" is enabled, apps and services can access data about the device's location from device sensors, such as GPS. If a user disables this setting on their device, no apps or services can access data from the device's location sensors.
- 41. Second, Android devices have "app-specific" location settings. Using these device settings, users can grant or deny a specific app, such as Google Maps or Uber, permission to access data from the device's location sensors. On some versions of Android, apps with location permission could access a user's location in the background (i.e., when the app is not in use).
- 42. 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 user's device in order to improve a Google platform called Google Location Services.⁹
- 43. Android mobile devices also have other settings that purportedly control access to specific types of location data. For example, Android users can control whether their device scans for nearby Wi-Fi access points or Bluetooth devices, which can help Google interpret the 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, GPS, or Google Location Services, to ascertain the user's precise location.
- 44. In order to protect their privacy, users must understand the nuanced and interrelated functions of Google Account settings and device settings. This complex web of settings misleads users into believing that they are not sharing their location with Google when in fact they are.

⁹ Google Location Services is also referred to as Google Location Accuracy.

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

- 45. One way that Google misleads users regarding their location data is through Google Account settings. As a result of deceptive and unfair trade practices with respect to these settings, Google has collected enormous amounts of location data from unwitting users and monetized that data in the service of Google's advertising offerings without users' knowledge or consent.
 - 1. <u>Google Misrepresented and Omitted Material Facts Regarding the Location History and Web & App Activity Settings.</u>
- 46. From at least 2014 to at least 2019, Google made misrepresentations regarding how the Location History and Web & App Activity settings used and collected location data. These misrepresentations confused users about which settings implicate location data, enabling Google to capture, store, and use such data without users' knowledge or consent.
- Android users that "[y]ou can turn off Location History at any time. With Location History off, the places you go are no longer stored" (emphasis added). 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" (emphasis added). Google thus presented Location History as the setting that controlled whether Google stored location information about a user.
- 48. That representation was deceptive. Even when Location History was off, Google continued to collect and store users' locations. Depending on a user's other settings, Google collected and stored a user's location data through Web & App Activity, Google apps on the user's device, Wi-Fi and Bluetooth scans from the user's device, Google's Location Services feature, the user's IP address, and
- 49. Google's statements prompting users to turn on Location History also deceptively implied that this setting alone allowed Google to store a user's location. For example, at various

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." These representations omit that Google collected and saved users' location data when using Google products whether or not the user enabled Location History.

- 50. Google's misrepresentations regarding Location History were exacerbated by separate misrepresentations in connection with the Web & App Activity setting. Google recognizes that the location of individual users over time constitutes sensitive information. Despite this, Google did not disclose that the Company collects, stores, and uses location data when Web & App Activity is enabled.
- 51. 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. Google also collects and stores information that could implicitly reveal a user's location, such as which places the user inputs into Google Maps.
- 52. 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.
- 53. Google concealed from users that the Web & App Activity setting controlled Google's storage and use of their location information in at least three ways.
- 54. First, Google did not disclose the Web & App Activity setting when users 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 user 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.

- 55. Furthermore, Android phones effectively require a user to sign in to a Google Account.¹⁰ In addition, Google apps like Search and Maps were (and are) granted location permission on Android devices by default. As a result, Google could track Android users' location without ever presenting users with an option to opt out.
- 56. One of the only ways users would become aware that Web & App Activity was storing location data was by navigating to a separate webpage called "My Activity" where Google recorded data stored under the Web & App Activity setting. But when users first landed on this webpage, Location History was presented as the only setting that related to location data. *See*:

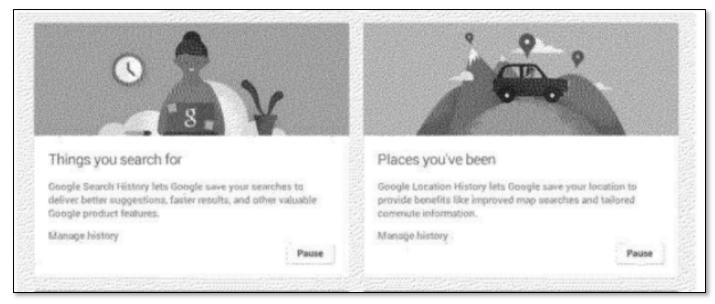


Fig. 1 ("Places you've been[:] Google Location History lets Google save your location to provide benefits like improved map searches and tailored commute information.")

¹⁰ A user must sign in to a Google Account on their Android device to access the Google Play 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 users sign into their Google Account, users must fully remove their Google Account(s) from their device in order to sign their device out of Google.

57. In 2018, Google revised its Google Account set-up process to reference Web & App Activity. However, the Company continued to conceal from new users 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" and then selected a second link to "Learn More" about the Web & App Activity setting.

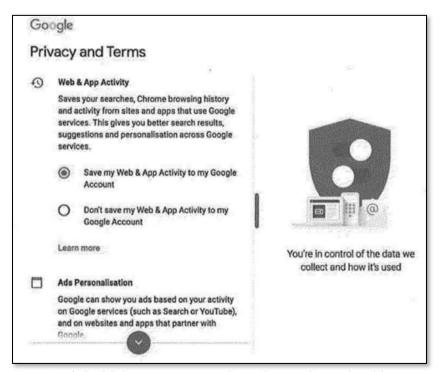


Fig. 2 ("Web & App Activity[:] Saves your searches, chrome browsing history and activity from sites and apps that use Google services. This gives you better search results, suggestions and personalization across Google services.")

58. 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 any device in to an existing Google Account, Google could begin tracking that device as long as Web & App Activity was enabled on the user's Google Account. Because Android

devices need to be signed in to Google to use critical functionalities and users sign in to Google at 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, without notifying those users.

- 59. Third, once consumers set up a Google Account or link 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 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" described Google's location-based settings and discussed Location History without mention of the Web & App Activity setting.
- 60. 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 specifically mention that "Location History allows Google to store a history of your location data," but makes no reference to the Web & App Activity setting.
- 61. 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 link to a pop-up window for more information).
- 62. 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 Google's 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. Users could not avoid Google's deceptive and unfair storage and use of their location because it occurred without their knowledge.

- 63. These misrepresentations and omissions were material to Google users in the District, as demonstrated by, among other things, users' 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."
- 64. 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."

	65.	The AP article set off a frenzy of negative press coverage. Google closely tracked
the pub	lic rela	ations fall-out,
	66.	

- 67. In internal discussions, 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 employee admitted, "I did not know Web and App Activity had anything to do with location."
- 68. Even before the AP article was published.

 Yet Google did not act to clarify the Web & App Activity and Location History settings until after the Company's misconduct was made public.
 - 2. <u>Google Misrepresents and Omits Material Facts Regarding Users' Ability to Control Their Privacy through Google Account Settings.</u>
- 69. Google misleads users about its location tracking practices by misrepresenting the extent to which Google Account settings control and prevent Google's collection and use of location data. Google offers simple "privacy controls" to attract users but continues to exploit users' location data regardless of their choices with respect to these settings.
- 70. Since at least 2014, 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*:

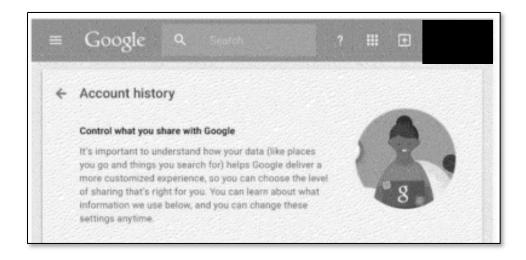


Fig. 3 ("Control what you share with Google[:] It's important to understand how your data (like places you go and things you search for) helps Google deliver a more customized experience, so you can choose the level of sharing that's right for you. You can learn about what information we use below, and you can change these settings anytime.")

- 71. 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."
- 72. 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. . . ."
- 73. 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."

- 74. In statements like these, Google frames Google Account settings as tools that allow a user to control the information Google collects and uses when a user interacts with Google products, including location information. 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.
- 75. But this is not true. Regardless of whether the user has disabled Web & App Activity or Location History, Google collects, stores, and uses location data when a user uses certain Google products,

While touting users' ability to control personal data collection through Google Account settings, Google flouts these controls by continuing to collect, store, and use location data regardless of whether the user disable these settings.

76. Google further misleads users by providing users only partial visibility into the location data Google collects about them. 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," "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 users 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 [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."

77.

	Users can delete this subset of location data, as well
as their Location	n History.
78.	
79.	Despite claiming it endeavors to "be clear about what information [Google]
collects, so tha	[users] can make meaningful choices about how it is used,"
80.	
81.	Until May 2018, Google did not disclose in its Privacy Policy that it stores
	m signed-out users. Even today, the webpage devoted to explaining "How Google
uses location i	nformation" only explains how location data is "saved in [a] Google Account,"

82. Put simply, contrary to the Company's representations, disabling or enabling
Google Account settings does not control whether Google will collect, store, or use a user's
location data. Even disabling <u>all</u> Google Account settings
not effective to prevent Google from storing and using a user's location data. As a result of
Google's misleading statements with respect to these settings, users cannot avoid Google's access
to and use of their location data.

83.	Google is aware that users do not understand Google Account settings or how these			
settings inter	settings interact with other location-related settings.			

- 3. <u>Google Misrepresented and Omitted Material Facts Regarding the Google Ad Personalization Setting.</u>
- 84. Google's deceptive and unfair practices extend to the Company's Google Ad Personalization (GAP) setting. The GAP setting purports to allow users to opt out of personalized advertising. Consistent with Google's other practices, this setting allows users to "control" the Company's use of their location data only to an extent.
- 85. According to Google, the GAP setting will "[l]et 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 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."
- 86. 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 user's location—both on and off Google products—even if the user opts out of ads personalization by disabling the GAP setting.

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

- 87. Google further misleads users into sharing location data through deceptive and unfair practices that contradict users' expectations regarding location-related device settings. Specifically, Google misrepresents the ability of users to control or limit Google's collection of their location data through their device settings. Google misleads users and withholds material facts about device settings in at least three respects.
- 88. *First*, Google tells users 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 with its May 2018 Privacy Policy, Google represents that "the types of location 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 that explain: "If [a user] turn[s] off Location for [a] device, then no apps can use [the user's] device location."
- 89. These representations, as well as the Android device setting itself, state and/or imply that when users disable the master location setting, Google does not collect, store, or use the user's location to provide "services" (including ads) to the user. However, since at least 2014 through the present, 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 and

	90.	Specifically, when a user turns the loca	tion "master switch" off, be	elieving that they
are not sharing location information, Google nevertheless uses the user's IP address				ddress
			to infer the user's locatio	n. Users have no
contro	l over w	hether Google derives their location		

- 91. **Second**, Google misleads users into believing that a 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. But contrary to what Google leads users to expect, when a user has denied location access to a Google app, Google deduces a user's location
- 92. *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. 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 user toggles this setting "off," Google can still obtain Wi-Fi scans from the user's device.
- 93. 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 and unfair practice. 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.

94.	

As one Google employee put it, "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 Uses Deceptive Practices that Undermine Users' Ability to Make Informed Choices About Their Data.

- 95. Google has relied on, and continues to rely on, deceptive and unfair 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. 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.
- 96. 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 users to provide more and more location data (inadvertently or out of frustration).

1. <u>Dark Patterns in Google Account Settings</u>

- 97. 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 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 users about the extent of its location tracking, but also made it difficult for users to opt out of this tracking.
- 98. Google also uses dark patterns in "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 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*:

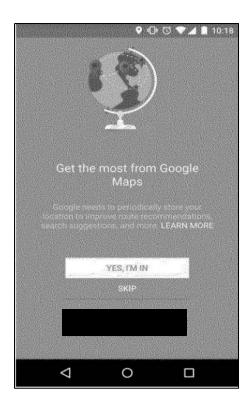


Fig 4 ("Get the most from Google Maps[:] Google needs to periodocally store your location to improve route recommendations, search suggestions, and more.")

- 99. However, these products could properly function without users agreeing to constant tracking. For example, Maps and Google Now did not "need" Location History in order to perform its 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 were not free to decline Google Account settings if they wished to use certain (often preinstalled) Google products as they were intended, users were left with effectively no choice but to enable these settings.
- 100. 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. In other words, users could only opt in or out of these settings collectively at set-up of the Google product. *See:*

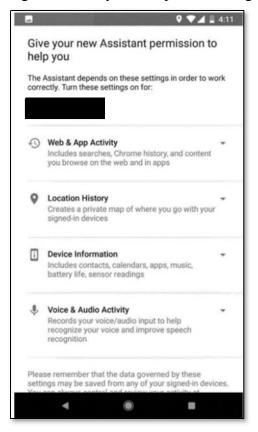
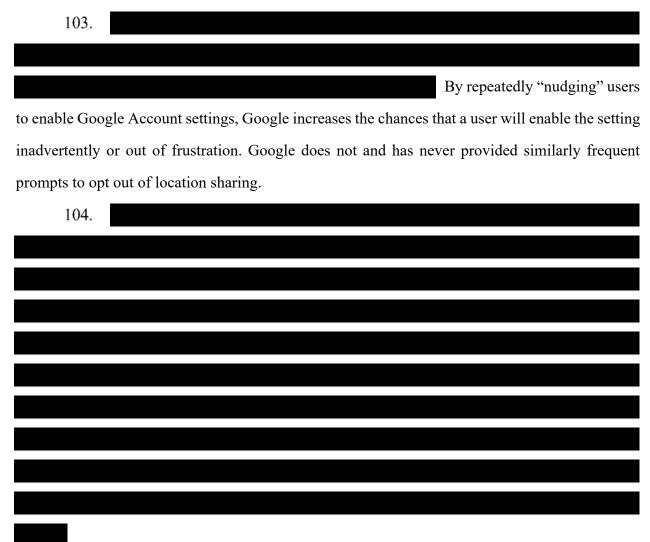


Fig. 5 ("Give your new Assistant permission to help you[.] The Assistant depends on these setting in order to work correctly. Turn these setting on for: . . . Web & App Activity[:] Includes searches, Chrome history, and content you browse on the web and in apps[;] Location History[:] Creates a private map of where you go with your signed-in devices.")

- 101. 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.
- 102. Google also did not (and still does not) give users 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.



Account settings were provided only vague and imbalanced information about the consequences of enabling Google Account settings, unless users clicked on links that led to further information. 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 users would likely never see. *See*:

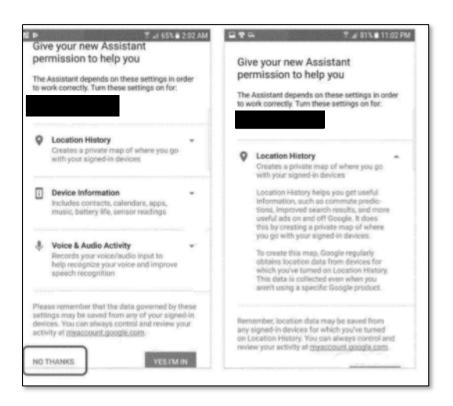
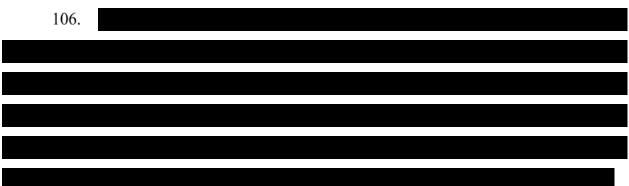


Fig. 6 ("Location History[:] Creates a private map of where you go with your sign-in devices[.] Location History helps you get useful information such as commute predictions, improved search results and more useful ads on and off Google.")



107. 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 falsely implied that Google products would not function unless the user agreed to provide location data on a continuous basis.

2. <u>Dark Patterns in Device Settings</u>

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

- 109. 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.
- 110. 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, 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,
111.

112. 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:



Fig. 7 (Old Version – "Use location? This app wants to change your device setting: Use GPS, Wi-Fi, and cell networks for location. Use Google's location service, sending anonymous location to Google even when no apps are running." New Version – "For best results, let your device turn on location, which uses Google's location service.")

113.

114. 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 has a substantially reduced ability to ascertain, extract, and monetize the locations of its users.

F. Google Engages in Deceptive and Unfair Trade Practices in the District.

115. Google's deceptive and unfair acts and practices alleged herein occurred in trade or commerce in the District. Google offers, sells, provides, and advertises its devices, software products, and services to District consumers. Consumers purchase Google's products with the deceptive settings in the District. Through its ad business, Google receives advertising revenue based on the District consumer location data that it collects through the unfair and deceptive acts and practices discussed herein.

CAUSES OF ACTION

Count One

Misrepresentations and Omissions in Violation of the Consumer Protection Procedures Act

- 116. The District re-alleges and incorporates the other allegations of this Complaint as if set forth fully herein.
- 117. The CPPA is a remedial statute that is to be broadly construed. It establishes an enforceable right to truthful information from merchants about consumer goods and services that are or would be purchased, leased, or received in the District.
- 118. Google, in the ordinary course of business, offers, sells, and supplies consumer goods and services and, therefore, is a merchant under the CPPA.
- 119. Google users receive consumer goods and services in the form of products and services from Google and are therefore consumers under the CPPA.
- 120. The CPPA prohibits unfair and deceptive trade practices in connection with the offer, sale, and supply of consumer goods and services.
- 121. By engaging in the acts and practices alleged herein, Google made or caused to be made to District consumers, directly or indirectly, explicitly or by implication, misrepresentations as to material facts which had a tendency to mislead consumers, in violation of D.C. Code § 28-3904(e). Google's misrepresentations include, but are not limited to, the following:
 - a. That consumers could prevent Google from retaining and using their location information by disabling (*i.e.*, turning off) the Location History setting;

- That consumers could prevent Google from 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).
- 122. By engaging in the acts and practices alleged herein, Google failed to state material facts and/or used innuendo or ambiguity as to material facts, which had a tendency to mislead District consumers, in violation of D.C. Code §§ 28-3904(f) and (f-1). Google failed to state and/or used innuendo or ambiguity regarding at least the following facts:
 - 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 through the Web & App Activity setting, which was defaulted "on" at set up;
 - c. That consumers could not prevent Google from retaining and using consumers' location information by adjusting Google Account settings;
 - 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 consumers' location information even when the consumer's "master" device location setting is disabled;

- f. That Google apps obtains a consumer's location information from other sources available to Google,

 even when consumers deny those apps permission to access location data; and
- 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.
- 123. Google's unlawful acts and practices in violation of the CPPA targeted and affected District residents.
- 124. Google's violations present a continuing harm and the unlawful acts and practices complained of here affect the public interest.
- 125. Google's actions to date have failed to fully address the misleading and deceptive nature of its business activities and the Company continues to engage in acts prohibited by CPPA.

Count Two

Unfair Trade Practices in Violation of the Consumer Protection Procedures Act

- 126. The State re-alleges and incorporates the other allegations of this Complaint as if set forth fully herein.
- 127. The CPPA is a remedial statute that is to be broadly construed. It establishes an enforceable right to truthful information from merchants about consumer goods and services that are or would be purchased, leased, or received in the District.
 - 128. The CPPA prohibits any person from engaging in unfair trade practices.
- 129. Google has engaged in unfair practices affecting District consumers, in violation of D.C. Code § 28-3904, including by:
 - a. Misleading users regarding location-related settings and collecting, storing, 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, storage, 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 user interfaces that make it difficult for consumers to deny Google access to and use of their location information, including making location-related user controls difficult to find and repeatedly prompting users 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, storage, or use of consumers' location data when a user enabled location-related device settings or Google Account settings.
- 130. These practices harm consumers who wish to protect their sensitive location information from disclosure to Google and Google's advertising customers, by making it difficult for consumers to deny Google access to their location information, regardless of whether that information is needed to provide services to the consumer.
- 131. Google's practices, including its use of dark patterns, causes or is likely to causes substantial injury to consumers, including but not limited to subjecting consumers to pervasive tracking of their location to which consumers did not consent and exposing consumers to targeted advertising to which consumers did not consent.
- 132. These injuries are not reasonably avoidable by consumers themselves, including because Google's misleading and conflicting settings and disclosures make it impossible for consumers to understand when and to what extent they are being tracked. *See infra* ¶¶ 53, 62, 82, 93, 99, 101-103, 109-110.
- 133. The injuries are not outweighed by countervailing benefits to consumers or to competition.
- 134. Google's unlawful acts and practices in violation of the CPPA targeted and affected District residents.

135. Google's violations present a continuing harm and the unlawful acts and practices

complained of here affect the public interest.

136. Google's actions to date have failed to fully address the misleading and deceptive

nature of its business activities and the Company continues to engage in acts prohibited by the

CPPA.

PRAYER FOR RELIEF

WHEREFORE, the District respectfully requests that this Court enter judgment against

Google and in favor of District as follows:

a. Permanently enjoining Google, pursuant to D.C. Code § 28-3909(a), from violating the

CPPA;

b. Order the disgorgement of monies, property, or data (including any algorithms developed

using such data) from Google based on its unlawful conduct and/or ordering Google to pay

damages and restitution;

c. Award civil penalties in an amount to be proven at trial and as authorized per violation of

the CPPA pursuant to D.C. Code § 28-3909(b);

d. Award the District the costs of this action and reasonable attorney's fees pursuant to D.C.

Code § 28-3909(b); and

e. Granting such further relief as the Court deems just and proper.

JURY DEMAND

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

Respectfully submitted,

Dated: January 24, 2022

KARL A. RACINE

Attorney General for the District of Columbia

36

/s/ Kathleen Konopka

KATHLEEN KONOPKA

Deputy Attorney General

Public Advocacy Division

/s/ Jimmy R. Rock

JIMMY R. ROCK [493521]

Acting Deputy Attorney General

Public Advocacy Division

/s/ Benjamin M. Wiseman

BENJAMIN M. WISEMAN [1005442]

Director, Office of Consumer Protection

/s/ Jennifer M. Rimm

JENNIFER M. RIMM [1019209]

Assistant Attorney General

441 4th Street, N.W.

Washington, D.C. 20001

(202) 741-5226 (Phone)

(202) 741-8949 (Fax)

benjamin.wiseman@dc.gov

jennifer.rimm@dc.gov

Attorneys for the District of Columbia

Superior Court of the District of Columbia

CIVIL DIVISION- CIVIL ACTIONS BRANCH

INFORMATION SHEET

District of Columbia	Case Number:		
Vs	Date: January 24, 2022		
Google LLC	One of the defendants is being sued in their official capacity.		
Name: (Please Print) Jennifer M. Rimm	Relationship to Lawsuit		
Firm Name: Office of the Attorney General for the District of Columbia	X Attorney for Plaintiff		
Telephone No.: Six digit Unified Bar No.: 1019209	☐ Self (Pro Se) ☐ Other:		
TYPE OF CASE: Non-Jury 6 Personand: \$_Restitution and civil penalties	on Jury Other: 12 Person Jury Other:		
PENDING CASE(S) RELATED TO THE ACTION BE Case No.: Judge:	EING FILED Calendar #:		
Case No.: Judge:	Calendar#:		
NATURE OF SUIT: (Check One Box Only)			
A. CONTRACTS COLL	ECTION CASES		
□ 01 Breach of Contract □ 14 Under \$25,000 Pltf. Grants Consent □ 16 Under \$25,000 Consent Denied □ 02 Breach of Warranty □ 17 OVER \$25,000 Pltf. Grants Consent □ 18 OVER \$25,000 Consent Denied □ 18 OVER \$25,000 Consent Denied □ 27 Insurance/Subrogation □ 26 Insurance/Subrogation Over \$25,000 Pltf. Grants Consent □ 34 Insurance/Subrogation □ 34 Insurance/Subrogation □ 15 Special Education Fees □ 18 OVER \$25,000 Consent Denied □ 34 Insurance/Subrogation □ 34 Insurance/Subrogation □ 34 Insurance/Subrogation □ 28 Motion to Confirm Arbitration Award (Collection Cases Only)			
B. PROPERTY TORTS			
☐ 01 Automobile ☐ 03 Destruction of Private Property ☐ 05 Trespass ☐ 02 Conversion ☐ 04 Property Damage ☐ 07 Shoplifting, D.C. Code § 27-102 (a)			
C. PERSONAL TORTS			
	nder Not Malpractice) erference 18Wrongful Death (Not Malpractice) osecution 19 Wrongful Eviction Legal 20 Friendly Suit cal (Including Wrongful Death) Not Automobile, 22 Toxic/Mass Torts		

SEE REVERSE SIDE AND CHECK HERE

IF USED

Information Sheet, Continued

C. OTHERS O1 Accounting O2 Att. Before Judgment O5 Ejectment O9 Special Writ/Warrants (DC Code § 11-941) I0 Traffic Adjudication I1 Writ of Replevin I2 Enforce Mechanics Lien I6 Declaratory Judgment	☐ 17 Merit Personnel Act (OEA) (D.C. Code Title 1, Chapter 6) ☐ 18 Product Liability ☐ 24 Application to Confirm, Modify, Vacate Arbitration Award (DC Cod ☐ 29 Merit Personnel Act (OHR) ☐ 31 Housing Code Regulations ☐ 32 Qui Tam ☐ 33 Whistleblower	e § 16-4401)
II. 03 Change of Name 06 Foreign Judgment/Domestic 08 Foreign Judgment/Internation 13 Correction of Birth Certificate 14 Correction of Marriage Certificate 26 Petition for Civil Asset Forfe 27 Petition for Civil Asset Forfe 28 Petition for Civil Asset Forfe	2-1802.03 (h) or 32-151 9 (a)] 20 Master Meter (D.C. Code § 42-3301, et seq.) iture (Vehicle) iture (Currency)	☐ 21 Petition for Subpoena [Rule 28-I (b)] ☐ 22 Release Mechanics Lien ☐ 23 Rule 27(a)(1) (Perpetuate Testimony) ☐ 24 Petition for Structured Settlement ☐ 25 Petition for Liquidation
D. REAL PROPERTY	l Sale 31 Tax Lien Bid Off Certifica	t Denied
grz-	J	anuary 24, 2022
Attorney's Signatur	re	Date



Superior Court of the District of Columbia CIVIL DIVISION

Civil Actions Branch

500 Indiana Avenue, N.W., Suite 5000 Washington, D.C. 20001 Telephone: (202) 879-1133 Website: www.dccourts.gov

Plaintiff vs.	
	Case Number
Defendant	

SUMMONS

To the above named Defendant:

You are hereby summoned and required to serve an Answer to the attached Complaint, either personally or through an attorney, within twenty one (21) days after service of this summons upon you, exclusive of the day of service. If you are being sued as an officer or agency of the United States Government or the District of Columbia Government, you have sixty (60) days after service of this summons to serve your Answer. A copy of the Answer must be mailed to the attorney for the plaintiff who is suing you. The attorney's name and address appear below. If plaintiff has no attorney, a copy of the Answer must be mailed to the plaintiff at the address stated on this Summons.

You are also required to file the original Answer with the Court in Suite 5000 at 500 Indiana Avenue, N.W., between 8:30 a.m. and 5:00 p.m., Mondays through Fridays or between 9:00 a.m. and 12:00 noon on Saturdays. You may file the original Answer with the Court either before you serve a copy of the Answer on the plaintiff or within seven (7) days after you have served the plaintiff. If you fail to file an Answer, judgment by default may be entered against you for the relief demanded in the complaint.

Name of Plaintiff's Attorney	_ Clerk of the Court
•	Ву
Address	Deputy Clerk
Telephone	
	r au (202) 879-4828 pour une traduction Để có một bài dịch, hãy gọi (202) 879-4828

IMPORTANT: IF YOU FAIL TO FILE AN ANSWER WITHIN THE TIME STATED ABOVE, OR IF, AFTER YOU ANSWER, YOU FAIL TO APPEAR AT ANY TIME THE COURT NOTIFIES YOU TO DO SO, A JUDGMENT BY DEFAULT MAY BE ENTERED AGAINST YOU FOR THE MONEY DAMAGES OR OTHER RELIEF DEMANDED IN THE COMPLAINT. IF THIS OCCURS, YOUR WAGES MAY BE ATTACHED OR WITHHELD OR PERSONAL PROPERTY OR REAL ESTATE YOU OWN MAY BE TAKEN AND SOLD TO PAY THE JUDGMENT. IF YOU INTEND TO OPPOSE THIS ACTION, DO NOT FAIL TO ANSWER WITHIN THE REQUIRED TIME.

If you wish to talk to a lawyer and feel that you cannot afford to pay a fee to a lawyer, promptly contact one of the offices of the Legal Aid Society (202-628-1161) or the Neighborhood Legal Services (202-279-5100) for help or come to Suite 5000 at 500 Indiana Avenue, N.W., for more information concerning places where you may ask for such help.

> See reverse side for Spanish translation Vea al dorso la traducción al español

CV-3110 [Rev. June 2017] Super. Ct. Civ. R. 4





TRIBUNAL SUPERIOR DEL DISTRITO DE COLUMBIA DIVISIÓN CIVIL

Sección de Acciones Civiles

500 Indiana Avenue, N.W., Suite 5000, Washington, D.C. 20001 Teléfono: (202) 879-1133 Sitio web: www.dccourts.gov

	Demandante	
contra		
	Número de Caso:	
	Demandado	
	CITATORIO	
Al susodicho Demandado:		
persona o por medio de un abogado, en el p citatorio, excluyendo el día mismo de la en agente del Gobierno de los Estados Unido sesenta (60) días, contados después que us enviarle por correo una copia de su Conta	ser y se le require entregar una Contestación a la Demanda a plazo de veintiún (21) días contados después que usted hay rega del citatorio. Si usted está siendo demandado en calida de Norteamérica o del Gobierno del Distrito de Columb ed haya recibido este citatorio, para entregar su Contestacion al abogado de la parte demandante. El nombre y o Si el demandado no tiene abogado, tiene que enviarle al desción que aparaga en esta Citatorio.	a recibido este ad de oficial o via, tiene usted ión. Tiene que dirección del
A usted también se le require prese Indiana Avenue, N.W., entre las 8:30 a.m. y los sábados. Usted puede presentar la Co demandante una copia de la Contestación o usted incumple con presentar una Contesta efectivo el desagravio que se busca en la den	ntar la Contestación original al Tribunal en la Oficina 500 5:00 p.m., de lunes a viernes o entre las 9:00 a.m. y las 12:0 ntestación original ante el Juez ya sea antes que usted en el plazo de siete (7) días de haberle hecho la entrega al ción, podría dictarse un fallo en rebeldía contra usted par	0 del mediodía le entregue al demandante. Si
A usted también se le require prese Indiana Avenue, N.W., entre las 8:30 a.m. y los sábados. Usted puede presentar la Co demandante una copia de la Contestación o usted incumple con presentar una Contesta efectivo el desagravio que se busca en la den	ntar la Contestación original al Tribunal en la Oficina 500 5:00 p.m., de lunes a viernes o entre las 9:00 a.m. y las 12:0 ntestación original ante el Juez ya sea antes que usted en el plazo de siete (7) días de haberle hecho la entrega al ción, podría dictarse un fallo en rebeldía contra usted paranda.	0 del mediodía le entregue al demandante. Si
A usted también se le require prese Indiana Avenue, N.W., entre las 8:30 a.m. y los sábados. Usted puede presentar la Co demandante una copia de la Contestación o usted incumple con presentar una Contesta efectivo el desagravio que se busca en la den	ntar la Contestación original al Tribunal en la Oficina 500 5:00 p.m., de lunes a viernes o entre las 9:00 a.m. y las 12:0 ntestación original ante el Juez ya sea antes que usted en el plazo de siete (7) días de haberle hecho la entrega al ción, podría dictarse un fallo en rebeldía contra usted par nanda. SECRETARIO DEL TRIBUNAL	0 del mediodía le entregue al demandante. Si
A usted también se le require prese Indiana Avenue, N.W., entre las 8:30 a.m. y los sábados. Usted puede presentar la Co demandante una copia de la Contestación o usted incumple con presentar una Contesta efectivo el desagravio que se busca en la den Nombre del abogado del Demandante	ntar la Contestación original al Tribunal en la Oficina 500 5:00 p.m., de lunes a viernes o entre las 9:00 a.m. y las 12:0 ntestación original ante el Juez ya sea antes que usted en el plazo de siete (7) días de haberle hecho la entrega al ción, podría dictarse un fallo en rebeldía contra usted paranda.	0 del mediodía le entregue al demandante. Si
A usted también se le require prese Indiana Avenue, N.W., entre las 8:30 a.m. y los sábados. Usted puede presentar la Co demandante una copia de la Contestación o usted incumple con presentar una Contesta efectivo el desagravio que se busca en la den Nombre del abogado del Demandante	ntar la Contestación original al Tribunal en la Oficina 500 5:00 p.m., de lunes a viernes o entre las 9:00 a.m. y las 12:0 ntestación original ante el Juez ya sea antes que usted en el plazo de siete (7) días de haberle hecho la entrega al ción, podría dictarse un fallo en rebeldía contra usted par nanda. SECRETARIO DEL TRIBUNAL Por:	0 del mediodía le entregue al demandante. Si
A usted también se le require prese Indiana Avenue, N.W., entre las 8:30 a.m. y los sábados. Usted puede presentar la Co demandante una copia de la Contestación o usted incumple con presentar una Contesta	ntar la Contestación original al Tribunal en la Oficina 500 5:00 p.m., de lunes a viernes o entre las 9:00 a.m. y las 12:0 ntestación original ante el Juez ya sea antes que usted en el plazo de siete (7) días de haberle hecho la entrega al ción, podría dictarse un fallo en rebeldía contra usted par nanda. SECRETARIO DEL TRIBUNAL Por:	0 del mediodía le entregue al demandante. Si

IMPORTANTE: SI USTED INCUMPLE CON PRESENTAR UNA CONTESTACIÓN EN EL PLAZO ANTES MENCIONADO O, SI LUEGO DE CONTESTAR, USTED NO COMPARECE CUANDO LE AVISE EL JUZGADO, PODRÍA DICTARSE UN FALLO EN REBELDÍA CONTRA USTED PARA QUE SE LE COBRE LOS DAÑOS Y PERJUICIOS U OTRO DESAGRAVIO QUE SE BUSQUE EN LA DEMANDA. SI ESTO OCURRE, PODRÍA RETENÉRSELE SUS INGRESOS, O PODRÍA TOMÁRSELE SUS BIENES PERSONALES O BIENES RAÍCES Y SER VENDIDOS PARA PAGAR EL FALLO. SI USTED PRETENDE OPONERSE A ESTA ACCIÓN, NO DEJE DE CONTESTAR LA DEMANDA DENTRO DEL PLAZO EXIGIDO.

Si desea conversar con un abogado y le parece que no puede pagarle a uno, llame pronto a una de nuestras oficinas del Legal Aid Society (202-628-1161) o el Neighborhood Legal Services (202-279-5100) para pedir ayuda o venga a la Oficina 5000 del 500 Indiana Avenue, N.W., para informarse sobre otros lugares donde puede pedirayuda al respecto.

> Vea al dorso el original en inglés See reverse side for English original

CV-3110 [Rev. June 2017] Super. Ct. Civ. R. 4