Ann Marie Mortimer (State Bar No. 169077)
amortimer@HuntonAK.com
Jason J. Kim (State Bar No. 221476)
kimj@HuntonAK.com
Jeff R. R. Nelson (State Bar No. 301546)
jnelson@HuntonAK.com
HUNTON ANDREWS KURTH LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627
Telephone: (213) 532-2000
Facsimile: (213) 532-2020

Attorneys for Plaintiff
FACEBOOK, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

FACEBOOK, INC., a Delaware corporation,

Plaintiff,

v.

JEDIMOBI TECH PTE. LTD. and LIONMOBI HOLDING, LTD.,

Defendants.

CASE NO.: 3:19-cv-04556

COMPLAINT FOR:

(1) BREACH OF CONTRACT

(2) COMPUTER FRAUD AND ABUSE ACT (18 U.S.C. § 1030(A))

(3) CALIFORNIA COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT (CAL. PENAL CODE § 502)

(4) FRAUD

(5) UNFAIR OR FRAUDULENT BUSINESS PRACTICES (CAL. BUSINESS AND PROFESSIONS CODE §§ 17200 ET SEQ.)

DEMAND FOR JURY TRIAL

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

INTRODUCTION

1. In 2018, Defendants JediMobi Tech Pte. Ltd. and LionMobi Holding, Ltd. were application developers that deceived their users ("the app users") into installing fraudulent and malicious apps from the Google Play store. Unbeknownst to the app users, Defendants delivered and installed malicious code ("malware") onto the app users' mobile devices through the apps. Defendants designed the malware to create the false impression that the app user clicked on advertisements delivered to the user's device, a practice known as "click injection fraud." Defendants specifically targeted ads serviced by social media companies, including Facebook and Google. As a result of their scheme, Defendants generated advertising revenue for themselves. Facebook identified Defendants and their scheme through an investigation of malicious apps and disabled Defendants' known Facebook and advertising accounts in 2018. Facebook seeks injunctive and other equitable relief and damages against Defendants.

PARTIES

2. Facebook is a Delaware corporation with its principal place of business in Menlo Park, San Mateo County, California.

3. Defendant JediMobi is corporation registered in Singapore, with its principal place of business at 60 Paya Lebar Road #09-26, Paya Lebar Square, Singapore.

4. Defendant LionMobi is a Hong Kong, China corporation headquartered and registered in China, with its principal place of business at Topsail Plaza, No. 11 On Sum Street, Hong Kong, China.

5. At all times material to this action, each Defendant was the agent, employee, partner, alter ego, subsidiary, or co-conspirator of and with the other Defendant, and the acts of each Defendant were in the scope of that relationship. In doing the acts and failing to act as alleged in this Complaint, each Defendant acted with the knowledge, permission, and the consent of each of the other Defendant; and, each

Defendant aided and abetted the other Defendant in the acts or omissions alleged in this Complaint.

JURISDICTION

6. This Court has federal question jurisdiction over the federal causes of action alleged in this complaint pursuant to 28 U.S.C. § 1331.

7. The Court has supplemental jurisdiction over the state law causes of action alleged in this complaint pursuant to 28 U.S.C. § 1367 because these claims arise out of the same nucleus of operative fact as Facebook's federal claims.

8. In addition, the Court has jurisdiction over all the causes of action alleged in this complaint asserted pursuant to 28 U.S.C. § 1332 because there exists complete diversity between Facebook and each of the named Defendants, and because the amount in controversy exceeds $75,000.

9. The Court has personal jurisdiction over Defendants because each Defendant used Facebook's platform and participated in Facebook's Audience Network and thereby agreed to Facebook's Terms of Service, Platform Policy, Audience Network Terms, and Audience Network Policy. LionMobi also used Facebook's advertising platform and thereby agreed to Facebook's Advertising Policies. In relevant part, Facebook's Terms of Service require Defendants to submit to the personal jurisdiction of this Court.

10. In addition, the Court has personal jurisdiction because Defendants knowingly directed and targeted their scheme at Facebook, which has its principal place of business in California. Defendants also participated in Facebook Audience Network, Facebook's advertising platform, and transacted business using Facebook, and engaged in commerce in California.

11. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) as the threatened and actual harm to Plaintiffs occurred in this District. Venue is also proper with respect to each of the Defendants pursuant to 28 U.S.C. §1391(c)(3) because none of the Defendants resides in the United States.

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

12. Pursuant to Civil L.R. 3-2(c), this case may be assigned to either the San Francisco or Oakland Division because Facebook is located in San Mateo County.

FACTS

A. Background

13. Facebook is a social networking website and mobile application that enables its users to create their own personal profiles and connect with each other on mobile devices and personal computers. As of June 2019, Facebook daily active users averaged 1.59 billion and monthly active users averaged 2.3 billion, worldwide.

14. Facebook's Audience Network is a product that Facebook offers to enable advertisers to display their ads to people who use (non-Facebook) apps and websites. By integrating their apps with Audience Network, third-party mobile app developers can generate revenue by displaying ads to Facebook users who use their apps. To implement Audience Network, a third-party mobile app developer adds code provided by Facebook to their app, which will show and track the Audience Network ads (the "Audience Network SDK"). Facebook pays the third-party mobile app developers a percentage of the net revenue generated from the ads delivered on their apps. Generally, the payment amounts depend on the number of clicks attributed to the ads displayed on a particular app through Audience Network.

15. Like Facebook's Audience Network, Google also has an advertising network for mobile apps called AdMob. AdMob allows advertisers to display ads in mobile apps visited by Google users. AdMob compensates the mobile app developers based on the number of clicks attributed to the ads displayed through AdMob.

16. Access and interaction with Facebook's computer network is subject to and restricted by Facebook's Terms of Service ("TOS"), Audience Network Terms ("AN Terms"), and Advertising Policies ("Ad Policies").

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

i. Facebook's TOS

17. Everyone who uses Facebook must agree to Facebook's TOS (available at https://www.facebook.com/terms.php), and other rules that govern different types of access to, and use of, Facebook.

18. Section 3.2.1 of the TOS prohibits using Facebook to do anything "[t]hat violates these Terms, and other terms and policies," and that "is unlawful, misleading, discriminatory or fraudulent" or "violates someone else's rights."

19. Section 3.2.2 prohibits uploading "viruses or malicious code or do[ing] anything that could disable, overburden, or impair the proper working or appearance of our Products."

ii. Facebook's AN Terms

20. All developers operating on Audience Network agree to the AN Terms (available at https://www.facebook.com/ads/manage/audience_network/publisher_tos/), which incorporate Facebook's Platform Policy ("Platform Policy") (available at https://developers.facebook.com/policy) and the Audience Network Policy ("AN Policy") (available at https://developers.facebook.com/docs/audience-network/policy).

21. Section 3.1 of the AN Terms requires developers "to comply with the Audience Network Service specifications provided by FB from time-to-time to enable proper delivery, display, tracking and reporting of Ads, including without limitation, by not modifying, misusing or deriving data from the technology (e.g., the FB SDK, FB tags, or FB API's, as applicable)."

22. Section 1.4 of the AN Policy prohibits the dissemination of "spyware, malware, or any software that results in an unexpected or deceptive experience."

23. Section 3.2 of the AN Policy requires that developers implement Audience Network "in a way that delivers the expected clicks, impressions or conversion" and specifically prohibits the use of "automated, deceptive, fraudulent or other invalid

means (ex: through repeated manual clicks or the use of bots) to artificially inflate clicks, impressions or conversions."

24. Section 1.7 of the Platform Policy requires that developer apps not "confuse, deceive, mislead, spam or surprise anyone."

iii. Facebook's Ad Policies

25. Facebook's TOS prohibit violations of Facebook's Ad Policies, which apply to ads run across Facebook Products (available at https://www.facebook.com/policies/ads/). Ad Policy 4.13 states "ads, landing pages, and business practices must not contain deceptive, false, or misleading content, including deceptive claims, offers, or methods."

26. Ad Policy 4.25 requires that "Ads must not contain spyware, malware, or any software that results in an unexpected or deceptive experience. This includes links to sites containing these products."

B. Defendants Agreed to Facebook's TOS, AN Terms, and Policies

i. LionMobi

27. LionMobi created a Facebook Page—a profile on Facebook used to promote a business or other commercial, political, or charitable organization or endeavor—on approximately October 24, 2014. A Facebook Page can only be created by a user with a Facebook account.

28. On approximately January 21, 2015, LionMobi signed up to participate in AN. To sign up for AN, LionMobi agreed to the AN Terms.

29. On approximately October 11, 2016, the Chief Operating Officer of LionMobi Holding Limited, signed a "Written Acknowledgement of Audience Network Terms" affirming that "use by LionMobi Holding Limited . . . of Facebook's Audience Network feature is governed by the then-current Audience Network Terms . . ." (See Exhibit 1.)

30. Between 2015 and 2018, LionMobi advertised its apps on Facebook. LionMobi ran numerous ads relating to their app called PowerClean. LionMobi agreed

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

to the Ad Policies before running an advertisement.

31. At all relevant times, LionMobi was a Facebook user that agreed to and was by bound by the TOS. LionMobi's employees and agents accepted and agreed to be bound by the TOS, AN Terms, AN Policy, Platform Policy, and Ad Policies on behalf of LionMobi.

ii. JediMobi

32. JediMobi created a Facebook Page on approximately August 8, 2016.

33. On approximately August 23, 2018, JediMobi registered to participate in Audience Network. JediMobi agreed to the AN Terms when it registered to participate in Audience Network.

34. At all relevant times, JediMobi was a Facebook user that agreed to and was bound by the TOS. JediMobi's employees and agents accepted and agreed to be bound by the TOS, Platform Policy, AN Terms, and AN Policy on behalf of JediMobi.

C. Defendants' Click Injection Fraud Scheme

i. Overview

35. In 2018, Defendants jointly engaged in a click injection fraud scheme targeting Facebook and Google. Defendants' scheme proceeded as follows:

36. *First*, Defendants developed fraudulent mobile apps for the Google Play store, which purported to be utility apps. Defendants falsely marketed their apps on the Google Play store, as calculator or cleaner apps for mobile devices. In fact, Defendants knew that the apps delivered malware, which the users unknowingly installed on their devices. At times, the malware was delivered in the form of "updates" to the apps and, after October 2018, the malware was included directly in the apps.

37. *Second*, Defendants registered their apps with Facebook's Audience Network and Google's AdMob in order to deliver ads purchased by advertisers through Facebook and Google. Defendants also advertised at least one of their fraudulent apps on Facebook, in violation of Facebook TOS and Policies, in order to entice Facebook users into visiting the Google Play store and installing the app.

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

38. *Third*, after Defendants' malware was installed on their app users' mobile devices, Defendants monitored advertising activity from Facebook and Google and injected fake user clicks. These fake clicks generated advertising revenue for Defendants.

ii. Defendants Offered and Promoted Fraudulent Apps on the Google Pay Store

39. Defendants created and promoted several apps on the Google Play store, which is Google's online store for Android apps, games, and other content. Users who visited the Google Play store could download and install Defendants' apps on an Android-compatible device. Facebook did not host the fraudulent apps or grant them access to user data.

a. LionMobi's Power Clean App

40. From approximately January 21, 2015 to the present, LionMobi offered an app called "Power Clean – Antivirus and Phone Cleaner App" on the Google Play store. On the Google Play store, LionMobi represented that the app was a "light, fast & smart android phone cleaner and booster app that clean (sic) phone memory and storage space with simply 1 tap." LionMobi did not disclose to its app users that the Power Clean app would be used as a conduit to install malware onto the app users' devices or inject fake user clicks, as set forth in further detail below.

41. According to LionMobi's website, the Privacy Policy for the Power Clean App claimed only to "use the information we collect from our applications and services to provide you better features and experiences on them." (See Exhibit 2.) The Policy failed to inform users that the Power Clean App infected their devices with malware designed to monitor advertising activity from Google, and inject fake clicks purporting to originate from the app user. (Exhibit 2.)

42. Beginning no later than October 2018, LionMobi advertised its Power Clean app on Facebook in a variety of ads. (See Exhibit 3.) The ads did not identify

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

that Power Clean would install malware on users' devices or inject fake user clicks. Instead, the ads misrepresented the app as an "antivirus" app.

b. JediMobi's Calculator Plus App

43. Between July 24, 2018 and December 2018, JediMobi offered an app called "Calculator Plus," which purported to operate as a calculator with multiple functions, including exchange rate calculation and time zone conversion. On the Google Play store, JediMobi represented that the app functioned as a "scientific calculator and math calculator do like calculus calculation, trigonometric calculation, but it also acts as your GPA calculator, BMI calculator and even discount calculator!"

44. Similarly, JediMobi's Privacy Policy failed to inform users that the Calculator Plus App infected their devices with malware designed to monitor advertising activity from Facebook and Google, and inject fake clicks purporting to originate from the app user. (See Exhibit 4.)

iii. Defendants' Fraudulent Apps Injected Fake Clicks

45. Defendants' apps did not operate as advertised on the Google Play store or consistent with their Privacy Policies. Instead, they installed malware designed to intercept ad-related data and inject fake clicks, in order to deceive Facebook's Audience Network and Google's AdMob into crediting the apps for clicks that did not occur. Among other things, this violated Facebook's TOS and the AN Terms.

a. Defendants Used the Calculator Plus App To Defraud Facebook

46. Between July 24, 2018 and December 27, 2018, JediMobi's Calculator Plus app was part of Audience Network. This means that the app showed its users ads served by Facebook. In connection with their participation in Audience Network, Defendants were paid a percentage of the advertising revenue and received additional compensation if app users clicked on the ads. In addition to receiving ads from Audience Network, the Calculator Plus app was also part of AdMob and showed ads from Google.

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

47. On approximately October 22, 2018, the Defendants updated Calculator Plus to version 1.1.8. This "update" included customized malware that would fraudulently simulate clicks on Audience Network ads. Specifically, the malware tampered with the Audience Network SDK, monitored the ads, and injected fake clicks on those ads. The fake clicks were delivered to Facebook servers in connection with Audience Network. The only purpose of this malware was to defraud Facebook into believing that additional users had clicked on Audience Network ads.

48. The malware was also designed to make the fake clicks appear to be those of a real user by falsifying user movements on the device and timing the fake clicks so that they occurred after a user would have the opportunity to view the ad.

49. The fabricated clicks generated payments for Defendants through their participation in Audience Network. In total, the app generated over 40 million ad impressions and 1.7 million clicks through Audience Network from October 2018 to December 2018—when Facebook detected the fraud and suspended them.

50. The Calculator Plus App also contained malware to simulate clicks on the AdMob network.

b. Defendants Used Deceptive Ads on Facebook to Promote the Power Clean App

51. Defendants advertised the Power Clean App on Facebook in violation of: (1) Ad Policy 4.13 because the ads contained "deceptive, false, or misleading content;" and (2) Ad Policy 4.25 because the ads directed Facebook users to the Google Play store to install the fraudulent apps. Defendants knew the ads and the apps were deceptive and misleading because, unbeknownst to the users, the app infected the users' devices with malware for the purpose of injecting fake clicks.

52. From at least October 26, 2018, the Power Clean app included malware designed to fabricate clicks on ads served by the AdMob system. Specifically, whenever a user performed certain activities in the Power Clean app, an ad was displayed through the AdMob system. The malware would then inject a fake click on

the AdMob ad. The only purpose of this malware was to deceive Google's AdMob system into believing that additional users had clicked on AdMob ads.

53. Like the malware contained in the Calculator Plus app, the AdMob malware took steps to make the simulated clicks appear to be those of a real user by, among other things, falsifying user movements and timing the simulated clicks so that they occurred after a user would have the opportunity to view the ad.

iv. JediMobi and LionMobi Share the Malware and Computer Infrastructure Used to Inject Clicks

54. JediMobi's Calculator Plus app and LionMobi's Power Clean app shared customized malware designed to inject clicks for Google's AdMob network.

55. Defendants also programmed the malware to rely on shared computer infrastructure. For example, the IP address of a LionMobi server was encoded into the malware on JediMobi's Calculator Plus app. JediMobi's Calculator Plus app also included code that checked for the presence of a LionMobi app on the app users' device and modified the malware's behavior based on that determination.

56. In addition, the malware developer used the encryption key "lionmobikey$)!1" for the malware on JediMobi's Calculator Plus app.

D. Facebook's Enforcement Actions Against Defendants

57. In approximately December 2018, Facebook detected and began investigating fake user clicks associated with the Calculator Plus app, JediMobi, and LionMobi.

58. On or about December 27, 2018, Facebook suspended Defendants from Audience Network and disabled Facebook accounts associated with Defendants. Facebook also refunded the impacted advertisers.

E. Defendants' Unlawful Acts Have Caused Facebook Substantial Harm.

59. Defendants' breaches of Facebook's TOS, AN Terms, and Ad Policies and other misconduct described above have harmed Facebook, by, among other things,

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

interfering with Facebook's service.

60. Defendants' misconduct also has injured Facebook's reputation, public trust, and goodwill, and has caused Facebook to spend resources investigating and redressing Defendants' wrongful conduct. Facebook has suffered damages attributable to the efforts and resources it has used to investigate, address, and mitigate the matters set forth in this Complaint.

61. Defendants have been unjustly enriched by their activities at Facebook's expense.

FIRST CAUSE OF ACTION

Breach of Contract

62. Facebook incorporates all other paragraphs as if fully set forth herein.

63. Access to and use of Facebook and services is governed by Facebook's TOS and its related policies. Access to and use of Facebook's Audience Network is governed by the AN Terms. Access to and use of advertising on Facebook is governed by Facebook's Advertising Policies.

64. Defendants agreed to and became bound by Facebook's TOS, Platform Policy, AN Terms, when they used Facebook, Facebook's platform, and Facebook's services. Similarly, Defendant LionMobi separately agreed to and became bound by Facebook's Advertising Policies by using Facebook's advertising platform.

65. Facebook has performed all conditions, covenants, and promises required of it in accordance with Facebook's TOS and related policies.

66. As alleged above, Defendants knowingly breached Facebook's TOS, Platform Policy, and AN Terms. In addition, LionMobi knowingly breached Facebook's Advertising Policies.

67. When Defendants agreed to and became bound by Facebook's TOS, Platform Policy, AN Terms, and Advertising Policies, both Facebook and Defendants knew or reasonably could have foreseen that the harm and injury to Facebook was likely to occur in the ordinary course of events because of Defendants' breach.

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

68. Defendants' respective breaches caused Facebook damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION

Violations of the Computer Fraud and Abuse Act

18 U.S.C. § 1030 et seq.

69. Facebook incorporates all other paragraphs as if fully set forth herein.

70. Facebook's computer network is comprised of protected computers involved in interstate and foreign commerce and communication as defined by 18 U.S.C. § 1030(e)(2).

71. Defendants knowingly and with intent to defraud, accessed Facebook's computer network without Facebook's authorization. Namely, Defendants used malware designed to deliver fake user clicks to the endpoints used by Facebook's Audience Network, which were only accessible through the Audience Network SDK on the users' compromised devices.

72. In violation of 18 U.S.C. § 1030(a)(4), Defendants, knowingly and with intent to defraud, accessed Facebook protected computers, by sending unauthorized commands, namely, fake user clicks which purported to originate from Android app users, but in fact originated from Defendants' malware. These commands were directed to Facebook's computer network for the purpose of furthering Defendants' click injection fraud scheme and obtaining anything of value, including payment for fraudulent ad clicks.

73. In violation of 18 U.S.C. § 1030(a)(5)(A), Defendants knowingly and intentionally caused the transmission of a program, information, code or command and as a result of such conduct intentionally damaged Facebook protected computers.

74. In violation of 18 U.S.C. § 1030(a)(5)(B), Defendants knowingly and intentionally accessed a protected computer without authorization, and as a result of such conduct, recklessly caused damage to Facebook protected computers.

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

75. In violation of 18 U.S.C. §1030(a)(5)(C), Defendants knowingly and intentionally accessed a protected computer without authorization, and as a result of such conduct, caused damage to Facebook protected computers and a loss.

76. In violation of 18 U.S.C. § 1030(b), Defendants conspired or attempted to commit the violations alleged in the preceding paragraphs.

77. Defendants' conduct has caused a loss to Facebook during a one-year period in excess of $5,000.

78. Defendants' actions caused Facebook to incur losses and other economic damages, including the expenditure of resources to investigate and respond to Defendants' fraudulent scheme.

THIRD CAUSE OF ACTION

Violations of the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502

79. Facebook incorporates all other paragraphs as if fully set forth herein.

80. Through the malicious software, Defendants knowingly and without permission accessed Facebook's computer networks, namely, endpoints used by Facebook's Audience Network, in order to devise and/or execute a scheme to defraud and deceive, all in violation of California Penal Code § 502(c)(1).

81. In violation of California Penal Code § 502(c)(3), Defendants knowingly and without permission used or caused to be used Facebook's computer services.

82. In violation of California Penal Code § 502(c)(5), Defendants knowingly and without permission disrupted or caused the disruption of computer services and/or denied or caused the denial of computer services to one or more authorized users of Facebook's computers, computer systems, and/or computer networks.

83. In violation of California Penal Code § 502(c)(7), Defendants knowingly and without permission accessed or caused to be accessed Facebook's computers, computer systems, and/or computer networks.

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

84. Because Facebook suffered damages and a loss as a result of Defendants' actions, Facebook is entitled to compensatory damages in an amount to be determined at trial, attorney fees, and injunctive relief under California Penal Code § 502(e)(1) and (2).

85. Because Defendants willfully violated California Penal Code § 502, and there is clear and convincing evidence that Defendants committed "fraud" as defined by section 3294 of the Civil Code, Facebook is entitled to punitive and exemplary damages under California Penal Code § 502(e)(4).

FOURTH CAUSE OF ACTION

Fraud

86. Facebook realleges and incorporates by reference all of the preceding paragraphs.

87. From approximately October 2018 until December 2018, Defendants knowingly used customized malware to defraud Facebook into believing that users had clicked on ads, when, in fact, the Defendants malware had fabricated the clicks. Defendants' used malware to create fake user clicks which Facebook received and relied on in issuing advertising revenue payments to Defendants. As a result of the false information, Defendants received higher payments for Audience Network as a direct result of clicks that they had fabricated. Defendants intended that their misrepresentations about the origin and number of clicks on each ad would be relied on by Facebook, and Facebook reasonably relied on Defendants' misrepresentations in providing Audience Network payments to Defendants.

FIFTH CAUSE OF ACTION

Unlawful, Unfair, or Fraudulent Business Practices

Cal. Business and Professions Code §§ 17200 et seq.

88. Facebook incorporates all other paragraphs as if fully set forth herein.

89. Defendants' actions described above constitute unlawful, unfair, or fraudulent acts or practices in the conduct of a business, in violation of California's

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Business and Professions Code Section 17200 et seq., including actions forbidden by other laws.

90. Defendants' practices are unlawful because they violate the Computer Fraud and Abuse Act and California Comprehensive Data Access and Fraud Act, as set forth above.

91. Defendants' practices are unfair because they offend established public policy and are substantially injurious to Facebook and its users.

92. Defendants' practices are fraudulent because they deceived Facebook into believing that clicks generated in Audience Network ads on their apps are genuine, when in fact they were not. Defendants' practices are also fraudulent because they deceived Facebook and its users into believing that Defendants' ads offered a legitimate app, when in fact, their apps concealed malicious software.

93. As a result of Defendants' acts and omissions, Facebook was injured in fact and lost money and property in the form of, among other things, payments to defendants predicated, in part, on the injected clicks and costs to investigate, remediate, and prevent Defendants' wrongdoings.

REQUEST FOR RELIEF

WHEREFORE, Facebook requests judgment against Defendants as follows:

1. That the Court enter judgment against Defendants that Defendants have:

   a. Breached their contracts with Facebook, in violation of California law;

   b. Violated the Computer Fraud and Abuse Act, in violation of 18 U.S.C. § 1030;

   c. Violated the California Comprehensive Computer Data Access and Fraud Act, in violation of California Penal Code § 502;

   d. Committed fraud on Facebook, in violation of California law; and

   e. Violated the California Unlawful, Unfair, or Fraudulent Business Practices law.

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

2. That the Court enter a permanent injunction enjoining and restraining Defendants from:

a. Accessing or attempting to access Facebook's website and computer systems;

b. Creating or maintaining any Facebook accounts in violation of Facebook's TOS;

c. Engaging in any activity to defraud Facebook or its users; and

d. Engaging in any activity, or facilitating others to do the same, that violates Facebook's TOS, Audience Network Terms, Audience Network Policies, Advertising Policies, or other related policies referenced herein.

3. That Facebook be awarded damages, including, but not limited to, compensatory, statutory, and punitive damages, as permitted by law and in such amounts to be proven at trial.

4. That Facebook be awarded a recovery in restitution.

5. That Facebook be awarded its reasonable costs, including reasonable attorneys' fees.

6. That Facebook be awarded pre- and post-judgment interest as allowed by law.

///

///

///

///

///

///

///

///

///

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

7. That the Court grant all such other and further relief as the Court may deem just and proper.

Dated: August 6, 2019

HUNTON ANDREWS KURTH LLP

By: /s/ Ann Marie Mortimer
Ann Marie Mortimer
Jason J. Kim
Jeff R. R. Nelson
Attorneys for Plaintiff
FACEBOOK, INC.

Jessica Romero
Tyler Smith
Michael Chmelar
Platform Enforcement and Litigation
Facebook, Inc.

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

JURY TRIAL DEMAND

Plaintiff hereby demands a trial by jury on all issues triable to a jury.

Dated: August 6, 2019

HUNTON ANDREWS KURTH LLP

By: /s/ Ann Marie Mortimer
Ann Marie Mortimer
Jason J. Kim
Jeff R. R. Nelson
Attorneys for Plaintiff
FACEBOOK, INC.

Jessica Romero
Tyler Smith
Michael Chmelar
Platform Enforcement and Litigation
Facebook, Inc.

Hunton Andrews Kurth LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

EXHIBIT 1

facebook

October 11, 2016

LIONMOBI HOLDING LIMITED
GCCD0582 RM B 14/F WAH HEN COMM CTR 383 HENNESSY RD
HongKong, 999077 Wan Chai District, Hong Kong

Re: Written Acknowledgement of Audience Network Terms

To Whom It May Concern,

Per your request, this letter serves as a written confirmation that use by Lionmobi Holding Limited ("**Publisher**") and Facebook, Inc. ("**Facebook**") of Facebook's Audience Network feature is governed by the then-current Audience Network Terms available at https://www.facebook.com/ads/manage/audience_network/publisher_tos (or a successor URL as designated by Facebook) and commenced in September 2015.

If the parties acknowledge and agree to the foregoing, kindly acknowledge acceptance by signing in the spaces provided below.

FACEBOOK, INC.

By: Erwin Castellanos
Erwin Castellanos (Oct 17, 2016)

Name: Erwin Castellanos

Title: Authorized Signatory

facebook LEGAL Menlo Park, CA

ACCEPTED AND AGREED:

PUBLISHER:
Lionmobi Holding Limited

By: You Tao

Name: YOU TAO

Title: COO

For and on behalf of
LIONMOBI HOLDING LIMITED

.....
Authorized Signature(s)

EXHIBIT 2

06/27/19 - Screenshot of Power Clean Privacy Policy - https://www.lionmobi.com/powerclean/privacypolicy.html

We respect the privacy of every individual users of our applications and services.

This Privacy Policy ("Policy") describes how LionMobi ("LionMobi", "We", "Us", or "Our") protects your privacy when you use LionMobi applications on all platforms ("App", "Apps", "Application" or "Applications") and the related services we provide ("Service" or "Services").

This Policy covers our collection, use and disclosure of your information through the Applications and the Services. It does not cover any collection, use or disclosure by third parties through any applications, web sites, products or services that we do not control or own, such as Facebook, or any third-party features or services made available via the Application or the Services.

PLEASE READ THIS PRIVACY POLICY CAREFULLY. BY INSTALLING AND/OR USING THE APPLICATION AND/OR SERVICE, YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS DESCRIBED HEREIN AND ALL TERMS AND CONDITIONS INCORPORATED BY REFERENCE. IF YOU DO NOT AGREE TO ALL THE TERMS AND CONDITIONS SET FORTH BELOW, YOU MAY NOT USE THE LIONMOBI APPLICATIONS AND/OR SERVICES.

Privacy Policy

Last modified: Sep 21, 2017

This Privacy Policy is meant to help you understand:

- what data we collect and why we collect that information.
- how the data we collected is used and shared.
- information security.
- international users
- sensitive information
- changes to this Privacy Policy.

We've tried to keep the Policy simple, but if you have any questions on the privacy or our privacy practices, or to report any violations of the Policy or abuse of the Applications or the Services, please feel free to contact us via email: contact@lionmobi.com.

What Information We Collect ?

We collect personal information to implement significant features and provide you better experience. This information includes:

- **Device Information.** We collect device-specific information (such as your hardware manufacturer & model, operating system version, screen size, CPU model, unique device identifiers, mobile network information and installed apps) to implement app features, provide our services, and improve the app performance for all our users.
- **App Usage Data.** We collect usage data includes information relating to the behavior and/or the habit when you are using the app to analyze and improve the user experience. We do not collect the content you may transmit or share within the app.
- **Google Advertising ID.** Google Advertising ID by Google Play Service for advertising is used in the third-party advertising network to provide personalized advertisements and prevent inappropriate advertisement content for you.
- **Photo in Gallery.** We access your device gallery to implement features (such as duplicate photo remover).
- **Camera Access.** We only access your device camera when using app features Flashlight or getting camera resolution.
- **Aggregate Information.** We collect about a group or category of services or users, which means information on how you use the Applications and the Services may be collected and combined with information about how others use the Applications and the Services.
- **Malicious App.** We collect Information about malicious applications, files and other potential threats on your tablet, mobile phone or other applicable device and their behaviors and origins.We collect there information to better understand how you access and use our antivirus service, We do not sell, trade, or transfer to outside parties your personally identifiable information.

How We Use Information We Collect ?

We use the information we collect from our applications and services to provide you better features and experience on them. We also use the data to measure the performance and improve the apps and services.
We do not sell, trade, or otherwise transfer to outside parties your personally identifiable information.

Opt-out of personalized advertising.

To show you personalized advertisements in our apps we use specific advertising networks and their partners to deliver advertisements that are tailored to you based on a determination of your characteristics or interests. To do so they use personal and non-personal information such as advertising identifiers, such as the Android advertising ID, and/or other tracking technologies to enable and optimize this advertising procedure.
You can opt-out from personalized advertisement experience, at any time by checking the privacy settings of your Android device and selecting "opt-out of interest-based ads" (Android). When you choose to opt-out, advertising networks will consider this choice as a withdrawal of consent to personalized advertisement experience and they will show only non-personalized advertisements and not targeted advertisements based on your interests.

Information Security

We work hard to protect your information from unauthorized access by providing administrative, technical, organizational, physical, electronic, and procedural safeguards and taking risk management measures in accordance with applicable laws to ensure your data is adequately protected against accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure, or access, use, and all other unlawful forms of processing of your data in our possession. We restrict access to personal and/or sensitive data only to highly related employees, contractors and agents who need to know that information for operation, development and/or improvement purposes. Please be aware that, although we endeavor to protect the information we collect and store, no security system guarantees absolute safety.

International Users

Your personal information may be stored and processed in any country where we have facilities, and by using the Applications or the Services you consent to the transfer of your personal information to countries, which may be outside of your country of residence and may provide for different and less stringent data protection rules than in your country. If you object to your personal information being transferred or used as described in this Policy, please do not use the Applications or the Services and immediately delete the Applications from your Devices.

Sensitive Information

We ask that you do not send us, and you do not disclose, any sensitive personal information (e.g., information related to racial or ethnic origin, political opinions, religion or other beliefs, health, sexual orientation, criminal background or membership in past organizations, including trade union memberships) on or through the Application or the Services or otherwise to us.

Changes to This Privacy Policy

Our Privacy Policy may change from time to time. We do not reduce your rights under this Privacy Policy without your explicit consent. We will post any privacy policy changes on this page and, if the changes are significant, we will provide a more prominent notice. We will also keep prior versions of this Privacy Policy in an archive for your review.

EXHIBIT 3

Power Clean - Antivirus & Phone Cleaner App

Sponsored ·

Install this application, delete junk files and viruses now. Keep your phone safe!

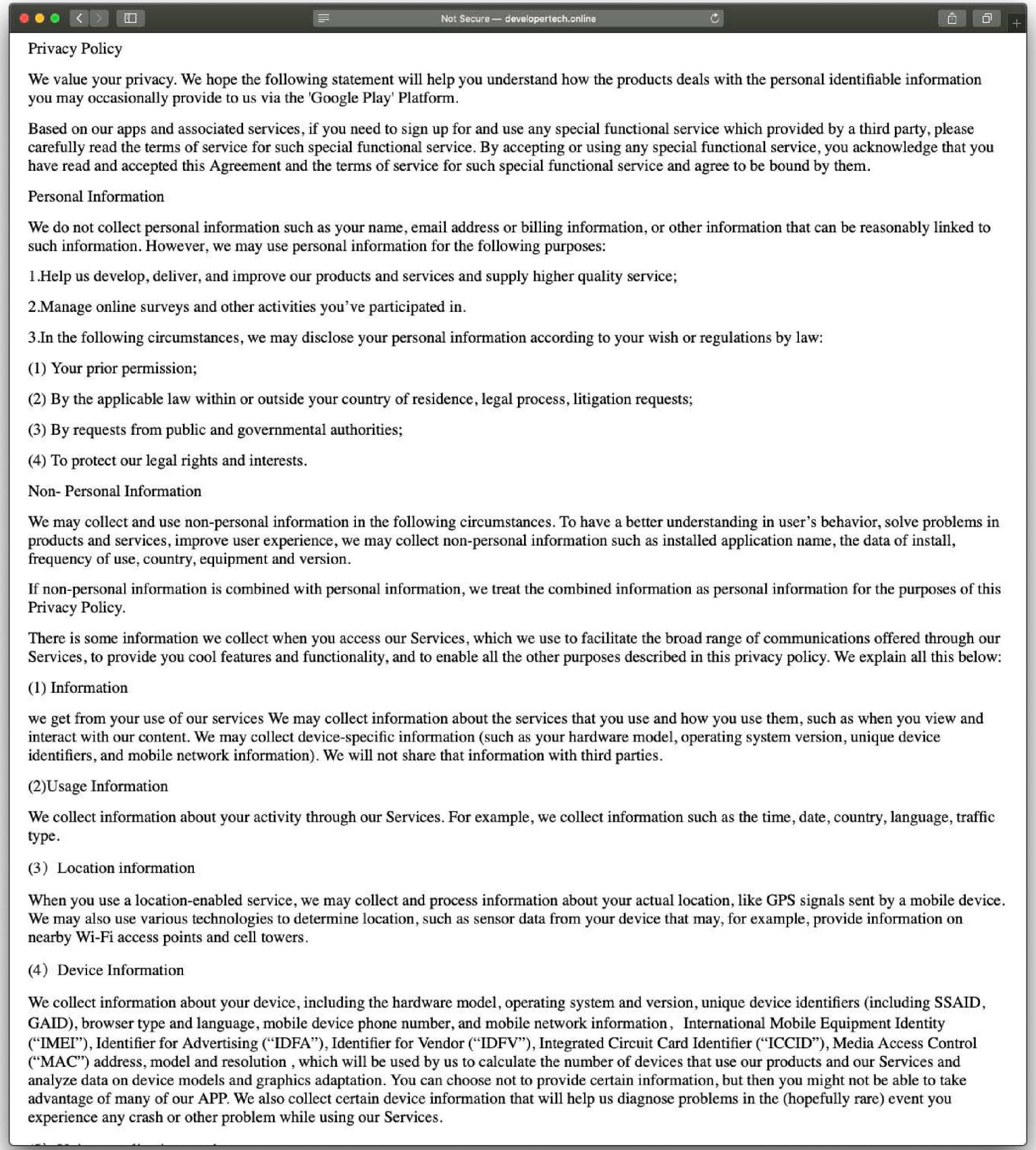
Power Clean - Antivirus & Phone Cleaner App Install Now

45K 652 Comments 1.1K Shares

Like Comment Share

EXHIBIT 4

06/27/19 - Screenshot of Privacy Policy for Calculator Plus - http://www.developertech.online/ca4/policy.html



Privacy Policy

We value your privacy. We hope the following statement will help you understand how the products deals with the personal identifiable information you may occasionally provide to us via the 'Google Play' Platform.

Based on our apps and associated services, if you need to sign up for and use any special functional service which provided by a third party, please carefully read the terms of service for such special functional service. By accepting or using any special functional service, you acknowledge that you have read and accepted this Agreement and the terms of service for such special functional service and agree to be bound by them.

Personal Information

We do not collect personal information such as your name, email address or billing information, or other information that can be reasonably linked to such information. However, we may use personal information for the following purposes:

1.Help us develop, deliver, and improve our products and services and supply higher quality service;

2.Manage online surveys and other activities you've participated in.

3.In the following circumstances, we may disclose your personal information according to your wish or regulations by law:

(1) Your prior permission;

(2) By the applicable law within or outside your country of residence, legal process, litigation requests;

(3) By requests from public and governmental authorities;

(4) To protect our legal rights and interests.

Non- Personal Information

We may collect and use non-personal information in the following circumstances. To have a better understanding in user's behavior, solve problems in products and services, improve user experience, we may collect non-personal information such as installed application name, the data of install, frequency of use, country, equipment and version.

If non-personal information is combined with personal information, we treat the combined information as personal information for the purposes of this Privacy Policy.

There is some information we collect when you access our Services, which we use to facilitate the broad range of communications offered through our Services, to provide you cool features and functionality, and to enable all the other purposes described in this privacy policy. We explain all this below:

(1) Information

we get from your use of our services We may collect information about the services that you use and how you use them, such as when you view and interact with our content. We may collect device-specific information (such as your hardware model, operating system version, unique device identifiers, and mobile network information). We will not share that information with third parties.

(2)Usage Information

We collect information about your activity through our Services. For example, we collect information such as the time, date, country, language, traffic type.

(3) Location information

When you use a location-enabled service, we may collect and process information about your actual location, like GPS signals sent by a mobile device. We may also use various technologies to determine location, such as sensor data from your device that may, for example, provide information on nearby Wi-Fi access points and cell towers.

(4) Device Information

We collect information about your device, including the hardware model, operating system and version, unique device identifiers (including SSAID, GAID), browser type and language, mobile device phone number, and mobile network information， International Mobile Equipment Identity ("IMEI"), Identifier for Advertising ("IDFA"), Identifier for Vendor ("IDFV"), Integrated Circuit Card Identifier ("ICCID"), Media Access Control ("MAC") address, model and resolution , which will be used by us to calculate the number of devices that use our products and our Services and analyze data on device models and graphics adaptation. You can choose not to provide certain information, but then you might not be able to take advantage of many of our APP. We also collect certain device information that will help us diagnose problems in the (hopefully rare) event you experience any crash or other problem while using our Services.

("MAC") address, model and resolution , which will be used by us to calculate the number of devices that use our products and our Services and analyze data on device models and graphics adaptation. You can choose not to provide certain information, but then you might not be able to take advantage of many of our APP. We also collect certain device information that will help us diagnose problems in the (hopefully rare) event you experience any crash or other problem while using our Services.

(5) Unique application numbers

Certain services include a unique application number. This number and information about your installation (for example, the operating system type and application version number) may be sent to us when you install or uninstall that service or when that service periodically contacts our servers, such as for automatic updates.

(6) Camera and Photos

Many of our Services require us to collect images and other information from your device's camera and photos. We'll access your camera and photos only after you give us your consent. You can choose not to provide it, but then you might not be able to take advantage of many of our Services.

How We Use Information

We collect user information and personal details so that we can provide our products and our Services to you and ensure our compliance with relevant laws. We will use your user information and personal details collected under "The Information We Collect" for the following purposes:

(1) Services To provide, process, maintain, improve and develop our Sites and/or our Services provided to you, including customer support, and other services provided through our devices or our Sites.

(2) Statistical analysis To develop and analyze statistics on the use of our products and our Services for the purpose of improving our products and our Services.

(3) To facilitate your use of forums Your personal details may be used when we display your profile, when you interact with other users and when you publish forum posts.

(5) To provide location-based services When you use our Services, we or third-party service providers may take advantage of your location information to provide you with the correct version of our Services and improve your user experience.

(6) To improve user experience Certain optional features such as user experience programs allow to analyze data regarding the use of our products and our Services and improve user experience.

(5) Personalize the Services by providing advertisements, content, or features that match user profiles or interests; if you do not want to receive any personal-interested ads or content, you can choose to adjust the setting;

Changes

Our Privacy Policy may change from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We will post any Privacy Policy changes on this page and, if the changes are significant, we will provide a more prominent notice (including, for certain services, email notification of Privacy Policy changes.

Contact Us

If you have questions about the privacy aspects of our applications or would like to make a complaint, please contact us via contact@jedimobi.com