

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

11 *Attorneys for United States*

12 UNITED STATES DISTRICT COURT  
 13 NORTHERN DISTRICT OF CALIFORNIA  
 14 SAN FRANCISCO DIVISION  
 15

17 United States of America,  
 18 Plaintiff,  
 19 v.  
 20 InMobi Pte Ltd., a private limited company,  
 21 Defendant.

Case No.: 3:16-cv-3474

**COMPLAINT FOR PERMANENT  
 INJUNCTION, CIVIL PENALTIES  
 AND OTHER RELIEF**

22  
 23  
 24 Plaintiff, the United States of America, acting upon notification and authorization to the  
 25 Attorney General by the Federal Trade Commission (“FTC” or “Commission”), for its Complaint  
 26 alleges that:

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

1 56(a), and Sections 1303(c) and 1306(d) of the Children’s Online Privacy Protection Act of 1998  
2 (“COPPA”), 15 U.S.C. §§ 6502(c) and 6505(d), to obtain monetary civil penalties, a permanent  
3 injunction, and other equitable relief for Defendant’s violations of Section 5 of the FTC Act and  
4 the Commission’s Children’s Online Privacy Protection Rule (“Rule” or “COPPA Rule”), 16  
5 C.F.R. Part 312.

6 **JURISDICTION AND VENUE**

7 2. This Court has subject matter jurisdiction over this matter under 28 U.S.C.  
8 §§ 1331, 1337(a), 1345, and 1355, and under 15 U.S.C. §§ 45(m)(1)(A), 53(b), and 56(a).

9 3. Venue is proper in the Northern District of California under 15 U.S.C. § 53(b) and  
10 28 U.S.C. §§ 1391(b) – (d) and 1395(a).

11 **INTRADISTRICT ASSIGNMENT**

12 4. Defendant markets its products throughout the United States, including throughout  
13 the county of San Francisco. Defendant’s wholly owned United States subsidiary has its primary  
14 place of business in the county of San Francisco.

15 **SECTION FIVE OF THE FTC ACT**

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

18 **THE CHILDREN’S ONLINE PRIVACY PROTECTION ACT RULE**

19 6. Congress enacted COPPA in 1998 to protect the safety and privacy of children  
20 online by prohibiting the unauthorized or unnecessary collection of children’s personal  
21 information online by operators of Internet Web sites and online services. COPPA directed the  
22 Commission to promulgate a rule implementing COPPA. The Commission promulgated the  
23 Children’s Online Privacy Protection Rule, 16 C.F.R. Part 312, on November 3, 1999, under  
24 Section 1303(b) of COPPA, 15 U.S.C. 6502(b), and Section 553 of the Administrative Procedure  
25 Act, 5 U.S.C. § 553. The Rule went into effect on April 21, 2000. Pursuant to Section 1303(c) of  
26 COPPA, 15 U.S.C. § 6502(c), and Section 18(d)(3) of the FTC Act, 15 U.S.C. § 57a(d)(3), a  
27 violation of the Rule constitutes an unfair or deceptive act or practice in or affecting commerce, in  
28 violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

1 **DEFENDANT**

2 7. Defendant InMobi Pte Ltd. is a Singaporean private limited company with its  
3 headquarters at 30 Cecil Street, #19-08, Prudential Tower, Singapore 049712, and transacts or has  
4 transacted business in the Northern District of California. At all times material to this Complaint,  
5 acting alone or in concert with others, InMobi Pte Ltd. purposefully directed its activities to the  
6 United States by marketing and providing online services throughout the United States.  
7 Specifically, InMobi Pte Ltd. operates a mobile advertising network.

8 8. The FTC’s claims against Defendant arise from Defendant’s acts or practices in  
9 the United States.

10 **COMMERCE**

11 9. At all times material to this Complaint, Defendant has maintained a substantial  
12 course of trade in or affecting commerce, as “commerce” is defined in Section 4 and 5 of the FTC  
13 Act, 15 U.S.C. § 44; 45.

14 **DEFENDANT’S BUSINESS PRACTICES**

15 10. Defendant provides an advertising platform for mobile application developers and  
16 advertisers. By integrating Defendant’s software development kit (“InMobi SDK”), Android and  
17 iOS application developers can monetize their applications by allowing third party advertisers to  
18 advertise to consumers through various ad formats, such as banner ads, interstitial ads, and native  
19 ads. Advertisers, in turn, can target consumers across all of the mobile applications that have  
20 integrated the InMobi SDK.

21 11. Defendant describes itself as the “world’s largest independent mobile advertising  
22 company.” In February 2015, Defendant reported its advertising network had reached over one  
23 billion unique mobile devices, with 19% of those devices located in North America, and had  
24 served 6 billion ad requests per day.

25 **DEFENDANT’S GEO-TARGETING PRODUCTS**

26 12. Defendant offers several geo-targeting products through which advertisers can  
27 target consumers based on their physical location: the “Now” targeting suite, the “Conditional”  
28 targeting suite, and the “Psychographic” targeting suite.



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

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

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

15 21. When a consumer allows an application to access the location API, Defendant  
16 collects the consumer's location in order to serve targeted advertising via the geo-targeting  
17 product suites described in Paragraphs 12-15.

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

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

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

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

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

15 25. In any instance where the location API is accessible (*i.e.*, the application developer  
16 has included the location permission and the consumer has allowed the application's access to the  
17 location API), Defendant simultaneously collects latitude/longitude coordinates alongside the  
18 BSSID and other network information described in Paragraphs 23-24. Defendant correlates these  
19 two sets of information in order to create its own geocoder database through which it can match  
20 specific WiFi networks to specific locations.

21 26. Until December 2015, even in those instances where the location API was  
22 inaccessible (*i.e.*, the application developer had not included the location permission or the  
23 consumer had restricted the application's access to the location API), Defendant still collected the  
24 WiFi network information described in Paragraphs 23-24, fed the information into its geocoder  
25 database, and inferred the consumer's latitude and longitude. Through this method, Defendant  
26 could track the consumer's location and serve geo-targeted ads, regardless of the application  
27 developer's intent to include geo-targeted ads in the application, and regardless of the consumer's  
28 location settings.

1           27. In response to the Commission's investigation, Defendant modified its location  
2 tracking practices at the end of 2015. Defendant released a new version of the InMobi SDK in  
3 November 2015 and made additional server-side changes in December 2015. As a result of these  
4 modifications, Defendant no longer tracks a consumer's location based on the WiFi network  
5 information described in Paragraphs 23-24 unless the Android or iOS location API is accessible  
6 to the application integrating the InMobi SDK (*i.e.*, the application developer has included the  
7 location permission and the consumer has allowed the application's access to the location API).

8           **DEFENDANT'S REPRESENTATIONS REGARDING GEO-TARGETING**

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

13           To allow InMobi to show Geo targeted ads, you need to add the  
14           ACCESS\_COARSE\_LOCATION [sic] and ACCESS\_FINE\_LOCATION  
15           permissions.

16           29. However, as explained in Paragraph 23, providing access to the Android location  
17 API was not the only way Defendant tracked the consumer's location and served geo-targeted  
18 ads. Defendant also collects BSSID and other information related to the WiFi network to which a  
19 consumer's device is connected or in-range, if the Android application developer has included the  
20 Access WiFi State or Change WiFi State permissions. Through these means, until December  
21 2015, Defendants tracked the consumer's location and serve geo-targeted ads, regardless of  
22 whether the application developer had included the Access Coarse Location or Access Fine  
23 Location permissions, and regardless of the consumer's location settings.

24           30. To iOS application developers, Defendant disseminated or caused to be  
25 disseminated the following statements in the InMobi SDK integration guide, representing that it  
26 tracks the consumer's location and serves geo-targeted ads only if the application developer and  
27 the consumer provide access to the iOS location API:

28           You can set the user location by using the location methods in the ad request. . .

1 Passing the location object allows for better targeting, and potentially higher  
2 eCPMs [effective cost per thousand impressions].

3 31. However, as explained in Paragraph 24, providing access to the iOS location API  
4 was not the only way Defendant tracked the consumer's location and served geo-targeted ads.  
5 Defendant also collects the BSSID of the WiFi network to which a consumer's device is  
6 connected from all iOS applications that have integrated the InMobi SDK. Through these means,  
7 until December 2015, Defendant tracked the consumer's location and served geo-targeted ads,  
8 regardless of whether the application developer had passed the location object, and regardless of  
9 the consumer's location settings.

10 32. Defendant also disseminated or caused to be disseminated to both Android and  
11 iOS application developers the following additional statements in the InMobi SDK integration  
12 guide:

13 This [location] parameter is passed to InMobi provided that the user allows it. It  
14 should contain the latitude, longitude, and accuracy, separated by commas. This  
15 parameter is required if the request is needed to be considered for geo-targeting.

16 33. However, as explained in Paragraphs 23-24, providing access to the location APIs  
17 was not the only way Defendant tracked the consumer's location and served geo-targeted ads.  
18 Defendant also collects BSSID and other information related to the WiFi network to which a  
19 consumer's device is connected or in-range. Through these means, until December 2015,  
20 Defendant tracked the consumer's location and served geo-targeted ads, regardless of the  
21 application developer's intent to include geo-targeted ads in the application, and regardless of the  
22 consumer's location settings.

23 34. Through the marketing campaign for their geo-targeted ad products, Defendant has  
24 also disseminated or caused to be disseminated the following statements representing that it tracks  
25 the consumer's location and serves geo-targeted ads only if the consumer provides opt-in consent:

26 First, we take in location data on each user, *in the form of user opt-in lat/long*  
27 *signals*. Then we add real world context to these signals to figure out what places  
28 or businesses the user has visited. Our machine learning algorithms mine for



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

3 35. However, as explained in Paragraphs 23-24, Defendant tracked the consumer's  
4 location and served geo-targeted ads even if the consumer had not provided opt-in consent.  
5 Defendant collects BSSID and other information related to the WiFi network to which a  
6 consumer's device is connected or in-range, and used this information to track the consumer's  
7 location and serve geo-targeted ads, regardless of whether the consumer had provided opt-in  
8 consent.

9 36. Defendant represented in the disclosures described in paragraphs 28, 30,  
10 32, and 34 that it tracked the consumer's location and served geo-targeted ads only if the  
11 application developer and the consumer provided access to the location APIs, and the  
12 consumer provided opt-in consent. In fact, Defendant collected and used BSSID and  
13 other WiFi network information to track the consumer's location and serve geo-targeted  
14 ads regardless of the application developer's intent to include geo-targeted ads, and  
15 regardless of the consumer's location settings.

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

24 38. Defendant's practices undermined consumers' ability to make informed  
25 decisions about their location privacy and to control the collection and use of their  
26 location information through the thousands of applications that have integrated the InMobi  
27 SDK. Defendant's practices also deprived consumers of the ability to ensure that they  
28 installed and used only those applications that would honor their location privacy

1 preferences.

2 **DEFENDANT’S BUSINESS PRACTICES REGARDING COLLECTION OF**  
3 **INFORMATION FROM CHILD-DIRECTED APPLICATIONS**

4 39. For purposes of Paragraphs 39 through 50, and 57 through 65, herein, the terms  
5 “child,” “collects,” “collection,” “disclosure,” “Internet,” “operator,” “parent,” “personal  
6 information,” “obtaining verifiable consent,” and “Web site or online service directed to  
7 children,” are defined as those terms are defined in Section 312.2 of the COPPA Rule, 16 C.F.R.  
8 § 312.2.

9 40. The Rule applies to any operator of a commercial Web site or online service  
10 directed to children that collects, uses, and/or discloses personal information from children,  
11 including an operator of a commercial Web site or online service that has actual knowledge that it  
12 is collecting personal information directly from users of another Web site or online service  
13 directed to children. Among other things, the Rule requires operators to meet specific  
14 requirements prior to collecting online, using, or disclosing personal information from children,  
15 including but not limited to:

- 16 a. posting a privacy policy on its Web site or online service providing clear,  
17 understandable, and complete notice of its information practices, including what  
18 information the operator collects from children online, how it uses such  
19 information, its disclosure practices for such information, and other specific  
20 disclosures set forth in the Rule;
- 21 b. providing clear, understandable, and complete notice of its information practices,  
22 including specific disclosures, directly to parents when required by the Rule; and
- 23 c. obtaining verifiable parental consent prior to collecting, using, and/or disclosing  
24 personal information from children.

25 41. In order to monetize applications through Defendant’s mobile advertising network,  
26 application developers must integrate the InMobi SDK and register their application with  
27 Defendant. On or around June 30, 2013, Defendant introduced an option in the registration  
28 process through which application developers could indicate to Defendant that the registered

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

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

8 **WHAT ABOUT CHILDREN?**

9 We do not knowingly collect any personal information about children under the  
10 age of 13. If we become aware that we have collected personal information about  
11 a child under the age of 13, that information will be immediately deleted from our  
12 database.

13 43. In addition, Defendant disseminated or caused to be disseminated the following  
14 statements regarding the collection and use of children’s personal information through a separate  
15 COPPA Policy:

16 InMobi has always adopted a policy of not knowingly collecting any personal  
17 information about children under the age of 13 and if we become aware that we  
18 have collected personal information about a child under the age of 13, that  
19 information will be immediately deleted from our database.

20 ...

21 The amended COPPA rules effective on July 1, 2013 apply to operators of  
22 websites and mobile apps that are directed at children under 13 that collect, use or  
23 disclose personal information from children or to operators that have actual  
24 knowledge that they are collecting personal information from users of sites or apps  
25 directed to children. The existing obligation requiring parental consent before  
26 collecting personal information from children has been expanded to include  
27 persistent identifiers that can enable operators and third parties to recognize users.

28 ...

1 In response to the new COPPA rules effective on July 1, 2013 InMobi is  
2 continuing to ensure that we do not collect and use information from children's  
3 sites for behavioral advertising (often referred to as interest based advertising).  
4 We will continue to only use any data in the manner that COPPA prescribes. We  
5 have identified all existing publisher sites and apps directed to children to ensure  
6 we are in full compliance with the new COPPA rules and from 30 June, 2013 shall  
7 ensure that new and existing publishers are required to notify InMobi of any new  
8 sites or app accounts that are directed at children to ensure we continue to comply  
9 with the COPPA rules.

10 44. Despite the representations described in Paragraphs 42-43, Defendant neither  
11 implemented adequate privacy controls to ensure its compliance with COPPA nor tested that the  
12 controls that it had implemented functioned as intended. As a result, for over two years, until  
13 October 2015, Defendant knowingly collected and used personal information – including unique  
14 device identifiers, geolocation information, and BSSIDs used to infer location (as described in  
15 Paragraphs 22-27) – from thousands of applications that had indicated to Defendant that they  
16 were directed to children.

17 45. Defendant used this personal information to track children's locations and serve  
18 interest-based, behavioral advertising, including through the "Now," "Conditional," and  
19 "Psychographic" geo-targeting products described in Paragraphs 12-15.

20 46. Collectively, hundreds of millions of consumers have downloaded the thousands  
21 of child-directed applications from which Defendant collected and used personal information.  
22 Defendant collected such personal information each time an application made an ad request to  
23 their network – typically every 30 seconds when an application is in use.

24 47. Defendant's online notice of its information practices did not clearly, completely,  
25 or accurately disclose all of Defendant's information collection and use practices for children, as  
26 required by the Rule.

27 48. Defendant did not provide parents with a direct notice of its information practices  
28 prior to collecting and using children's personal information.

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

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

5 **DEFENDANT'S VIOLATIONS OF THE FTC ACT**

6 **COUNT I**

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

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

19 **COUNT II**

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

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

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

2 **COUNT III**

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

6 56. In truth and in fact, as set forth in Paragraphs 41 and 44-46, Defendant collected  
7 and used personal information from applications directed to children. Therefore, the  
8 representation set forth in Paragraph 55 was false or misleading and constituted a deceptive act or  
9 practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

10 **DEFENDANT'S VIOLATION OF THE COPPA RULE**

11 **COUNT IV**

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

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

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

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

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

3 b. Section 312.4(b) of the Rule, 16 C.F.R. § 312.4(b), which requires an  
4 operator to provide direct notice to parents of the information Defendant  
5 collects online from children, how it uses such information, and its  
6 disclosure practices for such information, among other required content;  
7 and

8 c. Section 312.5(a)(1) of the Rule, 16 C.F.R. § 312.5(a)(1), which requires an  
9 operator to obtain verifiable parental consent before any collection, use,  
10 and/or disclosure of personal information from children.

11 60. Defendant's acts or practices, as described in Paragraph 57 above, violated the  
12 COPPA Rule, 16 C.F.R. Part 312.

13 61. Pursuant to Section 1303(c) of COPPA, 15 U.S.C. § 6502(c), and Section 18(d)(3)  
14 of the FTC Act, 15 U.S.C. § 57a(d)(3), a violation of the Rule constitutes an unfair or deceptive  
15 act or practice in or affecting commerce, in violation of Section 5(a) of the FTC Act, 15 U.S.C. §  
16 45(a).

17 **THE COURT'S POWER TO GRANT RELIEF**

18 62. Defendant violated the Rule as described above with the knowledge required by  
19 Section 5(m)(1)(A) of the FTC Act, 15 U.S.C. § 45(m)(1)(A).

20 63. Each collection or use of a child's personal information in which Defendant  
21 violated the Rule in one or more of the ways described above, constitutes a separate violation for  
22 which Plaintiff seeks monetary civil penalties.

23 64. Section 5(m)(1)(A) of the FTC Act, 15 U.S.C. § 45(m)(1)(A), as modified by  
24 Section 4 of the Federal Civil Penalties Inflation Adjustment Act of 1990, 28 U.S.C. § 2461, and  
25 Section 1.98(d) of the FTC's Rules of Practice, 16 C.F.R. § 1.98(d), authorizes this Court to  
26 award monetary civil penalties of not more than \$16,000 for each such violation of the Rule on or  
27 after February 10, 2009.

28 65. Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), empowers this Court to grant

1 injunctive and such other relief as the Court may deem appropriate to halt and redress violations  
2 of any provision of law enforced by the FTC.

3 **PRAYER**

4 WHEREFORE, Plaintiff United States of America, pursuant to Sections 5(a)(1),  
5 5(m)(1)(A), 13(b) and 16(a) of the FTC Act, 15 U.S.C. §§ 45(a)(1), 45(m)(1)(A), 53(b), and  
6 56(a), and the Court's own equitable powers, requests that the Court:

7 (1) Enter a permanent injunction to prevent future violations of the FTC Act by  
8 Defendant with respect to the privacy of consumers' personal information;

9 (2) Enter a permanent injunction to prevent future violations of the FTC Act and the  
10 COPPA Rule by Defendant;

11 (3) Award Plaintiff monetary civil penalties from Defendant for each violation of the  
12 COPPA Rule alleged in this Complaint; and

13 (4) Award such other and additional relief as the Court may determine to be just and  
14 proper.

15 ///

16 ///

17 ///

18 ///

19 ///

20 ///

21 ///

22 ///

23 ///

24 ///

25 ///

26 ///

27 ///

28 ///



1 Dated: June 22, 2016

Respectfully submitted,

2 **FOR THE FEDERAL TRADE**  
3 **COMMISSION:**

**FOR PLAINTIFF**  
**THE UNITED STATES OF**  
**AMERICA:**

4  
5 MANEESHA MITHAL  
Associate Director  
6 Division of Privacy and Identity  
7 Protection

BENJAMIN C. MIZER  
Principal Deputy Assistant  
Attorney General  
Civil Division

8 MARK EICHORN  
Assistant Director  
9 Division of Privacy and Identity  
10 Protection

JONATHAN F. OLIN  
Deputy Assistant Attorney General

11 NITHAN SANNAPPA  
Attorney  
12 Division of Privacy and Identity  
13 Protection  
14 Federal Trade Commission  
15 600 Pennsylvania Avenue, N.W.  
16 (202) 326-3185 (voice)  
(202) 326-3062 (fax)

MICHAEL S. BLUME  
Director  
Consumer Protection Branch

17 JACQUELINE CONNOR  
Attorney  
18 Division of Privacy and Identity  
19 Protection  
20 Federal Trade Commission  
21 600 Pennsylvania Avenue, N.W.  
(202) 326-2844 (voice)  
(202) 326-3062 (fax)

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