

**UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION**

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

DOCKET NO. C-4811

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

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.

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.

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 MAIDs associated with those locations.

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 conne(L)1 (c2 (i)-2 (19 t)-2m)-2 (eo)-10 obi cIs thaton pan,ventu-2 (l)-2 (ans)-1 (um)-2 (e)

though the

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, 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.

48. After collecting sensitive precise location data about consumers' daily movements, as well as

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-

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. ~~and 18-1001-FC(17002 Tw)024hyD4d(2)c4 0 Td(o4 0 Td(o4 0 Td411~~

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