BENJAMIN C. MIZER
Principal Deputy Assistant Attorney General
Civil Division
JONATHAN F. OLIN
Deputy Assistant Attorney General
MICHAEL S. BLUME
Director, Consumer Protection Branch
ANDREW E. CLARK
Assistant Director
JACQUELINE BLAESI-FREED
jacqueline.m.blaesi-freed@usdoj.gov
United States Department of Justice
Consumer Protection Branch, Civil Division
P.O. Box 386
Washington, DC 20044
Telephone: (202) 353-2809
Facsimile: (202) 514-8742

Attorneys for United States

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

United States of America, Plaintiff, v. InMobi Pte Ltd., a private limited company, Defendant.	Case No. 3:16-cv-3474 COMPLAINT FOR PERMANENT INJUNCTION, CIVIL PENALTIES AND OTHER RELIEF

Plaintiff, the United States of America, acting upon notification and authorization to the Attorney General by the Federal Trade Commission ("FTC" or "Commission"), for its Complaint alleges that:

1. Plaintiff brings this action under Sections 5(a)(1), 5(m)(1)(A), 13(b), and 16(a) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§ 45(a)(1), 45(m)(1)(A), 53(b), and

56(a), and Sections 1303(c) and 1306(d) of the Children's Online Privacy Protection Act of 1998

13. The "Now" suite allows advertisers to target consumers based on their current location. For example, an advertiser may target consumers when they visit a particular retailer.

14. The "Conditional" suite allows advertisers to target consumers who meet certain conditions, such as visiting a certain location at a particular time of day, or visiting a certain location more than once. For example, an advertiser may target consumers who visit Monday mornings and Thursday evenings.

15. The "Psychographic" suite allows advertisers to target consumers based on their location history for up to the last two months. For example, an advertiser may target consumers who live in affluent neighborhoods and, during the last two-month period, have visited luxury auto dealerships.

ANDROID AND iOS LOCATION SETTINGS

16. The Android and iOS operating systems each provide application developers with application programming interfaces ("APIs") that provide the application with the consumer's current location. In order to access these location APIs, both operating systems require application developers to obtain the consumer's consent through "permissions" – notifications that inform the consumer about the sensitive information (e.g., the consumer's location or contacts) or sensitive device functionality (e.g., the device's camera or microphone) that the application would like to access.

17. On Android 5.1 and earlier versions, the operating system protects the location API through two permissions: Access Coarse Location (accurate up to 2000 meters) and Access Fine Location (accurate up to the precise latitude/longitude coordinates). When installing an application, the consumer is prompted with any location permissions that the application has requested. If the consumer installs the application, the InMobi SDK can access any of the device resources, including location, to which the application has requested access. A consumer may decide not to install an application based on the fact it has requested access to the consumer's coarse or fine location.

18. In addition to these install-time permissions, Android provides the consumer with a system setting to restrict global access to the location API. Through this setting, the consumer

can prevent all applications on the device from accessing the location API. A consumer may decide to restrict access to the location API when, for example, visiting a sensitive location. If the consumer restricts access using this setting, the InMobi SDK would no longer have access to the location API.

19. On iOS, the operating system protects the location API through a permission dialog box that prompts the consumer the first time that an application attempts to access the consumer's location. If the consumer accepts the prompt, the application can then access the consumer's location and pass it to the InMobi SDK. A consumer may decide not to accept the prompt, in which case the application will not have access to the location API.

20. In addition to this run-time permission, iOS provides settings through which the consumer can later restrict access to the location API both on a global and application-by-application basis. A consumer may decide to restrict access to the location API, for example, visiting a sensitive location. If the consumer restricts access using these settings, the InMobi SDK would no longer have access to the location API.

21. When a consumer allows an application to access the location API, Defendant collects the consumer's location in order to serve targeted advertising via the geo-targeting product suites described in Paragraphs 11-12.

DEFENDANT'S USE OF WIFI NETWORK INFORMATION TO GEO-TARGET CONSUMERS

22. Even if the consumer had restricted an application's access to the location API, until December 2015, Defendant still tracked the consumer's location and, in many instances, served geo-targeted ads, by collecting information about the WiFi networks that the consumer's device connected to or that were in range of the consumer's device.

23. On Android, Defendant collects WiFi network information from the device if the application developer has included either of two WiFi-related permissions: Access WiFi State and Change WiFi State. If the application developer included the Access WiFi State permission, Defendant collects information about each network to which the consumer's device connects, including the ESSID (network name), BSSID (a unique identifier), and signal strength. If the

application developer has included the Change WiFi State permission, Defendant collects information about each network that is in range of the consumer's device (whether or not the consumer actually connects to the network), including the BSSID and signal strength. Although Android presents consumers with these WiFi-related permissions during application installation, consumers would have no reason to know that this information would be used to track location.

24. On iOS, Defendant uses an API known as CaptiveNetwork to collect the BSSID for each WiFi network to which a consumer's device connects. According to the iOS developer documentation, the CaptiveNetwork API is intended to allow an application to "assum[e] responsibility for authenticating with [captive] networks," such as those that appear at hotels. Although the InMobi SDK does not facilitate authentication with captive networks, Defendant nonetheless uses the CaptiveNetwork API to collect BSSIDs through any iOS application that integrates the InMobi SDK. iOS does not present a permission dialog box indicating that an application is accessing this API, and the consumer has no means to deny an application access to this information.

25. In any instance where the location API is accessible (i.e., the application developer has included the location permission and the consumer has allowed the application's access to the location API), Defendant simultaneously collects latitude/longitude coordinates alongside the BSSID and other network information described in Paragraphs 22-23. Defendant correlates these two sets of information in order to create its own geocoder database through which it can match specific WiFi networks to specific locations.

26. Until December 2015, even in those instances where the location API was inaccessible (i.e., the application developer had not included the location permission or the consumer had restricted the application's access to the location API), Defendant still collected the WiFi network information described in Paragraphs 22-23, fed the information into its geocoder database, and inferred the consumer's latitude and longitude. Through this method, Defendant could track the consumer's location and serve geo-targeted ads, regardless of the application developer's intent to include geo-targeted ads in the application, and regardless of the consumer's location settings.

27. In response to the Commission's investigation, Defendant modified its location tracking practices at the end of 2015. Defendant released a new version of the InMobi SDK in November 2015 and made additional server-side changes in December 2015. As a result of these modifications, Defendant no longer tracks a consumer's location based on the WiFi network information described in Paragraphs 22-23 unless the Android or iOS location API is accessible to the application integrating the InMobi SDK (i.e., the application developer has included the location permission and the consumer has allowed the application's access to the location API).

DEFENDANT'S REPRESENTATIONS REGARDING GEO-TARGETING

28. Defendant disseminated or caused to be disseminated to Android application developers the following statements in the InMobi SDK integration guide, representing that it tracks the consumer's location and serves geo-targeted ads only if the application developer and

patterns in this location history to identify what these trends mean about the user, from which we can infer what kind of consumer the user is. (Emphasis added.)

35. However, as explained in Paragraphs 22-23, Defendant tracked the consumer's location and served geo-targeted ads even if the consumer had not provided opt-in consent. Defendant collects BSSID and other information related to the WiFi network to which a consumer's device is connected or in range, and used this information to track the consumer's location and serve geo-targeted ads, regardless of whether the consumer had provided opt-in consent.

36. Defendant represented in the disclosures described in paragraphs 28, 30, 32, and 34 that it tracked the consumer's location and served geo-targeted ads only if the application developer and the consumer provided access to the location APIs, and the consumer provided opt-in consent. In fact, Defendant collected and used BSSID and other WiFi network information to track the consumer's location and serve geo-targeted ads regardless of the application developer's intent to include geo-targeted ads, and regardless of the consumer's location settings.

37. As a result, application developers could not provide accurate information to consumers regarding their applications' privacy practices. Indeed, numerous application developers that have integrated the InMobi SDK have represented to consumers in their privacy policies that consumers have the ability to control the collection and use of location information through their applications, including through the device location settings. These application developers had no reason to know that Defendant tracked the consumer's location and served geo-

preferences.

DEFENDANT'S BUSINESS PRACTICES REGARDING COLLECTION OF INFORMATION FROM CHILD-DIRECTED APPLICATIONS

39. For purposes of Paragraphs 39 through 50, and 57 through 65, herein, the terms "child," "collects," "collection," "disclosure," "Internet," "operator," "parent," "personal information," "obtaining verifiable consent," and "Web site or online service directed to children," are defined as those terms are defined in Section 312.2 of the COPPA o.13.43 0 TNS co

application is directed to children. The option – next to an unmarked checkbox – read, "My property is specifically directed to children under 13 years of age and/or I have actual knowledge that it has users known to be under 13 years of age." Since this option became available, thousands of application developers that have integrated the InMobi SDK have indicated to Defendant that their applications are directed to children.

42. Defendant disseminated or caused to be disseminated the following statements regarding the collection of children's personal information through their Privacy Policy:

WHAT ABOUT CHILDREN?

We do not knowingly collect any personal information about children under the age of 13. If we become aware that we have collected personal information about a child under the age of 13, that informacTDo-t w t4(n')3(r)3(m)-1.9(acT(i)-2(ng)1 1(l)-2(c

In response to the new COPPA rules effective on July 1, 2013 InMobi is continuing to ensure that we do not collect and use information from children's sites for behavioral advertising (often referred to as interest based advertising). We will continue to only use any data in the manner that COPPA prescribes. We have identified all existing publisher sites and apps directed to children to ensure we are in full compliance with the new COPPA rules and from 30 June, 2013 shreecoleeSa w

49. Defendant did not obtain verifiable consent from parents prior to collecting and using children's personal information.

50. Defendant knowingly collected and used personal information from thousands of child-directed applications in violation of the COPPA Rule.

DEFENDANT'S VIOLATIONS OF THE FTC ACT

COUNT I

51. Through the means described in Paragraphs 28, 30, and 32, Defendant represented, expressly or by implication, that it tracked the consumer's location and served targeted ads only if the application developer and consumer had provided access to the Android and iOS location APIs.

52. In truth and in fact, as set forth in Paragraphs 22-27, Defendant did not track the consumer's location and serve targeted ads only if the application developer and the consumer had provided access to the Android or iOS location APIs. Instead, Defendant tracked the consumer's location and served targeted ads by collecting BSSID and other information related to the WiFi network to which a consumer's device was connected or in range, even if the consumer had not provided access to the location APIs. Therefore, the representation set forth in Paragraph 51 was false or misleading and constituted a deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT II

53. Through the means described in Paragraph 34, Defendant represented, expressly or by implication, that it tracked the consumer's location and served targeted ads only if the consumer had provided opt-in consent.

54. In truth and in fact, as set forth in Paragraphs 22-27, Defendant did not track the consumer's location and serve targeted ads only if the consumer had provided opt-in consent. Instead, Defendant tracked the consumer's location and served targeted ads by collecting BSSID and other information related to the WiFi network to which a consumer's device was connected or in range, even if the consumer had not provided opt-in consent. Therefore, the representation set forth in Paragraph 53 was false or misleading and constituted a deceptive act

practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT III

55. Through the means described in Paragraphs 42-43, Defendant represented, expressly or by implication, that it did not collect or use personal information from applications directed to children.

56. In truth and in fact, as set forth in Paragraphs 41 and 44-45, Defendant collected and used personal information from applications directed to children. Therefore, the representation set forth in Paragraph 55 was false or misleading and constituted a deceptive act practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

DEFENDANT'S VIOLATION OF THE COPPA RULE

COUNT IV

57. In numerous instances, in connection with operating its mobile advertising network, Defendant collected and used, with actual knowledge, personal information from Web sites or online services directed to children. Pursuant to the COPPA Rule, 16 C.F.R. § 312.2, a Web site or online service shall be deemed directed to children when it has actual knowledge th it is collecting personal information directly from users of another Web site or online service directed to children. Therefore, Defendant has operated a Web site or online service directed to children, and has failed to: (1) provide sufficient notice on its Web site or online services of the information it collects online from children and how it uses such information, among other required content; (2) provide direct notice to parents of the information Defendant collects online from children and how it uses such information, among other required content; and (3) obtain verifiable parental consent before any collection or use of personal information from children.

58. Defendant is an "operator" as defined by the COPPA Rule, 16 C.F.R. § 312.2.

59. Through the means described in Paragraphs 41 through 50 above, Defendant violated:

a. Section 312.4(d) of the Rule, 16 C.F.R. § 312.4(d), which requires an operator to provide sufficient notice on its Web site or online services of the information it collects online from children, how it uses such

information, and its disclosure practices for such information, among other required content;

b. Section 312.4(b) of the Rule, 16 C.F.R. § 312.4(b), which requires an

Dated: June 22, 2016

Respectfully submitted,

FOR THE FEDERAL TRADE COMMISSION:

MANEESHA MITHAL
Associate Director
Division of Privacy and Identity Protection

MARK EICHORN
Assistant Director
Division of Privacy and Identity Protection

NITHAN SANNAPPA
Attorney
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
(202) 326-3185 (voice)
(202) 326-3062 (fax)

JACQUELINE CONNOR
Attorney
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
(202) 326-2844 (voice)
(202) 326-3062 (fax)

FOR PLAINTIFF THE UNITED STATES OF AMERICA:

BENJAMIN C. MIZER
Principal Deputy Assistant Attorney General
Civil Division

JONATHAN F. OLIN
Deputy Assistant Attorney General

MICHAEL S. BLUME
Director
Consumer Protection Branch

ANDREW E. CLARK
Assistant Director

/s/ Jacqueline Blaesi-Freed
JACQUELINE BLAESI-FREED
Trial Attorney
Consumer Protection Branch
U.S. Department of Justice
P.O. Box 386
Washington, DC 20044
(202) 353-2809
jacqueline.m.blaesi-freed@usdoj.gov