TUCKER ELLIS LLP
David J. Steele - SBN 209797
david.steele@tuckerellis.com
Howard A. Kroll - SBN 100981
howard.kroll@tuckerellis.com
Steven E. Lauridsen - SBN 246364
steven.lauridsen@tuckerellis.com
515 South Flower Street
Forty-Second Floor
Los Angeles, CA 90071
Telephone: 213.430.3400
Facsimile: 213.430.3409

Attorneys for Plaintiff,
FACEBOOK, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

FACEBOOK, INC., a Delaware corporation, Plaintiff, v. GLEB SLUCHEVSKY and ANDREY GORBACHOV, Defendants.	Case No. 19-1277 **COMPLAINT FOR:** **(1) COMPUTER FRAUD AND ABUSE ACT (18 U.S.C. § 1030);** **(2) CALIFORNIA COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT (Cal. Penal Code § 502);** **(3) BREACH OF CONTRACT; AND** **(4) FRAUD** **DEMAND FOR JURY TRIAL**

I. INTRODUCTION

1. In 2017 and 2018, Defendants Gleb Sluchevsky and Andrey Gorbachov (collectively, "Defendants") operated fraudulent web applications designed to deceive their users ("the app users") into installing malicious browser extensions ("malicious extensions"). The malicious extensions enabled Defendants to "scrape"[1] information from the app users' social media profiles and inject advertisements when the app users visited different social networking sites, including Facebook. Specifically, Defendants' scraped the app users' publicly viewable profile information (*i.e.* name, gender, age range, profile picture) and private (or non-publicly viewable) list of friends from various social networking sites. Facebook identified Defendants and their scheme through an investigation of malicious extensions and disabled all of Defendants' known Facebook accounts in 2018. In total, Defendants compromised approximately 63,000 browsers used by Facebook users and caused over $75,000 in damages to Facebook. Facebook seeks injunctive and other equitable relief and damages against Defendants.

II. THE PARTIES

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

3. Defendants Gleb Sluchevsky and Andrey Gorbachov are individuals residing in Kiev, Ukraine.

4. Defendants Sluchevsky and Gorbachov, using aliases such as "Elena Stelmah," "Amanda Pitt," and "Igor Kolomiiets," operated at least four web applications called "Supertest," "FQuiz," "Megatest," and "Pechenka" (collectively, the "fraudulent applications"). From 2016 to 2018, these applications were available on publicly available websites associated with several domains, including megatest.online, supertest.name, testsuper.su, testsuper.net, fquiz.com, and funnytest.pro.

5. Defendants were employed by an entity called the Web Sun Group, which offered web development and other technical consulting services. Defendant Sluchevsky represented himself as the founder of Web Sun Group.

[1] In this complaint, the terms "scrape" and "scraping" are used to describe an automated means to collect and extract data from websites. Scraping is sometimes also referred to as "web scraping," "web harvesting," or "data harvesting."

6. At all times material to this action, each Defendant was the agent, servant, employee, partner, alter ego, subsidiary, or coconspirator of and with the other Defendant, and the acts of each Defendant were in the scope of such 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.

III. JURISDICTION AND VENUE

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

8. 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.

9. 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.

10. The Court has personal jurisdiction over Defendants because each Defendant used the Facebook platform and thereby agreed to Facebook's Terms of Service ("TOS"), which, in relevant part, require Defendants to submit to the personal jurisdiction of this Court for litigating any claim, cause of action, or dispute with Facebook.

11. In addition, the Court has personal jurisdiction because Defendants knowingly directed and targeted parts of their scheme at Facebook, which has its principal place of business in California. By personally using Facebook, collecting Facebook user information, Defendants transacted business and engaged in commerce in California. For example, Defendants presence on Facebook included at least 13 Facebook accounts and 13 Facebook pages. Furthermore, Defendants created and marketed malicious extensions on browser stores operated by companies located in Mountain View, California. Facebook's claims arise directly from all of these contacts.

12. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) as the threatened and actual harm to the 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.

IV. INTRADISTRICT ASSIGNMENT

13. 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.

V. FACTUAL ALLEGATIONS

1. Background

A. Background on Facebook

14. 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 September 2018, Facebook had more than 1.49 billion daily active accounts and over 2.2 billion monthly active accounts.

15. Facebook's News Feed is an automated program that feeds different types of content into the users' individualized Facebook home page. Specifically, News Feed constantly updates lists of stories, friends' posts, videos, photos, and advertisements on the users' home pages.

16. To create an account, Facebook requires each user to register with a unique username and password. Registered users can create profiles and make connections on Facebook, including as "friends." Users who "friend" each other on Facebook agree to share posts and other connections. Facebook allows users to segment their friends into discrete lists and set these lists to private, which means they are not publicly viewable.

17. Facebook provides its users with control over how to customize their profiles and how much personal information to include. In addition, Facebook's Privacy Settings provide users with control over how much information is viewable online and to whom. For example, users may choose to share only portions of their profile and keep their list of Facebook friends as "private."

B. Facebook's TOS and Policies

18. Everyone who uses Facebook must electronically 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, including Facebook's Community Standards (available at

https://www.facebook.com/communitystandards/), Platform Policy (available at https://developers.facebook.com/policy/).

19. Facebook's TOS prohibit fake and inauthentic accounts. Section 3.1 of Facebook's TOS requires Facebook users provide accurate information about their identity and prohibits deceptive, misleading, and unlawful conduct. Section 3.1 specifically requires Facebook users to: (a) "Use the same name that [they] use in everyday life;" (b) "Provide accurate information about [themselves];" and (c) "Create only one account (your own)[.]"

20. Section 3.2 of the TOS prohibit use of the platform to do anything "[t]hat is unlawful, misleading, discriminatory or fraudulent," or anything "[t]hat infringes or violates someone else's rights." Section 3.2 also provides that users "may not access or collect data from our Products using automated means (without our prior permission) or attempt to access data you do not have permission to access."

21. Facebook's Community Standards also prohibit users from misrepresenting their identities or misusing their profiles by, for example, "[m]aintaining multiple accounts" or "[c]reating inauthentic profiles." Facebook users also may not "[i]mpersonate others" by "[c]reating a profile assuming the persona of or speaking for another person or entity," or "[e]ngage in inauthentic behavior" such as creating fake accounts, setting up profiles with fake names, or participating in "coordinated inauthentic behavior," defined to include deliberately misleading people "about the origin of content" or "about the destination of links off our services."

22. Section 1 of Facebook's Platform Policy expressly requires that third-party developers "not to "confuse, deceive, defraud, mislead, spam, or surprise anyone."

23. Section 3.3 of the Platform Policy restricts developers from using friend lists for any purpose other than enhancing the app users' experience in the application.

C. The "Facebook Login" Feature for Web Applications

24. "Facebook Login" is a feature available to Facebook users, which lets them log into third-party mobile and desktop applications using their Facebook login credentials. Facebook Login allows users to customize and optimize their online experiences and to create accounts with third-party web applications without having to set multiple usernames and passwords. In turn, these third-party web

applications can use the Facebook Login feature for authentication and to enhance a user's experience on the third-party application.

25. Third-party applications developers create independent web-based mobile and desktop applications. In order to use the Facebook Login feature on their applications, third-party applications developers must have a Facebook account and register a developer account with Facebook. In doing so, they must agree to Facebook's TOS, Community Standards, and Platform Policy.

26. The Facebook Login feature protects Facebook users' credentials and information in several ways. First, when users provide their credentials for the purpose of logging into the third-party application using the Facebook Login feature, those credentials are communicated only to Facebook's servers, not to the servers of the application. Second, before any of the users' public Facebook profile information is sent to the application for verification purposes, the user must first provide consent through a custom dialogue box that asks whether the user wants to share the information that the application has requested. Third, Facebook also monitors applications' use of the Facebook Login feature

D. Internet Browser Extensions

27. Internet browsers, such as the Google Chrome, Opera, and Firefox, are used to access the internet. Internet browsers follow instructions from websites, in computer code, to render and display a website's content for users to see. Websites content is largely delivered in HMTL code. Internet browsers are designed to render the HTML code and display it in images and text for the user's screen.

28. Internet browser extensions are software components that alter a browser's functionality. Browser extensions can be installed to enhance user experience and the functionality of the browser. For example, a browser extension can block pop-up ads.

29. Browser extensions can also be used in illicit ways. Browser extensions can be coded to access to the full array of information available to the browser and its functionalities. For example, a browser extension can be designed to monitor a user's browsing session, manipulate how the contents of visited websites is displayed, and take other unauthorized actions.

30. Browser extensions are available for download by users from online browser stores, which are often managed by the browser developer (*i.e.* Chrome Web Store). In order for a browser extension to install, the user typically must grant permissions for the extension to download and install on their device.

2. Defendants' Unlawful Data Harvesting Operation

A. Overview

31. Between 2016 and 2018, Defendants operated and administered fraudulent third-party applications, that they made available on public websites, to deceive internet users into installing malicious extensions. Through these malicious extensions, Defendants scraped user data from social networking sites, including Facebook. Using the same malicious extensions installed by the app users, Defendants were also able to inject unauthorized advertisements into app users' News Feed and into other views associated with various social networking sites.

32. Defendants' scheme generally proceeded in three steps:

a. *First*, Defendants operated and administered at least four web applications. These applications were available on websites unaffiliated with Facebook and they largely targeted Russian and Ukrainian speakers. These applications offered the Facebook Login feature, as well as similar login features for other social networking sites.

b. *Second*, after the app users logged into the fraudulent applications, Defendants caused the applications to prompt the users to permit notifications on their browsers and directed them to install certain browser extensions available in different browser stores. The app users then installed the malicious extensions, which had been created by Defendants and others operating in coordination with Defendants. As a result of installing the malicious extensions, the app users effectively compromised their own browsers because, unbeknownst to the app users, the malicious extensions were designed to scape information and inject unauthorized advertisements when the app users visited Facebook or other social networking site as part of their online browsing.

c. *Third*, Defendants used their fraudulent apps and compromise of the app users' browsers to scrape users' public profile information (*i.e.* name, gender, age range, and profile picture), their non-publicly viewable list of friends, and to inject advertisements on various social networking sites. When the user visited the Facebook site, Defendants injected advertisements purporting to originate from Facebook into users' News Feeds.

B. Defendants Knowingly and Intentionally Operated the Fraudulent Applications and Malicious Extensions.

33. Between 2016 and 2018, Defendants created and caused to be created Facebook accounts, using aliases such as “Elena Stelmah,” “Amanda Pitt,” “Igor Kolomiiets,” to register as web application developers with Facebook. In doing so, Defendants misrepresented to Facebook: (a) their true identities, and (b) that they agreed to and intended to comply with Facebook’s TOS, Community Standards, and Platform Policy.

34. From 2016 to 2018, Defendants operated and administered at least four applications called “Supertest,” “FQuiz,” “Megatest,” and “Pechenka.” These fraudulent applications purported to offer horoscopes, and character and popularity assessments. These were available on publicly accessible websites unaffiliated with Facebook, and targeted Russian and Ukrainian speakers. Screenshots of some of Defendants’ websites and applications are attached as Exhibits 1-3.

35. Defendants’ fraudulent applications falsely represented, to anyone using the Facebook Login feature, that the user was only granting the applications access to a limited amount of public Facebook profile information. In fact, Defendants knew that the applications were designed to scrape the app users’ public profiles on Facebook and other social networking sites, and to prompt users to install malicious extensions for the purpose of manipulating the users’ browsers and collect the users’ private and non-publicly viewable lists of friends when the app user visited the Facebook site.

36. After users logged into the fraudulent applications, Defendants caused the applications to falsely represent to users: (a) that the malicious extensions were legitimate, and (b) necessary in order for the applications’ notifications to operate. In fact, Defendants knew that the specific malicious extensions contained computer code triggered when the self-compromised app users visited different social networking sites in order to scrape users’ private and non-publicly viewable lists of friends, which had to been shared with the applications.

37. The malicious extensions were programmed to communicate with domains hosted on remote servers located in the Netherlands and controlled by Defendants.

38. Defendants promoted the malicious extensions on at least three official browser stores, which generally required users to consent to the installation but did not include consent to scrape user

information (public or private), inject ads, or otherwise modify their browsing experience when visiting social networking sites.

C. Defendants Used Fraud and Malicious Extensions To Access and Scrape Private User Information and To Insert Advertisements onto Facebook Users' News Feed Without Authorization.

39. In 2017 and 2018, Defendants gained unauthorized access to Facebook protected computers through the app users' compromised browsers. As explain in paragraph 32 above, Defendants gained access to the app users' browsers through malicious extensions which had been installed by the app users on their browsers. Unbeknownst to the app users, the malicious extensions they had installed were programmed to scrape the app users' list of friends when the app user visited the Facebook site and accessed their account. In this sense, Defendants used the compromised app users as a proxy to access Facebook computers without authorization. If the app user did not visit the Facebook site and access their account, the malicious extensions were unable to scrape any data from Facebook.

40. In connection with the malicious extensions, Defendants also used automated scripts in the form of JavaScript files ("scripts") to scrape the app users' list of friends on Facebook. The scripts were stored on the servers located in the Netherlands and hosted on some of the same domains as the fraudulent applications, including megatest.pro, megatest.su, testmega.ru, funnytest.pro, and testsuper.su.

41. The scripts were designed to scrape and exfiltrate the app users' non-publicly viewable list of friends, when the app users visited the Facebook site and access their own account. Specifically, when the app users visited the Facebook site and connected to a Facebook server (a Facebook HTTP server), the Defendants used the malicious extensions to inject scripts into their compromised browsers. The scripts were designed to send commands to Facebook's HTTP servers purporting to originate from the app user and collect their private list of friends. Defendants caused these commands to be sent—unbeknownst to the app users and without Facebook's authorization.

42. Defendants also created scripts designed to scrape non-public information from other social networking sites and hosted them on the same remote servers in the Netherlands.

43. Defendants also used the malicious extensions and scripts to inject advertisements onto the app users' News Feeds without users' knowledge or Facebook's authorization. These injects modified the

content rendered on the users' compromised browsers to include advertisements promoting the fraudulent applications. An example of one of the ads injected by Defendants is attached as Exhibit 4.

D. Facebook's Investigation and Remediation Measures

44. On or about October 12, 2018, Facebook suspended all of Defendants' known accounts, applications, and pages and issued Cease and Desist Letters to Defendants. On or about October 31, 2018, Facebook publicly announced that it had conducted an investigation into malicious extensions that may have been used to access private user information, contacted law enforcement, and provided users with information on how to uninstall browser extensions. In addition to the public announcement, Facebook also contacted browser makers to ensure that the malicious extensions were no longer available in their stores and shared information that could help identify additional malicious extensions potentially available to unwitting users.

45. In total, Facebook estimates it incurred over $75,000 in investigating and remediating Defendant's unlawful conduct.

46. In addition, Defendants' acts interfered with and undermined Facebook's relationship with its users.

47. Defendants' unlawful acts interfered with the integrity of Facebook's platform and services in violation of Facebook's TOS.

FIRST CAUSE OF ACTION

Violations of the Computer Fraud and Abuse Act

18 U.S.C. § 1030 *et seq*.

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

49. Facebook's HTTP servers are protected computers involved in interstate and foreign commerce and communication as defined by 18 U.S.C. § 1030(e)(2).

50. Defendants used fraud, malicious extensions, and Java Script code to knowingly and intentionally access and scrape Facebook's HTTP servers without authorization. Defendants also accessed, without authorization, the compromised users' News Feeds, to run unauthorized ads.

51. Defendants violated 18 U.S.C. § 1030(a)(4) because they knowingly and with intent to defraud accessed Facebook protected computers (Facebook's HTTP servers), by sending unauthorized

commands, through the malicious extensions, which purported to originate from Facebook users. These commands were directed to the Facebook HTTP servers for the purpose of furthering Defendants' fraudulent data harvesting operation, accessing users' News Feed, and obtaining anything of value, including user data and the placement of advertisements on the compromised users' News Feed.

52. Defendants violated 18 U.S.C. § 1030(a)(5)(A) because they 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.

53. Defendants violated 18 U.S.C. § 1030(a)(5)(B) because they intentionally accessed a protected computer without authorization and as a result of such conduct, reckless caused damage to Facebook protected computers.

54. Defendants violated 18 U.S.C. § 1030(a)(5)(C) because they intentionally accessed a protected computer without authorization, and as a result of such conduct, caused damage to Facebook protected computer and a loss.

55. Defendants violated 18 U.S.C. § 1030(b) by conspiring or attempting to commit the violation alleged in the preceding paragraph.

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

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

58. Facebook has no adequate remedy at law that would prevent Defendants from continuing their unlawful scheme. Preliminary and permanent injunctive relief are therefore warranted.

SECOND CAUSE OF ACTION

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

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

60. Through the malicious extensions, Defendants knowingly accessed and without permission used Facebook data and Facebook's HTTP servers in order to both (a) devise and/or execute a scheme to

defraud and deceive; and (b) wrongfully controlled and/or obtain data, all in violation of California Penal Code § 502(c)(1).

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

62. 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 user of Facebook's computers, computer systems, and/or computer networks in violation of California Penal Code § 502(c)(5).

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

64. Defendants knowingly and without permission used the profile of another individual or entity in connection with the sending of one or more electronic messages or posts, thereby causing damage to Facebook's computers, computer systems, and/or computer networks in violation of California Penal Code § 502(c)(9).

65. Pursuant to California Penal Code § 502(e), Facebook is entitled to injunctive relief, compensatory damages, punitive or exemplary damages, attorneys' fees, costs, and other equitable relief, including injective relief as Facebook possesses no adequate remedy at law that would otherwise force Defendants to stop their illegal activities as set forth in this complaint.

THIRD CAUSE OF ACTION

Breach of Contract

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

67. Access to and use of Facebook and services is governed by Facebook's TOS and its related policies.

68. Defendants agreed to and became bound by Facebook's TOS, Community Standards, Platform Policy, and other related policies by virtue of their use of Facebook, Facebook's platform, and various other Facebook services.

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

70. Defendants knowingly, willfully, repeatedly, and systematically breached Facebook's TOS, Community Standards, and Platform Policy.

71. Defendants' past violations of Facebook's TOS, Community Standards, and Platform Policy, have directly and proximately caused and continue to cause irreparable harm and injury to Facebook.

72. When Defendants agreed to and became bound by Facebook's TOS, Community Standards, and Platform Policy, 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 as a result of Defendants' breach.

FOURTH CAUSE OF ACTION

Fraud

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

74. Defendants created fake developer accounts on Facebook using knowingly false information in violation of Facebook's TOS, Community Standards, and related policies. Defendants also falsely represented that they intended to comply with Facebook's TOS, Community Standards, and Platform Policy. As a result of the false information, Defendants gained access to Facebook as a developer. Defendants intended that their misrepresentations would be relied on by Facebook, and Facebook reasonably relied on Defendants' misrepresentations to permit Defendants to access to and use of Facebook's platform.

75. Defendants also knowingly and intentionally deceived Facebook users, through false and misleading claims on the web applications, into installing malicious extensions. Defendants then used the malicious extensions to scrape Facebook users' list of friends by send commands onto Facebook, which were designed to appear as if they came from a legitimate Facebook user and not their compromised browser. Defendants intended that their misrepresentations would be relied on by Facebook, and Facebook reasonably relied on Defendants' misrepresentations to permit Defendants to access the app users' lists of friends available on Facebook HTTP servers.

76. Defendants' fraudulent conduct and Facebook's reliance thereon proximately and directly caused Facebook to suffer significant economic injury. Facebook's reliance on Defendants' misrepresentations was also a substantial factor in causing Facebook's injuries. Defendants have also caused Facebook to suffer irreparable reputational harm for which Facebook has no adequate remedy at law.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff Facebook requests judgment against Defendants as follows:

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

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

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

c. Breached their contracts with Facebook in violation of California law; and

d. Committed fraud on Facebook in violation of California law.

2. That the Court enter a temporary restraining order, preliminary injunction, and permanent injunction enjoining and restraining Defendants and their agents, servants, employees, successors, and assigns, and all other persons acting in concert with or conspiracy with any of them or who are affiliated with Defendants from:

a. Soliciting, storing, and/or using Facebook login information from any current, past, or future Facebook user;

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

c. Creating or maintaining any Facebook accounts in violation of Facebooks TOS;

d. Engaging in any activity that disrupts, diminishes the quality of, interferes with the performance of, or impairs the functionality of Facebook's website; and

e. Engaging in any activity, or facilitating others to do the same, that violates Facebook's TOS, Community Standards, Platform Policy, or other related policy 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 equal to any unjust enrichment enjoyed by Defendants.

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.

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

DATED: March 8, 2019

Tucker Ellis LLP

By: /s/David J. Steele
David J. Steele
Howard A. Kroll
Steven E. Lauridsen

Attorneys for Plaintiff,
FACEBOOK, INC.

Jessica Romero
Michael Chmelar
Stacy Chen
Platform Enforcement and Litigation
Facebook, Inc.

DEMAND FOR TRIAL BY JURY

Plaintiff Facebook, Inc. hereby demands a trial by jury to decide all issues so triable in this case.

DATED: March 8, 2019

Tucker Ellis LLP

By: /s/David J. Steele
David J. Steele
Howard A. Kroll
Steven E. Lauridsen

Attorneys for Plaintiff,
FACEBOOK, INC.