Exhibit 1
to
Declaration of
David A. Straite

Stephen G. Grygiel (*admitted pro hac vice*)
SILVERMAN THOMPSON SLUTKIN WHITE LLC
201 N. Charles Street, 26TH Floor
Baltimore, MD 21201
Tel. (410) 385-2225
Fax (410) 547-2432
sgrygiel@mdattorney.com

Frederic S. Fox (admitted *pro hac vice*)
David A. Straite (admitted *pro hac vice*)
KAPLAN FOX & KILSHEIMER LLP
850 Third Avenue, 14th Floor
New York, NY 10022
Telephone: (212) 687-1980
Facsimile: (212) 687-7714
dstraite@kaplanfox.com

Laurence D. King (206423)
Mario Choi (243409)
KAPLAN FOX & KILSHEIMER LLP
350 Sansome Street, 4th Floor
San Francisco, CA 94104
Tel.: (415) 772-4700
Fax: (415) 772-4707
lking@kaplanfox.com

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

IN RE: FACEBOOK, INC. INTERNET TRACKING LITIGATION

No. 5:12-md-02314-EJD

SECOND AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

PUBLIC REDACTED VERSION

TABLE OF CONTENTS

I. INTRODUCTION

1. On April 22, 2010, defendant Facebook, Inc. ("Facebook" or "Defendant") launched the "Like" button outside of the Facebook domain. Within weeks it became the single most important social plug-in ever created, quickly surpassing Facebook's "Share" button.

2. Less than five weeks after the Like button launch, 50,000 websites had installed it; less than ten weeks after launch, web site consultants were calling it "ubiquitous." By November 2013, Facebook claimed on its developer blog that its Like and Share buttons drove more referral traffic than all other social networks combined. Today, Facebook says that web pages containing the Like button are viewed more than 30 *billion* times each day, and more than 7 million websites now incorporate them. As the *Huffington Post* summed up, the Like button is now "omnipresent."

3. As discussed in more detail below, when a Facebook user logs into his Facebook account, a number of session cookies and tracking cookies are written to the user's browser. When an Internet user visits a webpage with Facebook functionality (including the Like button), Facebook causes the user's browser to send a real-time copy of the referrer URL of the page being viewed, along with whatever Facebook tracking and session cookies are written to the browser, *to Facebook*. The browser sends the data to Facebook regardless of whether the user actually clicks on the Like or Share button or even knows of its existence. This means that 30 billion times a day, Facebook causes computers around the world to report the real-time Internet communications of hundreds of millions of people – including the entire file path of URLs containing sensitive content – to Facebook. When Facebook's session and tracking cookies link the URLs to specific persons, anonymity disappears and Facebook's internet tracking becomes the single most pervasive and grave threat to data privacy today.

4. When a subscriber logs out of Facebook, however, Facebook promises to delete those cookies that contain subscriber's identifying information, such as user ID. This promise was made from the very first day Facebook launched the Like button. From the very first day, however, Facebook broke this promise – logging out did not in fact remove cookies with user IDs, and at times during the Class Period new cookies were written even when subscribers were

logged out. Discovery has revealed that from the very first day, [redacted]. Not until September 26, 2011 after an independent researcher publicly disclosed the problem and after the story was picked up by the *Wall Street Journal,* did Facebook choose to fix the problem.

5. The plaintiffs are four Facebook subscribers whose Internet use was tracked by Facebook between April 22, 2010 through September 26, 2011 (the "Class Period") while logged out of their Facebook accounts. They bring federal and California state law claims on behalf of other similarly-situated Facebook subscribers in the United States (the "Class") arising from Facebook's knowing and unauthorized interception and tracking of users' Internet communications and activity, and knowing and unauthorized access to users' computing devices and web browsers.

6. Plaintiffs Quinn, Davis and Lentz also bring these claims on behalf of a subclass of Facebook subscribers in the United States who used Microsoft's Internet Explorer (the "Subclass") from April 22, 2010 through September 17, 2010. During this period, Internet Explorer protected the privacy of its users by blocking certain tracking cookies of websites that did not adhere to standards set by the "Platform for Privacy Preferences" project, or P3P. Facebook knowingly circumvented P3P's cookie blocking by misrepresenting its privacy policy to Internet Explorer until September 17, 2010 when Facebook finally admitted it did not have a compliant P3P policy.

II. JURISDICTION AND VENUE

7. This Court has personal jurisdiction over Defendant Facebook because Facebook is headquartered in this District.

8. This Court has subject matter jurisdiction over the federal claims in this action, namely the Federal Wiretap Act, 18 U.S.C. § 2511 (the "Wiretap Act") and the Stored Communication Act, 18 U.S.C. § 2701 ("SCA"), pursuant to 28 U.S.C. § 1331.

9. This Court has subject matter jurisdiction over this entire action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because this is a class action in which

the amount in controversy exceeds $5,000,000, and at least one member of the class is a citizen of a state other than California or Delaware.

10. This Court also has supplemental jurisdiction over the state law claims in this action pursuant to 28 U.S.C. § 1367 because the state law claims form part of the same case or controversy as those that give rise to the federal claims.

11. Venue is proper in this District because Defendant Facebook is headquartered in this District. In addition, The Facebook Statements of Rights and Responsibilities in force during the Class Period, which Facebook claims govern the relationship between Facebook and its users, provides for exclusive venue in state or federal courts located in Santa Clara County, California.

III. THE PARTIES

12. Plaintiff Mrs. Perrin Davis ("Davis') is an adult domiciled in Illinois. Davis had an active Facebook account during the entire Class Period.

13. Plaintiff Prof. Cynthia Quinn ("Quinn") is an adult domiciled in Hawaii. Quinn had an active Facebook account during the entire Class Period.

14. Plaintiff Dr. Brian Lentz ("Lentz") is an adult domiciled in North Carolina. Lentz had an active Facebook account during the entire Class Period.

15. Plaintiff Mr. Matthew Vickery ("Vickery") is an adult domiciled in Washington State. Vickery had an active Facebook account during the entire Class Period.

16. Defendant Facebook is a Delaware corporation which maintains its headquarters at 1601 Willow Road, Menlo Park, California 94025. Facebook is a "social network" that permits its members to interact with one another through a web site located at www.facebook.com. By the end of the Class Period, Facebook had approximately 800 million members, of whom 150 million were in the United States. Today, Facebook claims approximately 1.4 billion members.

IV. FACTUAL ALLEGATIONS

A. The Facebook Terms of Service

17. Facebook asserts that the agreement governing its relationship with users is the "Statement of Rights and Responsibilities" or "SSR" which incorporates a number of other

documents by reference. The SSR at the start of the Class Period is dated April 22, 2010, and is attached to this complaint as Exhibit A.

18. Updated SSRs in the Class Period are dated August 25, 2010 (see Exhibit B), October 4, 2010 (see Exhibit C) and April 26, 2011 (see Exhibit D).

19. Each of these SSRs, regardless of date, provides that "[t]he laws of the State of California will govern this Statement, as well as any claims that might arise between you and us, without regard to conflict of law provisions." *See, e.g*., SSR dated April 22, 2010 at ¶ 15, Ex. A.

20. Each of these SSRs incorporated by reference the Privacy Policy (later called the "Data Use Policy" starting April 26, 2011). *See* Exhibits E through H. For example, Facebook said in the SSR "[w]e encourage you to read the Privacy Policy, and to use it to help make informed decisions." SSR dated April 22, 1010 at ¶ 1, Ex. A. At the end, the SSR stated, "The Privacy Policy is designed to help you understand how we collect and use information."

21. The Privacy Policies (and Data Use Policy) are long and difficult to comprehend. A December 8, 2011 inquiry from the United States House of Representatives noted that Facebook's privacy policy was "longer than that of all other social networks and exceed in length the United States Constitution. . . . . We are concerned . . . that long, complex privacy policy statements make it difficult for consumers to understand how their information is being used." *See* Ex. I., p. 8.

22. In its January 6, 2012 response to the Congressional inquiry, Facebook agreed: "We also agree that long and complex privacy policies can make it difficult for consumers to understand how their information is being used . . . . we use a layered approached, summarizing our practices on the front page and then allowing people to click through the Policy for more details." *Id*. at 9.

23. The Privacy Policies and the later Data Use Policy linked to Facebook's Help Page as a part of this "layered approach." One Help Page entry provided more detail related to Facebook's use of cookies, which "are small files that store information about your account, web browser, computer, mobile phone or other device." Facebook also represented in the social plug-

in discussion that "***when you log out of Facebook, we remove the cookies that identify your particular account***."

24. The Privacy Policies dated April 22, 2010 (Ex. E), October 5, 2010 (Ex. F) and December 22, 2010 (Ex. G) link to these representations, contradict none of them, and never purport to obtain consent for Facebook to use account-identifying cookies after logout. In fact, on September 7, 2011 Facebook moved the social-plugin discussion from the Help Center directly into the Data Use Policy, and continued to represent that Facebook would only use User ID cookies when the user is "logged in to Facebook." Ex. H, section I ("Other Information We Receive About You.").

25. The Facebook Privacy Policies as explained by the help pages are consistent with all public representations made by Facebook. For example, four days into the Class Period, on April 26, 2010, Facebook explained social plug-ins on its "Facebook Notes" blog. Facebook was clear that "you only see a personalized experience with your friends if you are logged into your Facebook account."

26. When privacy rights and civil liberties organizations 2010 raised a number of privacy concerns associated with social plug-ins and other changes to the Facebook Privacy Policy at the beginning of the Class Period, it was believed that Facebook was only tracking logged in users via the Like button. So, for example, the ACLU, Center for Democracy and Technology, Center for Digital Democracy, Consumer Action, Consumer Watchdog, Electronic Privacy Information Center, Electronic Frontier Foundation and the Privacy Rights Clearinghouse jointly wrote to Facebook CEO Mark Zuckerberg regarding a number of "outstanding privacy problems." *See* Open Letter dated June 16, 2010, attached as Ex. J. The authors objected that the Like buttons "provide Facebook with information about every visit to the site *by anyone who is logged in to Facebook*." *Id.* at 2 (emphasis added). Not one of these well-respected and tech-savvy privacy groups understood that Facebook was also tracking logged out as well as logged in users, which would have been a far more serious concern.

27. Throughout the entire Class Period and thereafter, Facebook consistently told the public that it was not tracking users post-logout. In a series of interviews with USA Today in

mid-November, 2011, for example, Facebook said it did not log any personal information associated with Internet surfing by logged out users – all logging would be done only by an anonymous browser cookie. When asked if even the anonymous data could somehow be re-associated with the browsing history, Facebook reiterated: "We've said that we don't do it, *and we couldn't do it without some form of consent and disclosure*."[1]

B. URLs Contain the "Contents" of an Electronic Communication

28. To browse the web via the Internet, users employ a web browser. The most popular web-browsers include Apple Safari, Microsoft Internet Explorer, Google Chrome, and Mozilla Firefox.

29. Web browsers are software applications that allow consumers to send, receive and view electronic communications on the Internet and to view the content of web pages. Web browsers include a Terms of Use or Service, which prohibit users from engaging in unlawful or unauthorized tracking of the communications of others or from using the service to engage in criminal or otherwise unlawful acts. For example, major web-browsers such as Google Chrome, Microsoft Internet Explorer, and Apple Safari all expressly prohibit unlawful acts.[2] Plaintiffs are not aware of any major web-browser which consents to the use of its service to engage in criminal or otherwise unlawful acts.

30. Every website is hosted by a server through which it sends and receives communications with Internet users and their web browsers to display web pages on users' monitors and screens, depending on the user's chosen computing device.

31. The basic command to communicate with websites is called the 'GET' command. For example, when an Internet user types a URL into the navigation bar of her web browser and

[1] *See* Acohido, Byron, *How Facebook Tracks you across the Web*, USA TODAY, Nov. 16, 2011. http://www.usatoday.com/tech/news/story/2011-11-15/facebook-privacy-tracking-data/51225112/1.

[2] See https://www.google.com/intl/en_US/chrome/browser/privacy/eula_text.html (last visited July 28, 2014); http://windows.microsoft.com/en-US/internet-explorer/products/ie-9/end-user-license-agreement (last visited July 28, 2014); and http://www.apple.com/legal/sla/docs/SafariWindows.pdf (last visited Sept. 10, 2014).

hits *enter* (or more commonly, when an Internet user clicks on a hyper-link), the user sends a 'GET' command to the server hosting the website to which the user is sending the communication. The 'GET' command instructs the website server to send the content contained within the file the Internet user has requested onto the user's browser for display.

32. Another basic command is the 'POST' command. The 'POST' command is used when a user enters data into a form on a website and clicks *enter* or the submit button. The 'POST' command sends the data entered into the form to the website.

33. Each website server has an IP address. For example, the IP address for the website "www.nytimes.com" is "170.149.161.130." An IP address, however, is not the same thing as a URL. The New York Times website has a single or just a handful of IP addresses for all of the articles, essays, and other content hosted on its webserver. Thus, revealing that an Internet user sent a series of communications to 170.149.161.130 only reveals the parties to the communication – the user and the New York Times. In contrast, a full-string detailed URL reveals both the parties to the communication and the contents of a communication.

34. A URL is composed of several different parts. For example, consider the following URL: http://progressivehealth.hubpages.com/hub/How-Do-I-Reduce-Herpes-Breakouts:

a. **http://** – This is the protocol identified by the web browser to the web server which sets the basic language of the interaction between the browser and the server. The forward-slashes indicate that the browser is attempting to make contact with the server.

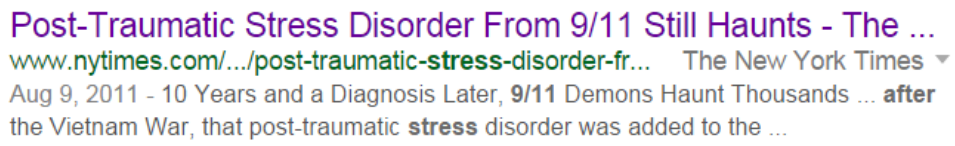
b. **progressivehealth.hubpages.com** – This is the name that identifies the website and corresponding website server with which the Internet user has initiated a communication. There is an IP address associated with the "progresivehealth.com" server.

c. **/hub/** – This part of the URL indicates a folder on the web-server where the communication is located, a file of which the Internet user has requested.

d. **/How-Do-I-Reduce-Herpes/Breakouts/** – This is the name of the precise file requested and it constitutes and/or contains information relating to the substance, purport, and meaning of a communication. The IP address attached to this particular URL would only reveal that the user was in the process of sending and receiving communications from HubPages.com. The full string details URL would reveal the user was interested in, and was seeking and requesting information from HubPages.com about, herpes breakouts and their reduction.

e. **/hub/How-Do-I-Reduce-Herpes-Breakouts** – This combination of the folder and exact file title is called the "file path."

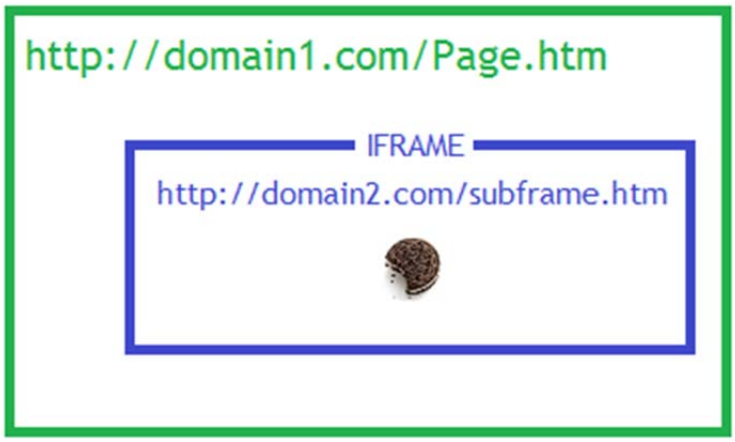
35. To further illustrate the distinction between an IP address and a full-string detailed URL, consider an Internet user seeking information on "stress after 9/11." This user might type that exact search term into Google and the first result they would get is a link to an article on the NYTimes.com website:



The user who clicks on the phrase "Post-Traumatic Stress Disorder from 9/11 Still Haunts" would be sending a communication through the user's browser to the New York Times seeking that information via a 'GET' request and the full-string detailed URL: *http://www.nytimes.com/2011/08/10/nyregion/post-traumatic-stress-disorder-from-911still-haunts.html.* The IP address for the New York Times would be the same whether the user went to NYTimes.com or sent this detailed request for information via a URL. The user would receive in return a 3,000 word article from the New York Times on the topic of Americans suffering from stress a full ten years after 9/11.

36. Although a single webpage appears on a user's screen as a complete product, it is

more often an assembled collage of independent parts. Some portions often exist on different servers, often operated by third parties, which send the additional information to a window called an iframe. In essence, the iframe is a small portion of the third-party's website that peeks through the first-party website, usually in the form of an advertisement or social plug-in:



37. To display each part of a single webpage as one complete product, the host server leaves the iframe blank. Upon receiving a 'GET' command from a user's web browser, the website server contemporaneously re-directs the user's web-browser to send a separate but simultaneous GET command to the third-party responsible for the iframe, thereby allowing the third-parties to gain limited access to the user's web-browsers.

38. In addition to the GET command received by the third-party, the detailed URL from the first domain is acquired by the third-party. These URLs are called "referrer headers" (technically spelled "referer" due to a quirk of history).

39. The re-direction of the referrer URL and the sending of the re-directed GET command is accomplished through the individual Internet user's web-browser without any further action or knowledge of the user.

40. The third-party servers to which the GET requests are contemporaneously re-directed, and which thereby gained access to the user's web-browser, responds by sending information to user's web-browser to fill in the blank iframe.

41. The sending of the re-directed GET request and acquisition of the referrer headers by third-parties occurs both contemporaneously with the user's communications with the first-

party website and while the information is in storage by the first-party website and the user's computing device and web-browser.

42. The entire process happens in milliseconds. The precise length of time from the original 'GET' request from the user to the website and the corresponding communication from the website back to the user is determined by the user's Internet speed and the speed of the website server and server(s) to which the user's referrer URL and GET request was contemporaneously re-directed.

43. Facebook has always understood the sensitivity of content included in referrers, and the privacy concerns associated with referring URLs to another website. One month into the class period, for example, Facebook engineer Matt Jones wrote a blog post called "Protecting Privacy with Referrers." *See* Ex. K. He first noted that Facebook does truly want to track its users across the internet:

> Here at Facebook, we're all about understanding how people interact with our site – including how they end up here from across the vast expanse of the internet. We're not the only ones, though – most web sites want similar insights about the people who use them.
>
> Despite its tragic misspelling, the HTTP standard's "referrer" header sent by browsers gives websites the information they need to see how users found them, and how they explore the sites once there.

44. Then under the heading "Referrers: not always welcome," Mr. Jones added:

> But sometimes referrers just don't belong – maybe there is sensitive information in a URL, or maybe a site just doesn't want its users' browsers telling others how they use the site. . . . ***Facebook is one site where referrers don't really belong*** . . .

Id. (emphasis added).

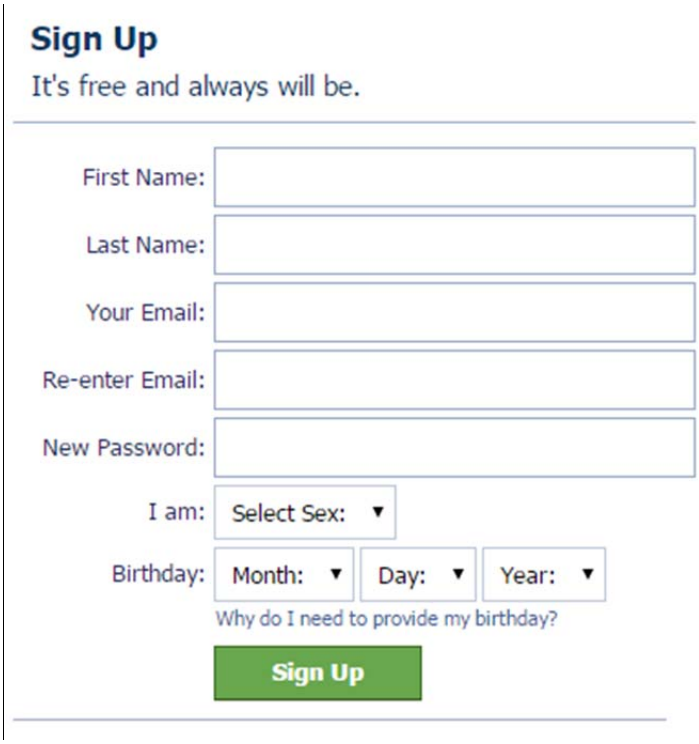
45. Similarly, at the beginning of the Class Period, Facebook met with representatives of [redacted] regarding [redacted] possible integration of Like buttons. Facebook employee Matt Kelly recorded that [redacted] wanted to use a version of the button that would provide greater privacy to its users; Mr. Kelly noted "[redacted]" In response, Facebook employee Ethan Beard noted the challenge of [redacted] request, and proposed an alternative "[redacted]

[redacted]." *See* Ex. Q at p. 1.

C. Internet Tracking Through the Facebook "Like" Button

1. *Tracking Logged-In Subscribers*

46. When signing up for a Facebook account, subscribers fill out an electronic form, sending communications to Facebook which personally identified them:



47. Each Facebook subscriber manually enters his or her first and last name, email address, a password, gender and birthdate before signing-up. Upon clicking the green "Sign Up" button, their web-browser sent a 'POST' communication to Facebook.

48. Facebook then creates a database entry for the new user in an internal database called [redacted] and assigned a unique user ID to the subscriber. Facebook also then writes a number of cookies to the user's web browser that Facebook correlates with the information in the [redacted] database. As each user adds more information to their Facebook account via communications while logged-in to Facebook, Facebook adds the information to the database entry for each user.

49. Facebook describes its social plug-ins as a "little piece of Facebook" embedded on a first-party website, as described above. When an internet user lands on a webpage with this embedded piece of Facebook, the user's browser is instructed to redirect a copy of the user-to-website communications, along with several Facebook cookies, to Facebook, which can then be added to the [redacted] database. The adoption rate and growth of Facebook social plug-ins, most importantly the Like button, has been historic:

a. By the beginning of June 2010, just weeks after launch, more than 50,000 websites incorporated Like buttons.

b. By August 2010, more than 350,000 websites had Like buttons.

c. By the one-year anniversary on April 22, 2011, 2.5 million websites had Like buttons, including 80 of the top 100 websites in the United States ranked by comScore. 250 million people each day were viewing websites with Like buttons.

50. The process differs for logged-in users compared to logged-out users and non-subscribers, and is described in detail in the attached Technical Report recently prepared for the Belgian Privacy Commission on June 25, 2015. *See* Ex. L.

51. When a Facebook subscriber is logged into Facebook, the users' browser will contain more than 10 Facebook cookies, written to the browser at various times.

52. Cookies are small text files that web-servers can place on a person's web-browser and computing device when that person's web-browser interacts with a website server. Cookies can perform different functions. Eventually, some cookies were designed to track and record an individual Internet user's communications with and activities on websites across the Internet.

53. In general, cookies are categorized by (1) duration and (2) party. There are two types of "duration" cookies, known as session cookies and persistent cookies.

54. "Session cookies" are placed on a person's computing device only for the period during which the user is directly communicating with the website that placed the cookie. The person's web-browser normally deletes session cookies when the user closes the browser.

55. "Persistent cookies" are designed to survive beyond a single browsing session. Persistent cookies are not permanent. Instead, the party creating the persistent cookie determines

its lifespan – which is longer than a single browsing session. A "persistent cookie" can record a person's Internet communications for months or years. By virtue of their lifespan, persistent cookies can track a person's communications with dozens, hundreds, or thousands of websites on the Internet. Persistent cookies are also sometimes called "tracking cookies."

56. Cookies can also be classified by "Party." "First-party cookies" are set on a user's web-browser by the website with which the user is knowingly communicating. For example, NYTimes.com sets a collection of its own first-party cookies on user's web-browsers when they visit pages at NYTimes.com. First-party cookies can be helpful to the user, server, and website to assist with security, log-in, and functionality.

57. "Third-party cookies" are set and accessed by website servers other than the website with which the user is knowingly communicating. For example, the same user who visits NYTimes.com will also have cookies placed and accessed from their web browser by third-party web-servers, including Facebook. Unlike first-party cookies, third-party cookies are typically not helpful to the Internet user. Instead, third-party cookies typically work in furtherance of data collection, behavioral profiling, and targeted advertising.

58. Facebook writes the following cookies to the browsers of logged-in users; the sample values below relate to an actual test in 2015 using Mozilla's Firefox browser:

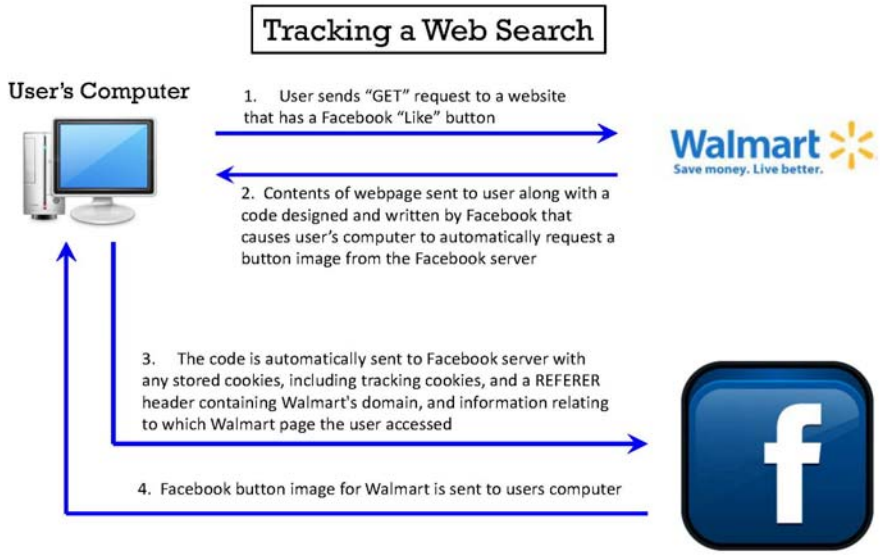
Cookie	Sample Value	Information Contained	Expires
c_user[3]	10000004223456398	User's Facebook ID	Session / 1 month
datr	S3fJVgeTh7_ikK5frtHsHPmE	Browser ID	2 years
fr	0glRJJKaszKOLdKz8.AWXGH1RrxSLM3PHeHxfrORv10H8.BCVchV.Sj.FUJ.0.AWWsuv8a	Encrypted Facebook ID plus browser ID	1 month
lu	wfKm8ItfbXqRKlNoERo10H1H	Encrypted ID of the last user	2 Years
p	-2	User's channel partition	Session
presence	EM426705095EuserFA21B0911298286A2EstateFDutF1426705095426Et2F	Chat state	Session
s	Aa67DZudqH2wPH19	?	Session /1 month
xs	244%3AjIZKp45fK9ceMA%3A%3A1426705088%3A3455	Session number and secret	Session / 1 month

[3] During the Class Period, Facebook used several cookies to identify users, including the a_user, c_user, and m_user cookies.

csm	2	Insecure indicator	Session / 1 month
act	1426704200575%2F14	Timestamp and counter of user actions	Session
wd	1280X653	Browser window dimensions	Session

59. Several of these cookies can identify the subscriber. Certainly the c_user cookie, which is the user ID, identifies the subscriber because Facebook assigned that ID to the user upon creating an account. But at least two other cookies can also uniquely identify the user. For example, the fr cookie has the user ID (encrypted) included therein. The lu ("last user") cookie contains the user ID (encrypted) of the last user to use that browser, which would precisely identify the current user if the computer is not a shared computer. Internal Facebook documents confirm that [redacted]. *See, e.g.*, Ex. V, at p. 5 ("[redacted]"). Finally, Facebook assigns each browser a unique identifier (the datr cookie) which can and do identify actual current users when a computer is not a shared computer. [redacted] *See* Ex. Y, p. 1.

60. When a logged-in subscriber visits a webpage with a Facebook Like button, a copy of the referrer URL is acquired by Facebook along with the cookies above. However, Facebook is not a party to the communication recorded in the referrer URL – instead it acquires the URL from the user. For example, if a logged-in Facebook subscriber visited www.walmart.com, the series of conversations among computers would look like this:



61. Even for an ostensibly innocuous page view – say, perhaps hand towels at Walmart – Facebook acquires an enormous amount of individualized data. Facebook gets the full referral URL (including the exact subpage of precise items being purchased), and through the use of cookies, correlates that URL with the user ID, time stamp, browser settings and even the type of browser used. Facebook not only receives a copy of the user's communication with Walmart, but can put the communication in the precise context of time of day and other user actions on the same website.

62. No matter how sensitive the website, the referral URL is acquired by Facebook along with the cookies that precisely identify the user. As the researchers noted in the Belgian Technical Report, if a user visited a certain explicit page of the gay website www.gayworld.be, Facebook would receive all of the cookies identified above, including time stamp and user ID, along with this referrer: http://www.gayworld.be/holebi-cultuur/wereldwijd/belgie/. *See* Ex. L, Fig. 7, Section 5.1.

2. *Tracking Logged-Out Subscribers*

63. When a subscriber logs out of his or her Facebook account, from the beginning of the Class Period until today Facebook has always represented publicly that it only receives "technical information" about user communications with other websites; when users "log out of Facebook, we remove the cookies that identify your particular account."

64. Thus, upon logout Facebook deletes the c_user cookie completely, and sets the lu cookie value to zero. Facebook still acquires substantial amounts of data when a logged out user visits a webpage with Facebook functionality – including referrer URLs – and sets a new cookie called "locale," which is the location of the last user to use that browser.

65. Facebook also records the unique browser ID of the browser used (via the datr cookie), and it appears from the Belgian Technical Report that the fr cookie also remains, despite containing the encrypted user ID. Discovery is still ongoing and it is not yet clear precisely how Facebook uses the datr cookie and/or the fr cookie to associate referrer URLs with actual users.

66. Finally, the "presence" cookie describes the "chat state," for example, which chat tabs are open. Although not mentioned by the Belgian Technical Report, [redacted]. Thus, for example, Facebook engineering director Alex Himel assigned [redacted] to engineer Adam Wolff on January 27, 2011, during the Class Period:

[redacted]

See Ex. M.

67. Discovery is ongoing and it is not yet clear to what extent Facebook [redacted] during the Class Period.

D. Facebook Unlawfully Tracked Logged-Out Subscribers

68. As soon as the Like button was rolled out on April 22, 2010, Facebook found it had a problem - a large number of users were logging out of their accounts prior to surfing the web. Facebook product manager Austin Haugen noted in an internal email dated October 28, 2010, "[redacted]" *See* Ex. N at p. 1. A few months later, after reviewing detailed cookie data, Mr. Haugen determined that only approximately "[redacted]" *See* Ex. O at p. 4.

69. The genesis for these discussions was pressure coming directly from [redacted]. In an email dated September 21, 2010, Mr. Haugen wrote: "[redacted]." *See* Ex. P at p. 2.

70. Facebook came up with an easy but unlawful interim solution: simply break Facebook's promise to stop tracking users post-logout. This was done both by failing to delete cookies containing user IDs (such as c_user, lu and fr) [redacted].

71. Facebook's deception was noticed by some investigators who alerted Facebook. The first was [redacted], who wrote the following in an email to Facebook spokesman Andrew Noyes on June 4, 2010, just 6 weeks after the launch of the Like button outside the Facebook domain:

[redacted]

Ex. R, bates numbers 7472-73. Evidently a flurry of activity within Facebook ensued, but subsequent emails have been redacted. *See id*., bates numbers 7469-72. In any event, Facebook continued to track users post-logout.

72. The next day, June 5, 2010, a task was created called "[redacted]." Facebook engineering director Alex Himel commented, "[redacted]." *See* Ex. S.

73. On June 7, 2010, Mr. Himel created a task with the tag "[redacted]" and assigned it to engineer Chuck Rossi. The task noted:

[redacted]

See Ex. T.

74. In the following month in July 2010, Mr. Himel "[redacted]" but noted in an August 19, 2010 email that changes still had not been made:

[redacted]

Ex. U.

75. After Mr. Himmel's email above, [redacted]. No attempt was made to delete user-

identifying cookies post-logout. These include any of the user cookies (for example, a_user, c_user), the fr cookie, and the lu cookie. This distinction was [redacted] on February 7, 2011: "[redacted]." *See* Ex. V (emphasis added).

76. Occasionally during the class period, [redacted]. For example, on January 28, 2011 Alex Himmel noted that [redacted]." *See* Ex. W. An unknown Facebook employee responded, "[redacted]"

77. No attempt was made to correct the false statements Facebook made publicly about tracking logged-out users, and communications with partners and customers were equally misleading. The internal emails on this point are revealing. For example, on February 2, 2011, Facebook partner [redacted] emailed Aimee Westbrook at Facebook to report that they might be willing to adopt the Like button. They noted, "[redacted]" *See* Ex. X, pp. 2-3. Alex Himel internally crafted a response which represented the data collected from logged in users, and then for logged out users he simply said "[redacted]" This statement was only five days before Mr. Himel noted the opposite internally: "[redacted]" upon logout. *See* Ex. V, discussed above.

78. Two weeks later, on February 19, 2011, Facebook employee Douglas Purdy drafted a table "[redacted]" which only listed [redacted] for logged out users. *See* Ex. Y. Facebook engineer Matt Jones made a number of revisions and comments, and said "[redacted]

[redacted]" *Id* at 2 (emphasis added). Alex Himel concluded by saying:

[redacted]

See Ex. Y at 1.

79. At exactly the same time, three Facebook employees filed a patent application (later assigned to Facebook), facilitating the post-logout tracking of Facebook users on other domains.

80. On February 8, 2011, Kent Matthew Schoen, Gregory Luc Dingle and Timothy Kendall (Facebook's "Director of Monetization") filed a patent application entitled "Communicating Information in a Social Network System about Activities from Another Domain."[4] As the first claim in the Patent Application explains, the applicants were seeking to patent:

> 1. A method for tracking information about the activities of users of a social networking system while on another domain, the method comprising: maintaining a profile for each of one or more users of the social networking system…; receiving one or more communications from a third-party website having a different domain than the social network system, each message communicating an action taken by a user of the social networking system on the third-party website; logging the actions taken on the third-party website in the social networking system…; and correlating the logged actions with one or more advertisements presented to one or more users.

Patent Application at 2.

81. The detailed description of this tracking method reveals that it enables Facebook to capture and log actions taken by Facebook users on websites other than Facebook, ***even when the user is not logged in:***

> [0054] As described above, in particular embodiments, the social network system 100 also logs actions that a user takes on a third

[4] *See* U.S. Patent Application No. 20110231240, filed February 8, 2011 and published September 22, 2011 (the "Patent Application") at 1.

> party website 140. The social network system 100 may learn of the user's actions on the third party website via any of a number of methods. In particular embodiment, in response to certain actions such as, a user registering with a third-party website140, purchasing a product from a third-party website 140, downloading a service from a third-party website 140, or otherwise making a conversion, the third-party website 140 transmits a conversion page, such as a confirmation or "thank you" page to the user at the user's client device. In particular embodiment, this page includes an embedded call or code segment (e.g., JavaScript) in the HTML or other structured document code (e.g., in an HREF(Hypertext REFerence) that, in particular embodiments, generates a tracking pixel that, when executed by the client's browser or other rendering application, generates a tracking pixel or image tag that is then transmitted to the social network system ***(whether the user is logged into the social network system or not).*** The tracking pixel or image tag then communicates various information to the social network system about the user's action on the third-party website. By way of example, the tracking pixel or call may transmit parameters such as the user's ID (user ID as registered with the social network system), a product ID, information about the third-website, timestamp information about the timing of the purchase or other action, etc. In one example, if the third party website 140 is a commercial website on which users may purchase items, the third party website 140 may inform the social network system 100 in this manner when a user of the social network system 100 buys an item on the third party website 140.

Patent Application at 5.

82. Further, in certain circumstances, Facebook has to hack its way past data protection software to do this: Facebook deposits a cookie that deliberately and without a user's consent bypasses security settings on the user's browser for the purpose of gathering intelligence as to what the user does on the internet in real time, such as what sites are visited, whether purchases are made, or whether information is downloaded or a link forwarded to a friend. This information is then instantly relayed back to Facebook, substantially enhancing the value of Facebook's vast repository of personal data. This is all done whether the Facebook user is logged onto Facebook *or logged off*.

83. Technically, this is how the Patent Application describes the bypass:

> [0099] In one embodiment, the third party website 140 and/or the social network system 100 determine whether the user is a user of the social network system 100. For example, the third party website 140 may access a cookie on the user's computer, where the cookie is associated with the social network system 100. Since the social network system 100 and the third party website 140 are on

> different domains, the user's browser program may include security features that normally prevent a website from one domain from accessing content on other domains. To avoid this, the third party website 140 may use nested iframes, where the third party website 140 serves a web page that includes a nested iframe in the social network website's domain, thereby allowing the nested iframe to access the user information and send the information back to the third party website 140. Repeated nesting of iframes further allows the social networking site 100 to communicate information back to the third party website 140. By using this technique, the third party website 140 and the social network system 100 can communicate about the user without sharing any of the user's personal information and without requiring the user to log into the social network system 100.

Patent Application 10-11.

84. Although Facebook's name does not appear in the Patent Application, it is listed in the U.S. Patent & Trademark Office database as assigned to Facebook. Tellingly, Mr. Kendall, Facebook's "Director of Monetization," is not an inventor or a computer scientist at all. According to his LinkedIn profile, Mr. Kendall's job at Facebook is "Product Strategy & Development for Facebook's revenue generating products." Essentially, Mr. Kendall is charged with figuring out new and better ways to sell user information to advertisers and third-party websites.

E. Facebook Unlawfully Circumvented P3P Privacy Protections on Internet Explorer

85. During the Subclass Period, Internet Explorer 6, 7 and 8 by default blocked certain cookies from websites that did not honor a privacy system called the Platform for Privacy Preferences Project (P3P). During the Subclass Period, Facebook circumvented this privacy protection by falsely representing its privacy policy to the browser.

86. P3P is a standard format for computer-readable privacy policies, which the World Wide Web Consortium (W3C) published in 2002. The standard includes a P3P full policy format and a P3P "compact policy" ("CP") format. The compact policy format is designed to be a shorter version of a full P3P policy that encodes in a computer-readable format only the parts of a privacy policy that relate to cookies. Use of a compact policy is optional for websites that use

P3P full policies. However, according to the P3P working group, "if a web site makes compact policy statements it MUST make these statements in good faith."[5]

87. The compact policy is designed to be transmitted in an HTTP header that also contains an HTTP cookie. It takes the form: CP = "POLICY" where POLICY is a series of three- and four-letter tokens associated with P3P policy elements as defined in the P3P 1.0 Specification.[6] Valid compact policies must have at least five of these elements. For example, the following is a valid P3P compact policy:

CP = "NOI NID ADMa OUR IND UNI COM NAV"

88. The P3P specification states "If an unrecognized token appears in a compact policy, the compact policy has the same semantics as if that token was not present."[7] This means that web browsers should ignore any tokens that appear in a P3P compact policy that are not defined in the P3P specification.

89. Microsoft introduced support for P3P in the Internet Explorer 6 web browser in 2002; and Microsoft included functionally identical implementations of P3P in its subsequent Internet Explorer 7, 8, and 9 web browsers (hereinafter, Internet Explorer versions 6-9 are all called "IE"). By default, without users taking any action to change configuration settings, IE is set to the "Medium" privacy setting. Users can view and change their privacy settings using the IE "Internet Options" panel. The panel describes the Medium setting as follows:

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

[5] W3C. The Platform for Privacy Preferences 1.1. http://www.w3.org/TR/P3P11/, November 2006.

[6] W3C. The Platform for Privacy Preference 1.0 (P3P1.0) Specification, W3C Recommendation 16 April 2002, http://www.w3.org/TR/P3P/.

[7] P3P1.0 at Section 4.2.

90. Microsoft documentation states, "For most users, Internet Explorer 6 default privacy settings provides enough privacy protection without disrupting the browsing process."[8]

91. Behind the scenes, IE checks for a P3P compact policy header whenever a website sends a cookie in an HTTP response. If IE finds a third-party cookie that is not accompanied by a compact policy, IE blocks that cookie. If IE finds a first-party cookie that is not accompanied by a compact policy, it "leashes" that cookie and prevents that cookie from being transmitted in a third-party context. If IE finds an accompanying compact policy, it evaluates that compact policy, and blocks the cookie if the compact policy is found to be "unsatisfactory." If IE finds a first-party cookie that is accompanied by a compact policy, it evaluates that compact policy and turns the cookie into a session cookie if the compact policy is found to be unsatisfactory. IE considers a cookie to be unsatisfactory if the corresponding compact policy indicates that the cookie is used to collect personally identifiable information and does not allow users a choice in its use.

92. By blocking cookies on the basis of their P3P compact policies, as described above, the IE default privacy settings allow users "to enjoy the benefits of cookies, while protecting themselves from unsatisfactory cookies."

93. At all relevant times, IE treated the representations made in compact policies as truthful statements. The software makes no attempt to verify the accuracy of the information in a compact policy. If a website with an unsatisfactory privacy policy were to make an untruthful statement and misrepresent its policy as a satisfactory one, it could trick IE into allowing its third-party cookie to be set when it would otherwise be blocked.

94. Websites can also trick IE into allowing their third-party cookies to be set without making affirmatively false statements. Because of the way Microsoft implemented the P3P compact policy feature, websites can trick IE by simply omitting any compact policy tokens that would lead IE to classify the compact policy as unsatisfactory. In fact, an invalid compact policy that contains only a made-up word is classified by IE as satisfactory.

---

[8] MSDN Library. How to Create a Customized Privacy Import File. 2002. http://msdn.microsoft.com/en-us/library/ms537344.

95. On September 10, 2010, researchers at Carnegie Mellon University published a technical report titled "Token Attempt: The Misrepresentation of Website Privacy Policies through the Misuse of P3P Compact Policy Tokens." *See* Ex. Z. This report described a research study in which the authors collected compact policies from 33,139 websites and used automated tools to check them for errors. The authors found errors in 11,176 compact policies on 4,696 domains, including 11 of the 50 most-visited websites.

96. The study reported that the most popular website to have a compact policy error was Facebook. The study reported that the Facebook compact policy at the time included only the tokens DSP and LAW, indicating that the Facebook privacy policy references a law that may determine remedies for breaches of their privacy policy and that there are ways to resolve privacy-related disputes. However, the Facebook compact policy was invalid because it did not include required tokens to disclose the categories of data associated with cookies, how they are used, who will receive the collected data, the data retention policy, and the policy on providing data access.

97. The report also stated, "When doing preliminary work for this study in 2009, the facebook.com compact policy contained only the single invalid token HONK... [T]hese CPs are useless for communicating with user agents and users. It is likely that facebook.com is using their CP to avoid being blocked by IE."

98. On September 16, 2010, Ryan McGeehan, a Security Incident Response Manager at Facebook emailed Dr. Lorrie Cranor, one of the authors of the report. He explained that he had seen the report and was trying to determine how to accurately represent Facebook's privacy policy in a P3P compact policy and "still enable functionality such as the like button."

99. On September 17, 2010, the New York Times Bits blog reported on the Carnegie Mellon study. The article included a comment from a Facebook spokesman:[9]

> A Facebook spokesman said in an e-mailed statement: "We're committed to providing clear and transparent policies, as well as comprehensive access to those policies. We're looking into the paper's findings to see what, if any, changes we can make." Ben Maurer, a software engineer at Facebook, said that the site used only two codes instead of five

[9] http://bits.blogs.nytimes.com/2010/09/17/a-loophole-big-enough-for-a-cookie-to-fit-through/

because current compact-policy codes do not "allow a rich enough description to accurately represent our privacy policy." Mr. Maurer said he did not know the history of how "HONK" made it into a compact policy.

100. Shortly thereafter, Facebook changed its compact policy to reflect the truth:

CP="Facebook does not have a P3P policy. Learn why here: http://fb.me/p3p"

101. By tricking IE with an intentionally invalid compact policy, Facebook was able to ensure that IE would improperly transmit a user-identifying Facebook cookie back to Facebook along with sensitive referrer URLs when users visited non-Facebook web sites that had Facebook like buttons or other embedded Facebook features.

V. FACEBOOK'S SURREPTITIOUS TRACKING REVEALED

102. In 2010, Australian researcher and blogger Nik Cubrilovic discovered that Facebook cookies were tracking users' Internet communications and accessing their computing devices and web browsers even after user had logged out of Facebook without the users' knowledge or consent. Cubrilovic's investigation revealed that several cookies that revealed personally identifiable information remained post logout, and some even remained after the browser was closed and restarted. Despite its representations to the contrary, Facebook was in fact secretly tracking its users' Internet communications and accessing their web-browsers without their knowledge or consent after logout.

103. Mr. Cubrilovic contacted Facebook on November 14, 2010 to report his findings and ask Facebook to fix the problem. He received no response. Again on January 12, 2011, Mr. Cubrilovic wrote to Facebook alerting it to his findings. Again, Facebook refused to respond. Mr. Cubrilovic of course had no way of knowing that Facebook [redacted]

104. On September 25, 2011, Mr. Cubrilovic made his findings public. He wrote, "Even if you are logged out, Facebook still knows and can track every page you visit." He explained that "[t]his is not what 'logout' is supposed to mean – Facebook is only altering the state of the cookies instead of removing all of them when a user logs out." Mr. Cubrilovic had revealed what [redacted]

[redacted]." *See* Ex. V (emphasis added).

105. Mr. Cubrilovic's blog post spread globally and was picked up the next day by the *Wall Street Journal*, in addition to dozens of other news outlets. Facebook engineer Gregg Stefancik contacted Mr. Cubrilovic and admitted he raised "important issues." However, Mr. Stafancik never disclosed that [redacted]. Instead, he falsely told Mr. Cubrilovic that a "bug" caused a particular user-identifying cookie, the a_user cookie, not to clear on logout, advising, "We will be fixing that today." Facebook further admitted that the Company had not "done as good a job as we could have to explain our cookie practices. Your post presents a great opportunity for us to fix that."

106. Mr. Stefancik also told Mr. Cubrilovic that "if you log out, [the lu] cookie does not contain your user ID" and is used to protect people using public computers. However, the lu cookie actually contained the encrypted user ID of the last user, so Mr. Stefancik's comment was deeply misleading. It would only be true if an intervening Facebook user were to use the shared computer and then the original user returned without logging into Facebook. For anyone else, the lu cookie continued to identify logged out users, and continued to do so for some time thereafter.

107. More than a month later, on Dec. 5, 2011, Facebook employee Tom Elliott [redacted]:

[redacted]

See Ex. AA.

108. Two days after the Cubrilovic revelations, on September 28, 2011, U.S. Representatives Edward Markey[10] and Joe Barton, Co-Chairmen of the Congressional Bi-Partisan Privacy Caucus, submitted a joint letter to the Chairman of the Federal Trade Commission urging the FTC to expand its investigation of Facebook. The FTC had already commenced an investigation related to the Like button roll-out and changes to the Facebook Privacy Policy in 2010, prior to discovery of the secret and pervasive post-logout tracking. Digital privacy rights group EPIC, joined by ten other civil liberties and privacy rights groups had also filed a complaint with the FTC on May 5, 2010 seeking to restrain Facebook's "data collection practices" among other relief, also before knowing about the post-logout tracking. *See* Ex. BB, Complaint in *EPIC vs. Facebook Inc.*

109. Congressmen Markey and Barton stated, "[I]n this instance, Facebook has admitted to collecting information about its users even *after its users had logged out of Facebook.*" They continued, "*We believe that tracking users without their knowledge or consent raises serious privacy concerns.* When users log-out of Facebook, they are under the impression that Facebook is no longer monitoring their activities. We believe this impression should be the reality."

110. The FTC sued Facebook under Section 5 of the FTC Act for multiple counts of misrepresenting its privacy policy, alleging that Facebook engaged in deceptive trade practices. *In the Matter of Facebook Inc.*, FTC File No. 0923184.

111. On November 29, 2011, Facebook settled, agreeing to an unprecedented 20 years of independent privacy audits. No fine was levied because a civil fine is not an available remedy absent a violation of a prior Commission order.

112. Marc Rotenberg, Executive Director of the Electronic Privacy Information Center, wrote to the FTC submitting an official comment and asking for clarification of a number of points, including whether the settlement covered Facebook's post-logout tracking. In response, the FTC confirmed it did. The complaint "does allege that Facebook violated Section 5 of the

[10] Congressman Markey is now Senator Markey.

FTC Act by falsely representing to users the protections provided by their privacy settings, [and] by making other false promises regarding privacy." *See* Letter from FTC to EPIC dated July 27, 2012 at p. 3 (Ex. CC). The FTC continued, "the proposed order contains provisions . . . designed to prevent Facebook from engaging in similar practices involving any Facebook product or service. These provisions are broad enough to address misconduct beyond that expressly challenged in the complaint." *Id*.

VI. PLAINTIFF-SPECIFIC FACTUAL ALLEGATIONS

113. Plaintiff Davis is an adult domiciled in Illinois and has an active Facebook account and had an active account during the entire proposed Class period.

114. She accessed the Internet and sent and received communications on several computing devices, including one that was not a shared computer that used Internet Explorer.

115. Using these same computers on which Facebook installed tracking and session cookies, Mrs. Davis visited websites after logging-out of her Facebook account which Facebook tracked, intercepted, and, in relation to which, Facebook accessed her computing device and web-browser. URLs for many of these websites contain detailed file paths containing the content of GET and POST communications, and are available to show the Court in camera if needed.

116. Plaintiff Quinn is an adult domiciled in Hawaii and has an active Facebook account and had an active account during the entire proposed Class period.

117. She accessed the Internet and sent and received communications on a computer that was not a shared computer that used Internet Explorer.

118. Using this same computer on which Facebook installed tracking and session cookies, Prof. Quinn visited websites after logging-out of her Facebook account which Facebook tracked, intercepted, and, in relation to which, Facebook accessed her computing device and web-browser. URLs for many of these websites contain detailed file paths containing the content of GET and POST communications, and are available to show the Court in camera if needed.

119. Plaintiff Lentz is an adult domiciled in North Carolina and has an active Facebook account and had an active account during the entire proposed Class period.

120. He accessed the Internet and sent and received communications on a computer shared with his wife that used Internet Explorer.

121. Using this same computer on which Facebook installed tracking and session cookies, Dr. Lentz visited websites after logging-out of his Facebook account which Facebook tracked, intercepted, and, in relation to which, Facebook accessed his computing device and web-browser. Dr. Lentz visited these websites immediately after logging out and prior to his wife using his computer. URLs for many of these websites contain detailed file paths containing the content of GET and POST communications, and are available to show the Court in camera if needed.

122. Plaintiff Vickery is an adult domiciled in Washington State and has an active Facebook account and had an active account during the entire proposed Class period.

123. He accessed the Internet and sent and received communications on a computer that was not a shared computer that used Google Chrome.

124. Using these same computers on which Facebook installed tracking and session cookies, Mr. Vickery visited websites after logging-out of his Facebook account which Facebook tracked, intercepted, and, in relation to which, Facebook accessed his computing device and web-browser. URLs for many of these websites contain detailed file paths containing the content of GET and POST communications, and are available to show the Court in camera if needed.

125. None of these four plaintiffs consented to the tracking and interception of their logged-off communications. Nor did they consent to Facebook's access to their computing devices and web-browsers while logged-off Facebook.

126. None of these four plaintiffs changed the default cookie blocking settings on their browsers during the Class Period.

127. None of these four plaintiffs installed extensions or plug-ins that disable or modify referrer headers sent to Facebook when visiting websites with embedded Facebook functionality.

128. Discovery is still ongoing, and despite Plaintiffs' document requests, Facebook has not yet produced any documents related to these plaintiffs. The parties have discussed this omission and Plaintiffs will continue to press for production.

VII. VALUE OF INTERCEPTED REFERRER URLS

129. Facebook is the brainchild of the Company's founder and Chief Executive Officer, Mark Zuckerberg, who wrote the first version of "The Facebook" in his Harvard University dorm room and launched the Company in 2004. The key to Facebook's success was to convince people to create unique, individualized profiles with such personal information as employment history and political and religious affiliations, which then could be shared among their own network of family and friends.

130. Facebook has become the largest social networking site in the world, approaching 1.5 billion members. At the end of the proposed Class Period, Facebook had over 800 million users world-wide and over 150 million users in the United States.

131. Facebook's enormous financial success is the result of connecting advertisers with its huge repository of personal data related to users. As Facebook explained in its Registration Statement following the end of the Class Period, "Advertisers can engage with more than 900 million monthly active users (MAUs) on Facebook or subsets of our users based on information they have chosen to share with us such as their age, location, gender, or interests. We offer advertisers a unique combination of reach, relevance, social context, and engagement to enhance the value of their ads." *See* Amendment No. 5 to Form S-1 Registration Statement, filed by Facebook, Inc. with the United States Securities and Exchange Commission on May 3, 2012 (the "Registration Statement") at 1.

132. From 2009 to 2012, over 90% of Facebook's revenue was attributable to third party advertising (*see* Registration Statement at 13), and now that Facebook is a public company, it is even more driven to continue to find new and creative ways to leverage its access to users' data in order to sustain its phenomenal growth (*see, e.g.*, Registration Statement at 88-91, 99-100).

133. Although Facebook does not require its members to pay a monetary subscription fee, ***membership is not free***, despite Facebook's false guarantee to the contrary. Facebook charges users by acquiring the users' sensitive and valuable personal information, which includes far more than mere demographic information and volunteering personal information like name,

birth date, gender and email address. More importantly, Facebook use entails Facebook's planting of numerous Facebook small text files, called cookies, on the user's computer and web-browser, which allows Facebook to track users' browsing histories and correlate them with user IDs – but – Facebook promised - only when users are logged in to Facebook.

134. The information Facebook tracks has and had massive economic value during the Class Period. This value is well understood in the e-commerce industry, and personal information is now viewed as a form of currency.

135. Professor Paul M. Schwartz noted in the Harvard Law Review:

> Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.

Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 HARV. L. REV. 2055, 2056-57 (2004). Professor Schwartz wrote those words in the same year Facebook was launched.

136. Likewise, in the *Wall Street Journal*, former fellow at the Open Society Institute (and current principal technologist at the ACLU) Christopher Soghoian noted:

> The dirty secret of the Web is that the "free" content and services that consumers enjoy come with a hidden price: their own private data. Many of the major online advertising companies are not interested in the data that we knowingly and willingly share. Instead, these parasitic firms covertly track our web-browsing activities, search behavior and geolocation information. Once collected, this mountain of data is analyzed to build digital dossiers on millions of consumers, in some cases identifying us by name, gender, age as well as the medical conditions and political issues we have researched online.
>
> Although we now regularly trade our most private information for access to social-networking sites and free content, the terms of this exchange were never clearly communicated to consumers.

Julia Angwin, *How Much Should People Worry About the Loss of Online Privacy?*, THE WALL STREET JOURNAL (Nov. 15, 2011).

137. The cash value of users' personal information provided during the Class Period to Facebook as a condition of membership can be quantified. For example, in a study authored by Tim Morey researchers studied the value that 180 internet users placed on keeping personal data secure.[11] Contact information of the sort that that Facebook requires was valued by the study participants at approximately $4.20 per year. Demographic information was valued at approximately $3.00 per year. But web browsing histories were valued at a much higher rate: $52.00 per year. The chart below summarizes the findings:

Across Facebook's approximately 800 million users at the end of the Class Period, these figures imply aggregate annual membership fees of $3.36 billion, $2.4 billion, and $41.6 billion, respectively, for each category of information.

138. Similarly, the value of user-correlated internet browsing history can be quantified, because companies were willing during the Class Period to pay users for the exact type of data that Facebook illegally intercepted from Plaintiffs and other members of the Class.

[11] ("What's Your Personal Data Worth? http://designmind.frogdesign.com/blog/what039s-your-personal-data-worth.html, Jan. 18, 2011).

139. For example, Google Inc. had a panel during the Class Period (and still has one today) called "Google Screenwise Trends" which, according to the Internet giant, is designed "to learn more about how everyday people use the Internet."

140. Upon becoming a panelist, Internet users would add a browser extension that shares with Google the sites that users visit and how the panelist uses them. The panelists consented to Google tracking this information for three months in exchange for one of a number of "gifts," including gift cards to retailers such as Barnes & Noble, Walmart and Overstock.com.

141. After three months, Google also agreed to pay panelists additional gift cards "for staying with" the panel. These gift cards, mostly valued at exactly $5, demonstrated conclusively that internet industry participants understood the enormous value in internet users' browsing habits. Indeed, Facebook's advertising revenues for 2011 roughly approximate $5 per user over its international user base of 800 million members, demonstrating the value of the information harvested by Facebook. Today, Google now pays Screenwise panelists up to $3 *per week* to be tracked.

142. In addition to the monetary value of user-correlated URLs, they have non-monetary privacy value. For example, in a recent study by the Pew Research Center, 93 percent of Americans said it was important for them to be "in control of who can get information" about them. Seventy-four percent said it was "very important." 87 percent of Americans said it was important for them not to have someone watch or listen to them without their permission. Sixty-seven percent said it was "very important." And 90 percent of Americans said it was important that they be able to "control[] what information is collected about [them]." Sixty-five percent said it was very important.

143. Likewise, in a 2011 Harris Poll study, 76 percent of Americans agreed that "online companies, such as Google or Facebook, control too much of our personal information and know too much about our browsing habits." 65 percent of American Facebook users said they were very or somewhat concerned about invasions of privacy "when using Facebook."

VIII. STATUTE OF LIMITATIONS

144. The following claims were brought on a class basis within days of the public reports of post-logout tracking, and the statutes of limitations are thus tolled: Violation of Federal Wiretap Act; Violation of the Stored Communications Act; Violation of CIPA § 631; Invasion of Privacy; Intrusion Upon Seclusion; Trespass to Chattels; and the California Computer Crime Law.

145. The following claims are new in this Second Amended Complaint but relate to the identical "conduct, transaction or occurrence" set out in the First Amended Complaint and thus relate back to the date of filing of the First Amended Complaint: CIPA § 632; Breach of Contract; Breach of the Duty of Good Faith and Fair Dealing; Civil Fraud; and California Statutory Larceny. All relevant statutes of limitations have therefore also been tolled.

IX. STATUS OF RELATED LITIGATION

A. Austria: *Schrems v. Facebook Ireland Limited*

146. On August 1, 2014, Austrian Facebook user Maximilian Schrems filed a class action against Facebook's European subsidiary alleging a number of privacy violations. An English-language version of the original complaint as provided by Mr. Schrems is attached as Ex. DD.

147. Section II.F (paragraphs 100 through 112) relate to the claims in this Action regarding data collection via Facebook social plug-ins including Like-buttons.

148. Section IV.A (paragraphs 180 through 194) set forth claims for damages under California law.

149. The Austrian action asserts 22 counts (numbered 1 through 21 plus claim 4.1) in the prayer for relief. Claims 7, 8 and 9 relate to consent generally, and claim 10 relates to social plug-ins (including the Like button) specifically.

150. The Austrian action, were it to proceed as a class action, is limited to Facebook users in Europe. Facebook users in the United States are specifically excluded from the proposed class definition.

151. On June 30, 2015, the Austrian regional court in Vienna (the "Landesgericht") dismissed the case for lack of jurisdiction, without addressing the merits.

152. On October 19, 2015, the Court of Appeals (the "Oberlandesgericht") reversed as to 20 of the 22 counts – agreeing with Facebook only as to the question of whether the case could proceed as a class action under Austrian law.

153. Mr. Schrems and Facebook both appealed to the Austrian Supreme Court (the "Oberster Gerichtshof") and on November 23, 2015, it was announced that the Supreme Court would hear the case.

B. Belgium: *Commission for the Protection of Privacy v. Facebook*

154. In January 2015, the Belgian Commission for the Protection of Privacy ("Privacy Commission"), following queries from Facebook users, media, and Parliament, launched an investigation of Facebook's privacy practices including the gathering of personal data and internet browsing history via the Like button.

155. On April 29, 2015, the Privacy Commission held a hearing and invited Facebook representatives as well as academic technical experts. At the hearing, the technical expert presented a draft report of their findings regarding Facebook social plug-ins. An updated English-language copy of the technical report dated June 24, 2015 is attached as Ex. L.

156. On May 13, 2015, the Privacy Commission issued Recommendation no. 04/2015, and found that Facebook tracks non-users' Internet browsing (or users' browsing post-logout) in violation of Belgian privacy law via the Like button, and recommended remedial action. The Privacy Commission sought an order from the Court of First Instance in Brussels via a writ of summons on June 10, 2015.

157. On November 9, 2015, the Court of First Instance granted the requested order, finding that non-consensual tracking of Internet browsing violates Belgian privacy law irrespective of how or whether Facebook uses the tracked data. The Court has not yet made an English-language version available, but the Privacy Commission summarized the order in English in an official summary on November 10, 2015, attached as Ex. EE.

158. The court ordered Facebook to stop tracking Internet users via the datr cookie and other means, and imposed a €250,000 fine for each day that Facebook fails to comply. The Court found that even anonymous tracking of users can violate European privacy laws, and also found the matter to be "urgent":

> because claims that relate to fundamental rights and freedoms (such as the protection of privacy) are always urgent, and because this claim does not relate to the fundamental right of one single individual but of an enormous group of people. Because of the millions of websites with Facebook social plug-ins, it is almost unavoidable to escape from these. In addition, it may relate to very sensitive data revealing, for instance, health or religious, sexual or political preference.

Summary of Court Order by the Privacy Commission, Ex. EE, section 2.

159. Facebook took issue with the Privacy Commission's use of the word "tracking," arguing instead to use the phrase "standard web impressions," and Facebook also argued that the tracking cookies (in particular the datr cookie) were necessary for security. The court rejected these arguments:

> With respect to the security argument invoked by Facebook, the Court finds it not credible that collecting the datr cookie each time a social plug-in is loaded on a website, would be necessary for the security of Facebook's services. According to the Court, "even an 'internet illiterate' understands that systematically collecting the datr cookie as such is insufficient to counter the attacks referred to by Facebook because criminals can very easily circumvent this cookie from being installed by means of software which blocks cookies being installed.

Id., section 4.

160. Facebook has stated that it "will appeal this decision" and is negotiating a resolution with the Belgian government while it awaits the official English translation of the order.

C. California: *Ung v. Facebook, Inc*.

161. In 2012, three California Facebook users filed a state-court class action in Superior Court in Santa Clara County. *Ung v. Facebook, Inc*., Case No. 1-12-cv-217244. Plaintiffs asserted various claims for invasion of privacy under California law related to Facebook's tracking of internet browsing via the Like button.

162. On July 2, 2012, the Superior Court denied in part and granted in part Facebook's demurrer. *See* Order of July 2, 2012 ("Ung Order"), attached as Ex. HH. Specifically, the court rejected Facebook's arguments regarding standing, and also found a fundamental privacy interest in users' internet browsing histories:

> Even tracking a portion of a person's browsing history, which would include visits to a large number of sites given that Facebook's cookies exist on millions of websites, can paint a comprehensive picture of a person's life. For example, repeated visits to certain websites could show a person has a particular disease, or religious affiliation, or is contemplating having an abortion.

Ung Order at 2-3.

163. The Superior Court also rejected Facebook's arguments regarding consent, and rejected Facebook's arguments regarding ordinary business practice. As to the latter argument, the Court noted that Facebook might be correct "as to the use of cookies on a single website," but:

> Facebook's alleged conduct goes far beyond that. Facebook is alleged to have used cookies to track large portions of people's browsing histories across numerous other websites so that a profile of each person can be put together . . . the Court finds that Facebook's alleged conduct constitutes a serious invasion of a privacy interest.

Id. at 4.

164. The *Ung* class action asserts claims only on behalf of California residents and thus only overlaps with the current Action for those class members who reside in California. Following the Ung Order, the court stayed the case pending a resolution of this Action.

D. Ireland: *Schrems v. Irish Data Protection Commissioner*

165. In 2013, following Edward Snowden's revelations of the NSA's bulk data collection programs, five complaints were filed in Europe to prevent the transfer of personal data from the European Economic Area (plus Switzerland, or "EEA/CH" for short). Complaints against Apple and Facebook were filed in Ireland, against Microsoft and Skype in Luxembourg, and against Yahoo in Germany.

166. The complaint against Facebook was made with the Irish Data Protection Commissioner (the "DPC") on June 25, 2013. The complaint alleged that Facebook's European subsidiary transferred protected "personal data" of EEA/CH citizens to Facebook, Inc. ("Facebook-US") in violation of data protection laws because Facebook-US could not guarantee the data would be protected from bulk surveillance by the NSA. The data includes but is not limited to Internet browsing history transferred to Facebook via Like-button functionality.

167. The DPC refused to investigate. Under an agreement with the United States in 2000 (the "Safe Harbor"), if a US company self-certifies that it complies with EU data protection laws, the transfer of personal data to the US would be lawful. Facebook self-certifies compliance with EU data protection laws, see, e.g., Privacy Policy dated April 22, 2010, section 1, attached as Ex. E, and thus the DPC found the complaint "frivolous." The DPC also found no evidence that the plaintiff's personal data specifically had be compromised.

168. The DPC's refusal to act was appealed to the Irish High Court, which ruled on June 18, 2014 that the data in question is "personal data" and the transfer would only be lawful if the Safe Harbor program was still valid. In light of the 2013 Snowden revelations, the Irish Court referred the matter to the European Court of Justice (the "ECJ"), the highest court in Europe. *See* Ex. FF, attached.

169. In the referral order of June 18, 2014, the High Court explicitly found that the plaintiff had standing to bring his complaint. The court noted:

> It is irrelevant that Mr. Schrems cannot show that his own personal data was accessed in this fashion by the NSA, since what matters is the essential inviolability of the personal data itself. The essence of that right would be compromised if the data subject had reason to believe that it

> could be routinely accessed by security authorities on a mass and undifferentiated basis.

Id., ¶ 75.

170. On October 6, 2015, in a landmark opinion, the ECJ invalidated the Safe Harbor. *See* Ex. GG. The ECJ noted that the processing of personal data is "liable to infringe fundamental freedoms." *Id*. ¶ 38. The court also held:

> To establish the existence of an interference with the fundamental right to respect for private life, it does not matter whether the information in question relating to public life is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference.

Id. ¶ 87.

171. Following the ECJ's ruling invalidating the Safe Harbor, the Irish High Court held further hearings on October 20, 2015, and immediately ordered that the DPC "is obligated now to investigate the complaint" against Facebook.

X. CLASS ACTION ALLEGATIONS

172. This is a class action pursuant to Rules 23(a) and (b)(3) of the Federal Rules of Civil Procedure on behalf of a Class of all persons who had active Facebook accounts and used Facebook between April 22, 2010 and September 26, 2011, both dates inclusive, and whose Internet use was tracked at times not logged into their Facebook accounts. Plaintiffs Quinn, Davis and Lentz also bring claims on behalf of a Subclass of Facebook subscribers who used Internet Explorer between April 22, 2010 and September 17, 2010, and whose Internet use was tracked while not logged into their Facebook accounts.

173. Excluded from the Class and the Subclass are the Court, Facebook, and its officers, directors, employees, affiliates, legal representatives, predecessors, successors and assigns, and any entity in which any of them have a controlling interest.

174. The members of the Class and Subclass are so numerous that joinder of all members is impracticable.

175. Common questions of law and fact exist as to all members of the Class and Subclass and predominate over any questions affecting solely individual members of the Class.

The questions of law and fact common to the Class and Subclass include whether Facebook violated state and federal laws by tracking Internet use and intercepting the communication of its users after the users had logged off of Facebook. Additional questions of fact and law are common to the Subclass related to Facebook's circumvention of default privacy protections on Internet Explorer during the Subclass Period.

176. Plaintiffs' claims are typical of the claims of other Class and Subclass members, as all members of the Class and Subclass were similarly affected by Facebook's wrongful conduct in violation of federal law as complained of herein.

177. Plaintiffs will fairly and adequately protect the interests of the members of the Class and Subclass and have retained counsel that is competent and experienced in class action litigation. Plaintiffs have no interest that is in conflict with, or otherwise antagonistic to the interests of the other Class or Subclass members.

178. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. Furthermore, as the damages individual Class and Subclass members have suffered may be relatively small, the expense and burden of individual litigation make it impossible for members of the Class and Subclass to individually redress the wrongs done to them. There will be no difficulty in management of this action as a class action.

XI. COUNTS

COUNT I

VIOLATION OF THE FEDERAL WIRETAP ACT, 18 U.S.C. § 2510, *ET. SEQ.*

179. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

180. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, prohibits the intentional interception of the contents any wire, oral, or electronic communication through the use of a device. 18 U.S.C. § 2511.

181. The Wiretap Act protects both the sending and receipt of communications.

182. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral or electronic communication is intercepted.

183. Facebook's actions in intercepting and tracking user communications while they were logged-off of Facebook was intentional as shown by the internal company emails detailed above.

184. Facebook's interception of Internet communications that the Plaintiffs were sending and receiving while logged-off Facebook (i.e., the referrer URLs) was done contemporaneously with the Plaintiffs' sending and receipt of those communications. In fact, Facebook received the communications before the communication between the plaintiffs and the various websites were completed.

185. The referrer URLs intercepted by Facebook included "contents" of electronic communications made from the plaintiffs to websites other than Facebook in the form of detailed URL requests and search queries which plaintiffs sent to those websites and for which plaintiffs received communications in return from those websites.

186. The transmission of data between plaintiffs and the websites on which Facebook tracked and intercepted their communications without authorization while they were logged-off were "transfer[s] of signs, signals, writing, … data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce[,]" and were therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

187. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. The cookies Facebook used to track the Plaintiffs' communications while they were logged-off of Facebook;

b. The Plaintiffs' browsers;

c. The Plaintiffs' computing devices;

d. Facebook's web servers;

e. The web-servers of websites from which Facebook tracked and intercepted the Plaintiffs' communications while they were logged-off of Facebook; and

f. The computer code deployed by Facebook to effectuate its tracking and interception of the Plaintiffs' communications while logged-off of Facebook;

g. The plan Facebook carried out to effectuate its tracking and interception of the Plaintiffs' communications while logged-off of Facebook

188. Facebook was not an authorized party to the communication because the Plaintiffs were unaware of Facebook's redirecting of the referrer URLs to Facebook itself, did not knowingly send any communication to Facebook, and were logged-off of Facebook when Facebook intercepted the communications between the Plaintiffs and websites other than Facebook. Facebook could not manufacture its own status as a party to the Plaintiffs' communications with others by surreptitiously redirecting or intercepting those communications.

189. As illustrated herein, "the" communications between the Plaintiffs and websites were simultaneous to, but *separate* from, the channel through which Facebook acquired the contents of those communications.

190. The Plaintiffs did not consent to Facebook's continued gathering of user IDs post-logout, and thus never consented to Facebook's interception of the referrer URLs to track or intercept their communications while they were logged-off of Facebook. Facebook explicitly promised Plaintiffs and the public that it would not track and intercept their communications to and from other websites while they were logged-off of Facebook except on an anonymous basis. Because the referrer URLs were intercepted with user-specific and user-identifying cookies included, no valid consent can exist.

191. After intercepting the communications, Facebook then used the contents of the communications knowing or having reason to know that such information was obtained through the interception of electronic communications in violation of 18 U.S.C. § 2511(1)(a).

192. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages to Plaintiffs; injunctive and declaratory relief; punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by

Defendant in the future, and a reasonable attorney's fee and other litigation costs reasonably incurred

COUNT II

VIOLATION OF THE STORED COMMUNICATIONS ACT, 18 U.S.C. § 2701, ET. SEQ.

193. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

194. The Stored Communications Act ("SCA") provides a cause of action against a person who "intentionally accesses without authorization a facility through which an electronic communication service is provided" or "who intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such a system." 18 U.S.C. § 2701(a).

195. The SCA defines an "electronic communication service" as "any services which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

196. Internet Service Providers provide a service – to allow users to send and receive electronic communications on the Internet. Accordingly, ISPs qualify as ECSs under the SCA. Each of the four plaintiffs used an ISP to communicate with first-party websites.

197. The web browsers used by the plaintiffs also qualify as ECSs because they allow users to send and receive electronic communications over the Internet. Each web browser provider requires users to agree to a Terms of Service or licensing agreement. Google has explained that a web browser is where Internet users "search, chat, email, and collaborate," and, "in our spare time, we shop, bank, read news, and keep in touch with friends – all using a browser."

198. The SCA does not provide a separate definition for "facility" but instead it is defined within the context of the sentence in which it is used. A "facility" under the SCA is, under the plain language of the statute, that "through which an electronic communication service is provided." 18 U.S.C. § 2701(a).

199. The items through which the electronic communication services of the Plaintiffs' ISPs and web-browsers include:

a. The Plaintiffs' personal computing devices;

b. The Plaintiffs' web-browsers; and

c. The browser-managed files which, together, constitute all of the programs contained within the Plaintiffs' web-browsers.

200. Facebook intentionally accessed the Plaintiffs' personal computing devices, web-browsers, and browser-managed files while the Plaintiffs were logged-off of Facebook.

201. The Plaintiffs did not authorize Facebook to track their communications and access their personal computers, web-browsers, and browser-managed files while they were logged-off of Facebook if such communications (the referrer URLs) were coupled with user-identifying cookies.

202. The detailed URLs obtained by Facebook contain contents.

203. The SCA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof;" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

204. Web browsers store cookie information and referrer URLs in browser-managed files that are temporary, intermediate and incidental to the electronic transmission of electronic communications.

205. Web-browsers store cookie information and referrer URLs for purposes of back-up protection.

206. Web-browsers store a copy of the Plaintiffs' URL requests in the toolbar while the user remains present at a particular webpage. When the user leaves the webpage, the copy of the detailed URL request is no longer present on the toolbar. Storage in the toobar after the user hits the Enter button or clicks on a link is "incidental to the electronic communication thereof" because once a user hits Enter or clicks on a link, the communication is in the process of being sent and received between the user and the first-party website.

207. Web-browsers also immediately store a copy of users' detailed URL requests in their browsing history. The precise length of time that each web-browser keeps a copies of users'

URL requests varies. For example, Google Chrome stores browsing history for approximately 90 days while Microsoft Internet Explorer only stores the browsing history for three weeks. Storage via browsing history qualifies as "temporary storage" because it exists in browsing history for "purposes of backup protection" to benefit the users of the web-browsing service.

208. Plaintiffs and Class Members were harmed by Facebook's actions, and pursuant to 18 U.S.C. § 2707(c), are entitled to actual damages including profits earned by Facebook attributable to the violations or statutory minimum damages of $1,000 per plaintiff, punitive damages, costs, and reasonable attorney's fees.

COUNT III

VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT CALIFORNIA CRIMINAL CODE §§ 631 AND 632

209. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

210. The California Invasion of Privacy Act is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

Cal. Penal Code § 630.

211. Cal. Penal Code § 631(a) provides, in pertinent part:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner ….willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to lawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not

exceeding two thousand five hundred dollars …

212. California Penal Code § 632 provides, in pertinent part:

> Every person who, intentionally and without the consent of all parties to a confidential communication, by means of any electronic amplifying or recording device, eavesdrops upon or records the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio, shall be punished by a fine not exceeding two thousand five hundred dollars.

213. Under either section of the CIPA, a defendant must show it had the consent of all parties to a communication.

214. Facebook is headquartered in California; designed and contrived and effectuated its scheme to track its users while logged-off from California; and has adopted California substantive law to govern its relationship with its users.

215. At all relevant times, Facebook's tracking and interceptions of the Plaintiffs' Internet communications while logged-off of Facebook was without authorization and consent from the Plaintiffs.

216. Facebook's non-consensual tracking of logged-out users' Internet browsing was designed to attempt to learn at least some meaning of the content in the URLs.

217. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, Facebook's deliberate and admittedly purposeful scheme that facilitated its interceptions falls under the broad statutory catch-all category of "any other manner":

a. The cookies Facebook used to track the Plaintiffs' communications while they were logged-off of Facebook;

b. The Plaintiffs' browsers;

c. The Plaintiffs' computing devices;

d. Facebook's web servers;

e. The web-servers of websites from which Facebook tracked and intercepted the Plaintiffs' communications while they were logged-off of Facebook; and

f. The computer code Facebook deployed to effect its tracking and interception of the Plaintiffs' communications while Plaintiffs were logged-off of Facebook;

g. The plan Facebook carried out to achieve its tracking and interception of the Plaintiffs' communications while they were logged-off of Facebook

218. Plaintiffs and Class Members have suffered loss by reason of these violations, including, but not limited to, violation of their rights to privacy and loss of value in their personally-identifiable information.

219. Pursuant to Cal. Pen. Code § 637.2, Plaintiffs and the Class have been injured by the violations of Cal. Pen. Code §§ 631 and 632, and each seek damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive relief.

COUNT IV

INVASION OF PRIVACY

220. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

221. Article I, section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, *and privacy*." The phrase "*and privacy*" was added by the "Privacy Initiative" adopted by California voters in 1972.

222. The right to privacy in California's constitution creates a right of action against private as well as government entities.

223. The principal purpose of this constitutional right was to protect against unnecessary information gathering, use and dissemination by public and private entities, [including] computer stored and generated dossiers and cradle-to-grave profiles on every American.

224. To plead a California constitutional privacy claim, a plaintiff must show an invasion of (1) a legally protected privacy interest; (2) where the plaintiff had a reasonable expectation of privacy in the circumstances; and (3) conduct by the defendant constituting a serious invasion of privacy.

225. As described herein, Facebook has intruded upon the following legally protected privacy interests:

a. A Fourth Amendment right to privacy contained on personal computing devices, including web-browsing history, as explained by the United States Supreme Court in the unanimous decision of *Riley v. California*;

b. The federal and California Wiretap Acts as alleged herein;

c. The Stored Communications Act as alleged herein;

d. The California Computer Crime Law, Cal Pen. Code § 502, which applies to all plaintiffs in this case by virtue of Facebook's choice of California law to govern its relationship with Facebook users;

e. Cal. Penal Code § 484(a) which prohibiting the knowing theft or defrauding of property "by any false or fraudulent representation or pretense[.]"

f. The Facebook Statement of Rights and Responsibilities; Data Use Policy, Privacy Policy, and other public promises Facebook made not to track or intercept the Plaintiffs' communications or access their computing devices and web-browsers while logged-off of Facebook.

g. The Pen Register Act, codified in 18 U.S.C. § 3121, which prohibits the non-consensual installation or use of a "pen register" or "trap and trace" device. Under the statute, a "pen register" is "a device or process which records or decodes dialing, routing, addressing, or signaling (DRAS) information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication." The

cookies and URLs at issue in this case contain both "content" and DRAS information and therefore fall under both the Wiretap and Pen Register Acts. Similarly, a "trap and trace device" is a "device or process which captures the incoming electronic or other impulses which identify the originating number or other DRAS information reasonably likely to identify the source of a wire or electronic communication." The cookies at issue in this case also work as "trap and trace" devices because, in addition to capturing content, they also capture impulses identifying the originating number of other DRAS information of communications. The Pen Register Act creates a statutorily protected privacy interest in an Internet user's IP address.

226. Plaintiffs had a reasonable expectation of privacy in the circumstances in that:

a. Plaintiffs could not reasonably expect Facebook would commit acts in violation of federal and state civil and criminal laws;

b. Facebook affirmatively promised users it would not track their communications or access their computing devices or web-browsers while they were logged-off of Facebook.

227. Facebook's actions constituted a serious invasion of privacy in that they:

a. Invaded a zone of privacy protected by the Fourth Amendment, namely the right to privacy in data contained on personal computing devices, including web search and browsing histories;

b. Violated several federal criminal laws, including the Wiretap Act, Stored Communications Act, and Pen Register Act;

c. Violated dozens of state criminal laws;

d. Invaded the privacy rights of hundreds of millions of Americans without their consent;

e. Constituted the unauthorized taking of valuable information from hundreds of millions of Americans through deceit;

f. Took actions constituting exactly what the drafters of the Privacy Initiative sought to stop, namely the collection and stockpiling by a business of unnecessary information without consent, and the misuse of information gathered for one purpose in order to serve other purposes.

228. Committing criminal acts against hundreds of millions of Americans constitutes an egregious breach of social norms.

229. The surreptitious and unauthorized tracking of the internet communications of millions of Americans' constitutes an egregious breach of social norms.

230. Facebook lacked a legitimate business interest in tracking users while they were logged-off of Facebook without their consent.

231. Plaintiffs have been damaged by Facebook's invasion of their privacy and are entitled to just compensation.

COUNT V

INTRUSION UPON SECLUSION

232. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

233. Plaintiffs asserting claims for intrusion upon seclusion must plead (1) intrusion into a private place, conversation, or matter; (2) in a manner highly offensive to a reasonable person.

234. In carrying out its scheme to track and intercept Plaintiffs' communications and access their computing devices and web-browsers while they were logged-off of Facebook in violation of its own privacy promises, Facebook intentionally intruded upon the Plaintiffs' solitude or seclusion in that it effectively placed itself in the middle of conversations to which it was not an authorized party.

235. Facebook's tracking and access was not authorized by the Plaintiffs, the websites with which they were communicating, the Plaintiffs' Internet Service Providers, or the Plaintiffs' web-browsers.

236. Defendant's intentional intrusion into their Internet communications and their computing devices and web-browsers was highly offensive to a reasonable person in that they

violated federal and state criminal and civil laws designed to protect individual privacy and against theft.

237. The taking of personally-identifiable information from hundreds of millions of Americans through deceit is highly offensive behavior.

238. Secret monitoring of web browsing is highly offensive behavior.

239. Wiretapping and surreptitious recording of communications is highly offensive behavior.

240. Public polling on Internet tracking has consistently revealed that the overwhelming majority of Americans believe it is important or very important to be "in control of who can get information" about them; to not be tracked without their consent; and to be in "control[] of what information is collected about [them]."

241. Plaintiffs have been damaged by Facebook's invasion of their privacy and are entitled to reasonable compensation including but not limited to disgorgement of profits related to the unlawful internet tracking.

COUNT VI

BREACH OF CONTRACT

242. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

243. Facebook's relationship with its users is governed by the Statement of Rights and Responsibilities and several other documents and policies, including a Data Use Policy and a Privacy Policy.

244. The governing documents contain enforceable promises that Facebook made to the Plaintiffs and the Class.

245. In the governing documents, Facebook promised that it would not track user's web browsing after log-out except on an anonymous basis. Facebook unambiguously emphasized, "When you log out of Facebook, we remove the cookies that identify your particular account."

246. Despite this promise, Facebook received more than mere "technical information" about its users' IP addresses, browsers, and operating systems, but instead received personally-identifiable information about the same that were akin to and directly connect in Facebook's

databases to the very User ID which Facebook promised only to track for logged-in users.

247. The governing documents constitute Facebook's offer to potential users of its products, by which Facebook promises to respect those users' privacy in specified ways, including by not tracking or intercepting users' Internet communications or accessing their computing devices or web-browsers while users were logged-off of Facebook. Plaintiffs and other Class members accepted Facebook's offer by using Facebook.

248. The promises contained in Facebook's governing documents and the Plaintiffs' and other Class members' use of Facebook are each sufficient consideration to support Facebook's contractual obligations to Plaintiffs.

249. Under the agreement, Plaintiffs and Class members transmitted personally identifiable information to Facebook in exchange for use of Facebook and Facebook's promise that it would not track users' communications or access their computing devices or web-browsers while the users were logged-off of Facebook.

250. By reason of the conduct described herein, Facebook materially and uniformly breached its contract with Plaintiffs and each of the Class members by tracking and intercepting the Internet communications and accessing the computing devices and web-browsers of Facebook users while they were logged-off of Facebook.

251. Facebook collects revenues in large part because the personal information submitted by its users and the tracking of their Internet communications across a wide variety of websites increases the value of Facebook's advertising services. As a result of Facebook's breach of the contract, it was unjustly enriched.

252. As a further result of Facebook's breach, Plaintiffs and the class sustained non-monetary privacy damages. Plaintiffs and Class Members also did not receive the benefit of the bargain for which they contracted and for which they paid valuable consideration in the form of their personally-identifiable information, which, as alleged above, has ascertainable value to be proven at trial.

COUNT VII

BREACH OF THE DUTY OF GOOD FAITH AND FAIR DEALING

253. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

254. Every contract imposes upon each party a duty of good faith and fair dealing in its performance and enforcement.

255. In dealing between Facebook and its users, Facebook is invested with discretionary power affecting the rights of its users.

256. Facebook purports to respect and protect its users' privacy.

257. Despite its contractual privacy promises not to track users while they were logged-off of Facebook, in fact, Facebook took actions outside those contractual promises to track users while they were logged-off and to deprive Plaintiffs and the class of the benefits of their contract with Facebook – that Facebook would not track logged-off users and use the information to increase revenues.

258. Facebook's tracking and interception of the Internet communications and access to the computing devices and web-browsers of logged-off users was objectively unreasonable given Facebook's privacy promises.

259. Facebook's conduct in tracking and intercepting the Internet communications and accessing the computing devices and web-browsers of logged-off users evaded the spirit of the bargain made between Facebook and the plaintiffs.

260. Facebook's conduct in this case abused its power to specify terms – in particular, Facebook's failed to accurately disclose its tracking of users while they were logged-off of Facebook.

261. As a result of Facebook's misconduct and breach of its duty of good faith and fair dealing, Plaintiffs and the Class suffered damages. Plaintiffs and the Class members did not receive the benefit of the bargain for which they contracted and for which they paid valuable consideration in the form of their personal information, which, as alleged above, has ascertainable value to be proven at trial.

COUNT VIII

CIVIL FRAUD
VIOLATION OF CAL. CIV. CODE §§ 1572 AND 1573

262. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

263. Cal. Civ. Code § 1572 provides in relevant part that actual fraud exists when a party to a contract suppresses "that which is true, by one having knowledge or belief of the fact" "with intent to deceive another party thereto, or to induce him to enter into the contract."

264. Cal. Civ. Code § 1573 provides in relevant part that constructive fraud exists "[i]n any such act or omission as the law specially declares to be fraudulent, with respect to actual fraud."

265. Facebook violated § 1572 through its repeated and false assertions that it did not track or intercepts users' communications or access their computing devices or web-browsers while they were logged-off of Facebook.

266. Facebook further violated § 1572 by suppressing knowledge of its tracking, intercepting, and accessing Plaintiffs' Internet communications, computers, and web-browsers while they were logged-off of Facebook.

267. Plaintiffs relied on Facebook's false assertions in contracting with and using Facebook.

268. Additionally and/or alternatively, Facebook violated § 1573 by breaching its duty not to track, intercept, or access its users' Internet communications, computers, or web-browsers while they were logged-off of Facebook and gaining an advantage by doing so, by misleading users to their prejudice, as describe herein.

269. Plaintiffs, on behalf of themselves and the Class, seek damages from Facebook, including but not limited to disgorgement of all proceeds Facebook obtains from its unlawful business practices.

COUNT IX

TRESSPASS TO CHATTELS

270. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

271. Defendant, intentionally and without consent or other legal justification, failed to delete cookies on Plaintiffs' browsers after logout, enabling Facebook to connect Plaintiffs' personally identifiable information to specific communications.

272. Defendant, intentionally and without consent or other legal justification, also placed cookies on Plaintiffs' computers post-logout without consent which allowed Facebook to track their activity while logged-off of Facebook.

273. Defendant's intentional and unjustified placing of a cookie designed to track Plaintiffs' internet activities while logged-off of Facebook and actual tracking of Plaintiffs activities interfered with Plaintiffs' use of the following personal property owned by Plaintiffs: (a) Plaintiffs' computers; and (b) Plaintiffs' personally identifiable information.

COUNT X

VIOLATIONS OF CALIFORNIA PENAL CODE § 502
THE CALIFORNIA COMPUTER CRIME LAW ("CCCL")

274. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

275. Defendant violated Cal. Penal Code § 502(c)(2) by knowingly and without permission accessing, taking and using Plaintiffs' and the Class Members' personally identifiable information.

276. Defendant accessed, copied, used, made use of, interfered with, and/or altered data belonging to Plaintiffs and Class Members: (1) in and from the State of California; (2) in the states in which the Plaintiffs and the Class Members are domiciled; and (3) in the states in which the servers that provided services and communication links between Plaintiffs and the Class Members and Facebook.com and other websites with which they interacted were located.

277. Cal. Penal Code § 502 provides: "For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction."

278. Defendants have violated California Penal Code § 502(c)(1) by knowingly and without permission altering, accessing, and making use of Plaintiffs and Class Members'

personally identifiable data in order to execute a scheme to defraud consumers by utilizing and profiting from the sale of their personally identifiable data, thereby depriving them of the value of their personally identifiable data.

279. Defendants have violated California Penal Code § 502(c)(6) by knowingly and without permission providing, or assisting in providing, a means of accessing Plaintiffs' and Class Members' computer systems and/or computer networks.

280. Defendants have violated California Penal Code § 502(c)(7) by knowingly and without permission accessing, or causing to be accessed, Plaintiffs' and Class Members' computer systems and/or computer networks.

281. Pursuant to California Penal Code § 502(b)(10) a "Computer contaminant" is defined as "any set of computer instructions that are designed to ... record, or transmit information within computer, computer system, or computer network without the intent or permission of the owner of the information."

282. Defendants have violated California Penal Code § 502(b)(8) by knowingly and without permission introducing a computer contaminant into the transactions between Plaintiffs and the Class Members and websites; specifically, a "cookie" that intercepts and gathers information concerning Plaintiffs' and the Class Members' interactions with certain websites, which information is then transmitted back to Facebook.

283. As a direct and proximate result of Defendant's unlawful conduct within the meaning of California Penal Code § 502, Defendant has caused loss to Plaintiffs and the Class Members in an amount to be proven at trial. Plaintiffs and the Class Members are also entitled to recover their reasonable attorneys' fees pursuant to California Penal Code § 502(e).

284. Plaintiffs and the Class Members seek compensatory damages, in an amount to be proven at trial, and declarative or other equitable relief.

285. Plaintiffs and the Class Members are entitled to punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) because Defendant's violations were willful and, upon information and belief, Defendant is guilty of oppression, fraud, or malice as defined in Cal. Civil Code § 3294.

COUNT XI

STATUTORY LARCENY
CALIFORNIA PENAL CODE §§ 484 AND 496

286. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

287. Section 496(a) prohibits the obtaining of property "in any manner constituting theft."

288. Section 484 defines theft, and provides:

> Every person who shall feloniously steal, take, carry, lead, or drive away the personal property of another, or who shall fraudulently appropriate property which has been entrusted to him or her, or who shall knowingly and designedly, by any false or fraudulent representation or pretense, defraud any other person of money, labor or real or personal property, or who causes or procures others to report falsely of his or her wealth or mercantile character and by thus imposing upon any person, obtains credit and thereby fraudulently gets or obtains possession of money, or property or obtains the labor or service of another, is guilty of theft.

289. Section 484 thus defines "theft" to include obtaining property by false pretense.

290. Defendant intentionally designed a program that would operate in a manner unbeknownst to Plaintiffs whose computers were thus deceived into providing personally identifiable information to Defendant.

291. Defendant acted in a manner constituting theft and/or false pretense.

292. Defendant stole, took, and/or fraudulently appropriated Plaintiffs' PII without Plaintiffs consent.

293. Defendant concealed, aided in the concealing, sold, and/or utilized Plaintiffs PII that was obtained by Defendant for Defendant's commercial purposes and the financial benefit of Defendant.

294. Defendant knew that Plaintiffs' PII was stolen and/or obtained because Defendant's intentionally failed to delete user-identifying cookies which enabled Defendant to steal and/or obtain Plaintiffs' PII in a manner that was concealed and/or withheld from Plaintiffs.

295. The reasonable and fair market value of the unlawfully obtain personal data can be determined in the marketplace.

XII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court:

A. Certify this action is a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure;

B. Award compensatory damages, including statutory damages where available, to Plaintiffs and the Class against Defendant for all damages sustained as a result of Defendant's wrongdoing, in an amount to be proven at trial, including interest thereon;

C. Permanently restrain Defendant, and its officers, agents, servants, employees and attorneys, from installing cookies on its users' computers that could track the users' computer usage after logging out of Facebook or otherwise violating its policies with users;

D. Award Plaintiffs and the Class their reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

E. Grant Plaintiffs such further relief as the Court deems appropriate.

XIII. JURY TRIAL DEMAND

The Plaintiffs demand a trial by jury of all issues so triable.

Dated: November 30, 2015

KIESEL LAW LLP

By: */s/ Paul R. Kiesel*
Paul R. Kiesel (SBN 119854)
8648 Wilshire Blvd.
Beverly Hills, CA 90211-2910
Telephone: (310) 854-4444
Facsimile: (310) 854-0812
kiesel@kiesel-law.com

Interim Liaison Counsel

SILVERMAN, THOMPSON, SLUTKIN & WHITE LLC

By: */s/ Stephen G. Grygiel*
Stephen G. Grygiel (admitted *pro hac vice*)
201 N. Charles St., #2600
Baltimore, MD 21201
Telephone (410) 385-2225
Facsimile: (410) 547-2432
sgrygiel@mdattorney.com

Interim Co-Lead Counsel

KAPLAN, FOX & KILSHEIMER LLP

By: */s/ David A. Straite*
Frederic S. Fox (admitted *pro hac vice*)
David A. Straite (admitted *pro hac vice*)
850 Third Avenue
New York, NY 10022
Telephone: (212) 687-1980
Facsimile: (212) 687-7714
dstraite@kaplanfox.com

Laurence D. King (206423)
Mario Choi (243409)
350 Sansome Street, 4th Floor
San Francisco, CA 94104
Tel.: (415) 772-4700
Fax: (415) 772-4707
lking@kaplanfox.com

Interim Co-Lead Counsel

CERTIFICATE OF SERVICE

I hereby certify that on November 30, 2015, I caused the foregoing to be electronically filed with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the e-mail addresses denoted on the Electronic Mail Notice List.

I certify under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on November 30, 2015.

KIESEL LAW LLP

/s/ *Paul R. Kiesel*

Paul R. Kiesel
kiesel@kbla.com
8648 Wilshire Boulevard
Beverly Hills, California 90211
Tel.: (310) 854-4444
Fax: (310) 854-0812

Interim Liaison Counsel