UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Lina M. Khan, Chair**
Rebecca Kelly Slaughter
Alvaro M. Bedoya
Melissa Holyoak
Andrew Ferguson

In the Matter of

MOBILEWALLA, INC., a corporation,

DOCKET NO.

COMPLAINT

The Federal Trade Commission, having reason to believe that Mobilewalla, Inc., a corporation,") has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Mobilewalla, Inc. ("Mobilewalla") is a Delaware corporation with its principal office or place of business at 5170 Peachtree Road, Bldg 100, Suite 100, Chamblee, Georgia 30341.

2. The acts and practices of Respondent alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

Respondent's Business Practices

3. Mobilewalla is a data broker that collects and aggregates huge quantities of consumer information, including precise location information tied to individual consumers that reveals sensitive information about those consumers. Mobilewalla touts its ability, among other things, to "create a comprehensive, cross channel view of the customer, understanding online and offline behavior."

4. Mobilewalla does not collect location data or other personal information directly from consumers. Rather, Mobilewalla obtains consumer location data and other personal information from data suppliers. Indeed, consumers generally have no interactions with Mobilewalla and, in most circumstances, have no idea that Mobilewalla has obtained their data.

5. Mobilewalla also licenses consumer "audience segments" tied to a device's mobile advertising identifier ("MAID") for use by third parties. Mobilewalla analyzes the location data

it obtains and, based on the locations and events visited by consumers' mobile devices, categorizes MAIDs into "audience segments" based on interests or characteristics purportedly revealed by the locations or events. Mobilewalla has offered standard audience segments such as "Music Lovers" but has also created custom audience segments for clients, such as an audience segment specifically targeting pregnant women and young mothers.

6. Mobilewalla's products are used for a variety of purposes including advertising, political campaigning, and government purposes. Mobilewalla has also used its products to attempt to track union organizers.

Respondent Collects and Sells Massive Amounts of Personal Data

7. Mobilewalla has collected large swaths of consumers' personal information, including location data, from multiple sources including real-time bidding exchanges and data brokers. These sources may themselves obtain consumer data from other data suppliers, the mobile or online advertising marketplace, or mobile applications.

8. Mobilewalla has collected consumers' personal information from two sources: (i) real-time bidding exchanges and (ii) data brokers and data aggregators.

9. Mobilewalla's products and services have relied primarily on consumer information that Mobilewalla collected from real-time bidding exchanges ("RTB exchanges"). The primary purpose of RTB exchanges is to enable instantaneous delivery of advertisements and other content to consumers' mobile devices, such as when scrolling through a webpage or using an app. An app or website implements a software development kit, cookie, or similar technology that collects the consumer's personal information from their device and passes it along to the RTB exchange in the form of a bid request. In an auction that occurs in a fraction of a second and without consumers' involvement, advertisers participating in the RTB exchange bid to place advertisements based on the consumer information contained in the bid request. Advertisers can see and collect the consumer information contained in the bid request (even when they do not have a winning bid) and successfully place the advertisement.

10. When Mobilewalla bid to place an advertisement for its clients through an RTB exchange, it collected and retained the information contained in the bid request, even when it did not have a winning bid, and even though the terms of the RTB exchanges disallowed such collection and retention. Among other information, a bid request contains a consumer's device MAID and precise geolocation information, if the consumer had location sharing turned on.

11. Mobilewalla has estimated that approximately 60% of its consumer data came from RTB exchanges between January 1, 2018, and June 30, 2020.

12. During this period, Mobilewalla estimates that it collected approximately 77 million unique advertising identifiers paired with location information in 2018, over 273 million unique advertising identifiers paired with location information in 2019, and approximately 269 million unique advertising identifiers paired with location information in 2020.

13. Over this same period, Mobilewalla also collected MAIDs that were not paired with location information, but were associated with other consumer data, such as the name of the app sending the bid request to the RTB exchange. Mobilewalla uses this information to build out its data profiles for those unique advertising identifiers.

14. In total, Mobilewalla estimates that it collected more than 2 billion unique advertising identifiers over this period.

15. Additionally, Mobilewalla obtained MAIDs paired with location information for more than 183 million devices in 2021 and over 10 million devices in the first four months of 2022, until news outlets exposed its business practices.

16. By collecting data in this manner, Mobilewalla has amassed immense volumes of sensitive consumer information, including precise latitude and longitude coordinates of the consumer's device along with a timestamp and the device's unique advertising identifier, which allows Mobilewalla to link the consumer information collected through different RTB exchanges and other means.

17. In addition to the location and other consumer information that Mobilewalla collected through RTB exchanges, Mobilewalla purchases consumer information from data brokers and other companies that aggregate consumer information collected through various apps and websites. These third parties transfer data directly to Mobilewalla, including MAIDs paired with precise geolocation information, the name of the app through which the device identifier was collected, and other consumer information. For example, Mobilewalla has purchased consumers' phone numbers in clear text associated with the advertising identifier as well as hashed phone numbers and hashed e-mail addresses associated with MAIDs. Data is hashed by converting the data into a sequence of letters and numbers through a cryptographic tool.

18. Mobilewalla sells access to this data in various ways, including raw location data and audience segments.

Respondent Sells Raw Location Data That Can
Identify Individuals and Track Them to Sensitive Locations

19. Mobilewalla licenses to third parties raw location data tied to MAIDs. These third parties include advertisers, data brokers, analytics firms, and other companies. These third parties can then analyze and use the data for their own purposes, such as advertising or brand analytics, or to provide access to the information for their own customers.

20. Mobilewalla's raw location data is not anonymized. Typically, Mobilewalla's raw location data includes a MAID, the latitude, longitude, and a timestamp of the location. This raw location data can be used to identify an individual consumer and match an individual consumer's mobile device with the locations they visited.

21. MAIDs can be and are used to identify a mobile device's user or owner. For example, some data brokers advertise services to match MAIDs with "offline" information, such as consumers' names and physical addresses. Indeed, in a March 2020 email, a Mobilewalla's

chief executive officer explained that Mobilewalla's ability to identify consumers' home addresses using a consumer's mobile device location history is more accurate than Mobilewalla's competitors because of "our ability to store longer periods of data cheaply due to compression schemes we have developed in house."

22. Even without using data to connect a MAID to a consumer's name, email address, phone number, or other identifying information, the MAID associated with precise geolocation data that tracks consumers' movements over time can be and is used to identify consumers and sensitive information about them. MAIDs are assigned by a mobile device's operating system to allow companies to track a consumer's mobile activity and are used to send targeted advertisements. Indeed, targeting individual consumers is the MAIDs' primary purpose.

23. The geolocation data is quite precise. Mobilewalla asserts they can target geolocation to a radius as small as 25 meters.

24. Mobilewalla does not have any policies or procedures in place to remove sensitive locations from the raw location data sets they sell. The data can, therefore, be used to identify the sensitive locations that individual consumers have visited.

25. Mobilewalla's location data associated with MAIDs can be used to track consumers to sensitive locations, including medical facilities, places of religious worship, places that offer services to the LGBTQ+ community, domestic abuse shelters, and welfare and homeless shelters. It can also be used to infer sensitive information about those consumers. For example, by plotting the latitude and longitude coordinates included in the Mobilewalla data stream using publicly-available map programs or land parcel data Mobilewalla purchases, it is possible to identify which consumers' mobile devices visited specific medical facilities that specialize in treating specific medical conditions, and infer from that data that the consumer has that condition. Further, because each set of coordinates in Mobilewalla's data is time-stamped, it is also possible to identify when a mobile device visited the location.

26. Mobilewalla's collection and sale of consumers' precise geolocation data to its clients to identify and target consumers based on sensitive characteristics causes or is likely to cause substantial injury in the form of stigma, discrimination, physical violence, emotional distress, and other harms.

Respondent's Audience Segments Target Consumers Based on Sensitive Characteristics

27. Using the personal information that Mobilewalla collects from consumers, Respondent categorizes consumers into numerous audience segments to, among other things, allow its clients to target consumers for advertising. Mobilewalla develops standard audience segments, such as "Young Mothers," that Mobilewalla sells its clients and Mobilewalla also creates custom audience segments based on specific criteria that its clients request. Mobilewalla does not place any restrictions on the characteristics it uses to create audience segments.

28. Custom audience segments have been based on sensitive consumer information. For example, Mobilewalla has helped its clients target pregnant women, Hispanic churchgoers, and members of the LGBTQ+ community.

29. Mobilewalla's audience segments, including the ones that identify consumers based on sensitive characteristics, are also associated with MAIDs. As alleged in paragraphs 19 to 22 above, Mobilewalla connects such MAIDs to individual consumers. Thus, Mobilewalla sells data products that its clients use to associate individual consumers with health conditions, gender identity and sexual orientation, political activity, and religious practices, among other sensitive characteristics, which puts individuals at significant risk of stigma, discrimination, physical violence, emotional distress, and other harms.

30. Mobilewalla has created geo-fences around pregnancy centers and maternity clinics and searched through its vast amounts of location information to determine which consumer devices visited those healthcare centers in order to build its audience segments of pregnant women and expectant families.

31. Mobilewalla has used consumers' precise location information to determine sensitive political and religious characteristics of these consumers. For example, Mobilewalla has created retroactive geo-fences around the sites of political rallies or protests to create audience segments of the consumers that attended those rallies or protests. On other occasions, Mobilewalla has created geo-fences around polling places and state capitols to identify devices belonging to consumers who visited those locations, often identifying the home addresses for consumers found within the geo-fence by tracking where the individual spends the evening.

32. Additionally, Mobilewalla used such an audience segment to publish a report in June 2020 that analyzed individuals who protested the death of George Floyd; this report published aggregated findings about whether protestors were from the cities in which they protested and the racial and gender demographics of the protestors. To help determine the racial demographics of the protestors, Mobilewalla retroactively geo-fenced the places of worship that an individual had previously visited because, as a Mobilewalla employee explained in an internal email, "Hindu temples indicate you are highly likely to be Hindu/Indian, African-American churches indicate you are likely black etc."

Respondent Collected Consumers' Information from RTB Exchanges and Used it for Non-Advertising Purposes

33. As described in paragraphs 9 to 16 above, Mobilewalla amassed immense volumes of consumer information from RTB exchanges by collecting and retaining the information contained in a bid request. The information contained in a bid request included the consumer's device MAID, a timestamp, the name of the app or website in which the consumer will see the advertisement, the consumer's device manufacturer, and the consumer's precise geolocation information if the consumer had location sharing turned on.

34. Mobilewalla collected and retained the information contained in the bid request and used it for non-advertising purposes, even when Mobilewalla did not have a winning bid, and even

though the terms of the RTB exchanges disallowed such collection and retention. Indeed, the RTB exchanges prohibited non-advertising uses of consumer data.

35. Among the non-advertising uses of consumers' information, Mobilewalla created a "geo-fence" around the home addresses of a set of employees and certain healthcare centers, in order for the client to "poach these nurses from these centers to a competitor." Mobilewalla has also experimented with other non-advertising uses of consumers' information, such as attempting to geo-fence a work location to track where union organizers travel.

36. Additionally, Mobilewalla has transferred consumers' information, including precise geolocation information along with timestamps and unique device advertising identifiers, the type or brand of device that a specific consumer used, and IP addresses for government purposes.

37. On multiple occasions, Mobilewalla retroactively geo-fenced distinct locations and collected and transferred consumers' information for devices found in the geo-fence during that period of time. On one occasion a client provided Mobilewalla with MAIDs for devices of interest. Mobilewalla then searched its database of consumer information and transferred sensitive information about the devices, including thousands of latitude and longitude coordinates of where the consumer had traveled, the IP addresses associated with the signals, the city, state, and ZIP code associated with the locations, the timestamp of when the device was seen at each location, and the devices' MAIDs. Respondent also transferred the name of the app from which each location signal originated, which included "Grindr iOS," "Jack'd – Gay Chat & Dating," and "My Mixtapez iOS."

Respondent Fails to Take Reasonable Steps to Confirm with Other Data Suppliers that Consumers Consented to Respondent's Collection and Use of Their Information

38. As described in paragraph 17, Mobilewalla also collects consumer information from data brokers and data aggregators.

39. Mobilewalla does not obtain consent directly from consumers. Instead, Mobilewalla relies on its suppliers to obtain consumer consent.

40. However, Mobilewalla does not know whether consumers were informed of or consented to Mobilewalla's collection and use of their information.

41. Mobilewalla does not contractually require its suppliers to obtain consumer consent. Typically, Mobilewalla has merely relied on vague contractual assurances that the suppliers' sale of consumers' information complied with applicable law.

42. Additionally, Mobilewalla fails to take reasonable steps to verify that its suppliers have obtained consumer consent. For example, although in 2020 Mobilewalla began requiring its suppliers to certify annually that they had consumers' consent to collect and transfer their information, Mobilewalla failed to implement any procedures to verify the accuracy of these certifications such as requesting and reviewing consumer notices.

43. In many instances, Mobilewalla has failed to review examples of notices used by the data suppliers to purportedly collect consent or request and review evidence from the suppliers demonstrating that consumers have consented. When Mobilewalla evaluates a new data supplier, Mobilewalla has asked the supplier to complete a questionnaire about the supplier's data collection practices and submit a list of the apps from which the supplier collects consumers' information.

44. Although some suppliers collect consumers' information from thousands of apps, Mobilewalla has typically only checked whether three to five of the apps disclosed to consumers that the app was collecting location information and sharing it with third parties. In addition, Mobilewalla has only checked these apps *once*, when evaluating whether to sign a contract with a new supplier. Even though app disclosures regularly change over time, Mobilewalla has not subsequently or periodically checked whether any of these apps continued to disclose that they collected location data and shared it with third parties.

45. Internal communications demonstrate that Mobilewalla has made little to no effort to verify whether its suppliers have obtained informed consumer consent to collect and share consumers' information with Mobilewalla in particular. During initial contract negotiations, one client reviewed disclosures made by some apps from which Mobilewalla collected consumers' information and noted deficiencies, such as an app not listing Mobilewalla as a potential recipient of consumers' information. The client requested that Mobilewalla tell the app to fix the issue. In an email, a Mobilewalla employee wrote that if, for U.S. consumers, the client wanted "specific consents…. This deal is dead." Mobilewalla ultimately did not consummate the deal with this potential client, and also failed to cease using the information or follow up with its supplier who provided consumers' information from that app.

46. Moreover, Mobilewalla's minimal review of consumer disclosures is insufficient to verify that consumers consent to the various purposes that Mobilewalla uses consumer data, as described in paragraphs 35 through 37 above, including marketing, commercial, and government purposes.

47. These facts would be material to consumers in deciding whether to use or grant location permissions to mobile apps and whether to opt out of Mobilewalla's collection of their information. Consumers have expressed concern about the amount of personal information various entities - like advertisers, data aggregators, employers, or law enforcement - know about them and about how such entities use their personal data. Consumers are increasingly reluctant to share their personal information, such as digital activity, emails, text messages, and phone calls, especially without knowing which entities will receive it. Such collection and use impose an unwarranted invasion into consumers' privacy.

Respondent Retains Consumers' Location Information Indefinitely

48. After collecting sensitive precise location data about consumers' daily movements, as well as timestamps and MAIDs, Mobilewalla retains the sensitive consumer information for an indefinite period of time. Mobilewalla touts that it collects over "50B Mobile Signals Daily" from "2.2B Devices" for "40+ Countries" and store "5+ Years of Data."

49. In fact, Mobilewalla has created a vast repository of consumer location information that enables Mobilewalla and its clients to track consumers' movements and, by virtue of knowing where the consumers traveled, to infer other sensitive information about consumers over years. Such vast amounts of data about identifiable individual consumers makes them vulnerable to significant harms, including stalking, targeted scams, and a variety of reputational harms.

50. For example, using Mobilewalla's data, a client proposed to geo-fence the homes of individuals relevant to a private lawsuit and track where those individuals had traveled over the preceding two years, including whether they visited federal law enforcement offices. Additionally, Mobilewalla has marketed its ability to determine whether a consumer attended any political rallies in the last five years. Respondent has even begun to collect and store indefinitely clear text phone numbers and hashed phone numbers and email addresses, paired with MAIDs, which could be used to identify the name of the consumer associated with the sensitive location data.

51. Mobilewalla often touted its long-term retention of consumer location information. For example, in a March 2020 email, a Mobilewalla employee explained that Mobilewalla's ability to identify consumers' home addresses using a consumer's mobile device location history is more accurate because of "our ability to store longer periods of data cheaply due to compression schemes we have developed in house."

Respondent's Practices Cause and Are Likely to Cause Substantial Injury to Consumers

52. As described above, the data sold by Mobilewalla can be used to identify individual consumers and their visits to sensitive locations, such as visits to houses of worship, political protests, and doctors' offices. The sale of such data poses an unwarranted intrusion into the most private areas of consumers' lives and causes or is likely to cause substantial injury to consumers.

53. For example, location data can be used to track individual consumers to places of worship, and thus reveal their religious beliefs and practices. In fact, Mobilewalla sold location data collected from houses of worship and have used such data to infer the race of the individual. Using this location data, it is possible to identify where individual consumers lived, worked, and worshipped, thus suggesting the mobile device user's religion and routine and identifying the user's friends and families. This data can then be used to identify and target consumers based on their religion.

54. In fact, targeting and harm based on precise geolocation collected from mobile devices has and does occur. In one well-publicized example, a group used precise mobile geolocation data to identify by name a Catholic priest who visited LGBTQ+-associated locations, thereby exposing the priest's sexual preferences and forcing him to resign his position.

55. As another example, the location data can be used to track individual consumers who have visited women's reproductive health clinics and as a result, may have had or contemplated sensitive medical procedures such as an abortion or in vitro fertilization. In fact, Mobilewalla has created geo-fences around pregnancy centers and maternity clinics to build its audience

segments of pregnant women and expectant families. Using the data Mobilewalla provide, it is possible for third parties to target individual consumers visiting such healthcare facilities and trace that mobile device to a single-family residence. This data can then be used to identify and target consumers seeking reproductive healthcare.

56. Such targeting and harm occur in the data marketplace. For example, the Massachusetts Attorney General brought a law enforcement action in 2018 against a data broker that sent targeted advertisements about abortion and alternatives to abortion to "abortion-minded women." The "abortion-minded women" audience segment was identified as consumers who, according to their precise geolocation, were "close to or entered the waiting rooms of women's reproductive health clinics."

57. As another example, another group advertised the ability to reach "abortion-vulnerable women" by capturing "the cell phone IDs [i.e. MAIDs] of women coming and going from Planned Parenthood and similar locations and then serve them life-affirming ads" online, including on their Facebook, Instagram, and other social media feeds. According to news reports, one such ad read, "Took the first pill at the clinic? It may not be too late to save your pregnancy." According to reports, the ads pointed consumers who had visited those locations to websites that attempted to persuade consumers to attempt a scientifically unsupported "abortion reversal" procedure. The group further alarmingly asserted on its website that its product "takes the guesswork out of the marketing equation" because its customers will "no longer have to wonder if women can find *you.* Now, you'll find *them*!" Those ads served by the group were seen 14.3 million times.

58. Identification of sensitive and private characteristics of individual consumers from the location data sold by Mobilewalla is an invasion of consumers' privacy and injures or is likely to injure consumers through loss of privacy, exposure to discrimination, physical violence, emotional distress, and other harms.

59. Additionally, the use of location data to categorize consumers based on sensitive characteristics also causes or is likely to cause substantial injury. Such categorizations, particularly by companies that consumers never directly interact with, are far outside the expectations and experience of consumers, and can result in and cause additional injuries to consumers, including by exposing them to risks of discriminatory treatment.

60. Mobilewalla's practice of indefinitely retaining consumers' location information also increases the likelihood that consumers could suffer substantial injury through, for example, a cybersecurity intrusion by an outside bad actor or other unauthorized access. It also exposes consumers to greater risk of stalking, targeted scams, and reputational harm.

61. The collection and use of data collected from their mobile devices and other sources are opaque to consumers, who typically do not know who has collected their data or how it is being used. To the extent that consumers are even given a chance to opt in to a particular collection of information, such opt-in processes typically do not explain to the consumer that Mobilewalla will receive the data, use it to classify the consumer based on sensitive characteristics, and disclose such information to additional third parties unknown to the consumer.

62. Indeed, once information is collected about consumers from their mobile devices or other sources, the information can be, and in many instances, is provided multiple times to companies that consumers have never heard of or interacted with. Consumers have no insight into how this data is used – they do not, for example, typically know or understand the information collected about them can be used to track and map their past movements and that inferences about them and their behaviors will be drawn from this information. Consumers are therefore unable to take reasonable steps to avoid the above-described injuries.

63. These injuries are exacerbated by the fact that Mobilewalla lacks any meaningful controls protecting consumers' privacy. Mobilewalla could implement safeguards to protect consumer privacy, such as blacklisting sensitive locations from its data feeds or removing sensitive characteristics from its data. Such safeguards could be implemented at a reasonable cost and expenditure of resources. However, far from protecting consumers' privacy, Mobilewalla actively promotes its data as a means to evade consumers' privacy choices. Thus, the harms described above are not outweighed by countervailing benefits to consumers or competition.

Violations of the FTC Act

64. Section 5(a) of the FTC Act, 15 U.S.C. §45(a), prohibits "unfair or deceptive acts or practices in or affecting commerce."

65. Acts or practices are unfair under Section 5 of the FTC Act if they cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that are not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

Count I
Unfair Sale of Sensitive Location Information

66. As described in paragraphs 19 to 26 and 29 to 32, Respondent sells, licenses, or otherwise transfers precise location information associated with MAIDs that reveal consumers' visits to sensitive locations, including, among others, locations associated with medical facilities, places of religious worship, places that offer services to the LGBTQ+ community, domestic abuse shelters, and welfare and homeless shelters.

67. This practice has caused or is likely to cause substantial injury to consumers in the form a loss of privacy about the day-to-day movements of millions of consumers, the chilling of consumers' First Amendment rights and an increased risk of public or other harmful disclosure of sensitive information about consumers' private lives, including their fertility choices, religious worship, sexuality, and other such information. This injury is not reasonably avoidable by consumers and is not outweighed by countervailing benefits to consumers or competition. Consequently, Respondent's sale of sensitive information is an unfair act or practice.

Count II
Unfair Targeting Based on Sensitive Characteristics

68. As described in paragraphs 27 to 32, Respondent has targeted consumers into audience segments based on sensitive characteristics, such as medical conditions and religious beliefs, derived from location data. Respondent has sold or transferred these audience segments to third parties for marketing and other purposes, including identifying and targeting consumers who participate in political rallies and protests or attempting to identify and target consumers who participate in union organizing.

69. Respondent's categorization of consumers based on sensitive characteristics derived from location information has caused or is likely to cause substantial injury in the form of loss of privacy for consumers and an increased risk of disclosure of such sensitive information. This injury is not reasonably avoidable by consumers and is not outweighed by countervailing benefits to consumers or competition. Consequently, Respondent's categorization of consumers based on sensitive characteristics for marketing and other purposes is an unfair act or practice.

Count III
Unfair Collection of Consumer Information from RTB Exchanges

70. As described in paragraphs 7 to 16 and 33 to 37, Respondent collected consumers' personal information, including location information, from RTB exchanges, when Respondent had no winning bid.

71. This practice has caused or is likely to cause substantial injury in the form of a loss of privacy about the day-to-day movements of millions of consumers, the chilling of consumers' First Amendment rights and an increased risk of public or other harmful disclosure of sensitive information about consumers' private lives, including their fertility choices, religious worship, sexuality, and other such information. This injury is not reasonably avoidable by consumers and is not outweighed by countervailing benefits to consumers or competition. Consequently, Respondent's collection of consumers' information from RTB exchanges is an unfair act or practice.

Count IV
Unfair Collection and Use of Consumer Location Information Without Consent Verification

72. As described in paragraphs 33 to 47, Respondent collects consumers' location information through the means described in paragraphs 3 to 17 without taking reasonable steps to verify that consumers consent to Respondent's collection and use of their location information.

73. This practice has caused or is likely to cause substantial injury in the form of a loss of privacy about the day-to-day movements of millions of consumers, the chilling of consumers' First Amendment rights and an increased risk of public or other harmful disclosure of sensitive information about consumers' private lives, including their fertility choices, religious worship, sexuality, and other such information. This injury is not reasonably avoidable by consumers and is not outweighed by countervailing benefits to consumers or competition. Consequently, Respondent's collection of consumers' location information is an unfair act or practice.

Count V
Unfair Retention of Consumer Location Information

74. As described in paragraphs 7 to 17 and 48 to 51, Respondent indefinitely retains detailed, sensitive information about consumers' movements, including consumers' location information Respondent has collected from their RTB exchange suppliers and from data brokers.

75. Respondent's indefinite retention of detailed location information has caused or is likely to cause substantial injury in the form of a loss of privacy about the day-to-day movements of millions of consumers, including through the use of retroactive geofences, and an increased risk of disclosure and use of such sensitive information. This injury is not reasonably avoidable by consumers and is not outweighed by countervailing benefits to consumers or competition. Consequently, Respondent's retention of consumers' detailed location information is an unfair act or practice.

Violations of Section 5

76. The acts and practices of Respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this _____ day of _____, 20_, has issued this Complaint against Respondents.

By the Commission, Commissioner Holyoak dissenting.

April J. Tabor
Secretary

SEAL